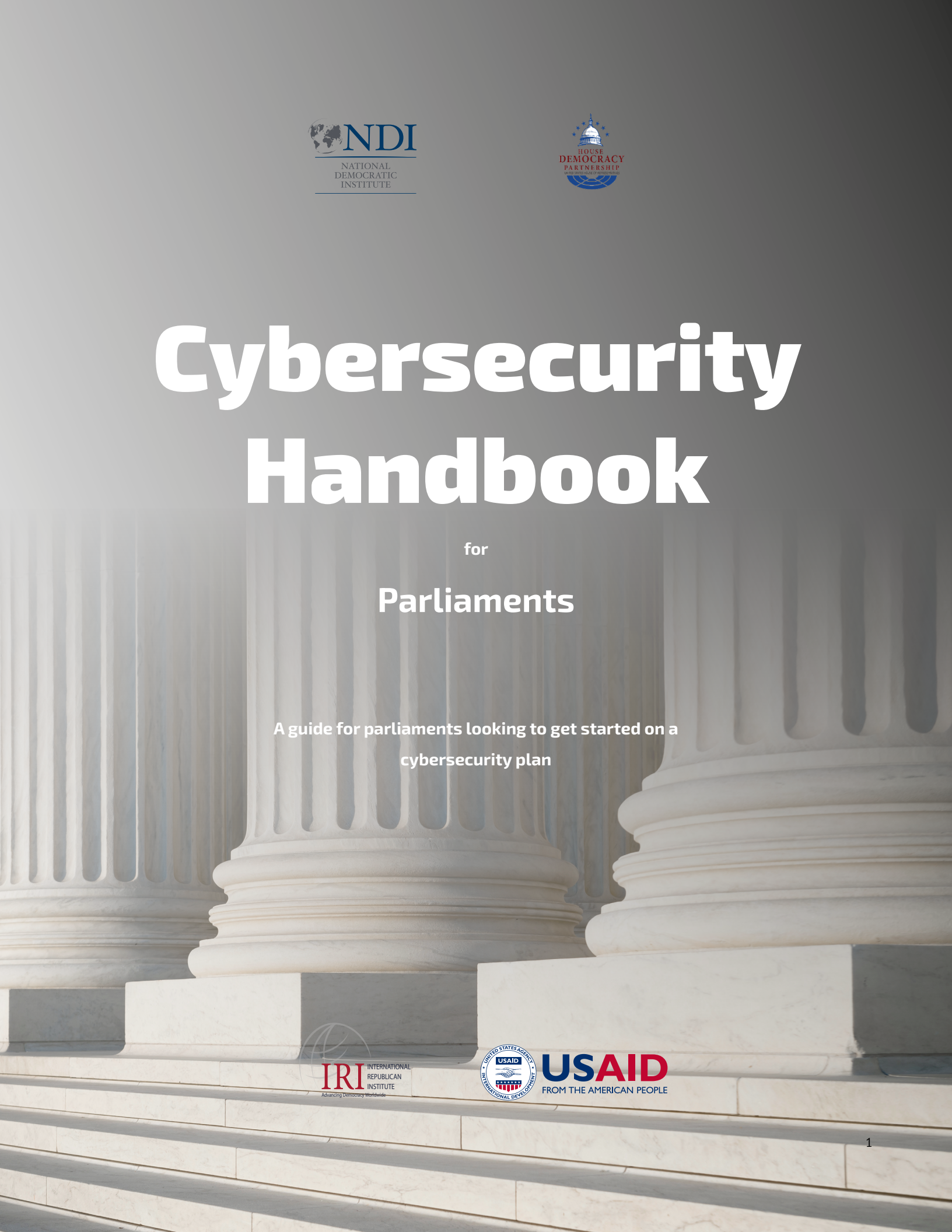


NDI
NATIONAL DEMOCRATIC INSTITUTE

HOUSE DEMOCRACY PARTNERSHIP

Cybersecurity Handbook

for

Parliaments

A guide for parliaments looking to get started on a cybersecurity plan

IRI INTERNATIONAL REPUBLICAN INSTITUTE
Advancing Democracy Worldwide

USAID
FROM THE AMERICAN PEOPLE

NDI
NATIONAL DEMOCRATIC INSTITUTE

HOUSE DEMOCRACY PARTNERSHIP
UNITED STATES HOUSE OF REPRESENTATIVES

Cybersecurity Handbook

for

Parliaments

A guide for parliaments looking to get started on a cybersecurity plan

IRI INTERNATIONAL REPUBLICAN INSTITUTE
Advancing Democracy Worldwide

USAID
FROM THE AMERICAN PEOPLE

Table of Contents

Visual Legend

Throughout the Handbook, you will find a few different recurring, highlighted elements in addition to the main text. Here is a short "legend" to help you understand the core elements:

Case Study

Indicates case studies that highlight the real-life impact of a certain topic on parliaments globally or in a specific country.

Extra Tips

Highlights some extra tips and information to pay attention to as you read the Handbook.

Real World

Calls out common examples of cybersecurity tactics tools used in the "real world", both for good and for bad.

Advanced

Indicates an advanced topic - information that is important for your parliament to consider, but that might be a bit more technical or complicated.

Security Plan Building Blocks

Indicates the "Security Plan Building Blocks", which are the key take-aways from each section of the Handbook.

The Top 10

These 10 elements are critical to your parliament's security plan. If you are looking for somewhere to start, look here first.

1. **Conduct regular security training within your parliament**
2. **Be alert to phishing and have a reporting system**
3. **Use encryption for all communication - end-to-end, when possible**
4. **Require strong passwords and implement a password manager across your parliament**
5. **Require two-factor authentication wherever possible**
6. **Ensure all staff devices and software are kept up-to-date**
7. **Use secure cloud storage**
8. **Use HTTPS and, if appropriate, a VPN, for accessing the internet**
9. **Protect your parliament's physical assets**
10. **Develop an organizational incident response plan**

1

Building a Culture of Security

2

A Strong Foundation: Securing Accounts and Devices

3

Communicating and Storing Data Securely

4

Staying Safe on the Internet

5

Protecting Physical Security

6

What To Do When Things Go Wrong

Authors & Acknowledgments

This guide was produced by the National Democratic Institute (NDI) and House Democracy Partnership (HDP).

Lead Author: **Evan Summers (NDI)**
Contributing Authors: **Sarah Moulton (NDI); Chris Doten (NDI)**

In developing this Handbook, we'd like to particularly thank our expert external reviewers who provided us with valuable feedback, edits, and suggestions as we pulled together this content, including:

Fiona Krakenburger, Open Technology Fund; Bill Budington and Shirin Mori, Electronic Frontier Foundation; Jocelyn Woolbright, Cloudflare; Martin Shelton, Freedom of the Press Foundation; Dave Leichtman, Microsoft; Stephen Boyce, International Foundation for Electoral Systems; Amy Studdart, International Republican Institute; Emma Hollingsworth, Global Cyber Alliance; Caroline Sinders, Convocation Design + Research; Dhyta Caturani; Sandra Pepera, NDI; Aaron Azelton, NDI; Frieda Arenos, NDI; Anthony DeAngelo, NDI; Whitney Pfeifer, NDI; and Derek Luyten, House Democracy Partnership. We would also like to thank Paul Kollie at the Legislative Information Services in Liberia, Nihad Bahram and Fuad Ahmed at the Kurdistan parliament in Iraq, Diana Plata at the Senate of Colombia; Ayad Abbas and Majid Khudhur at the Iraqi Council of Representatives, and Tanja Danailovska at the Assembly of North Macedonia for their valuable insights and contributions.

We also want to acknowledge all the incredible manuals, guides, workbooks, training modules and other materials developed and maintained by the Organizational Security (OrgSec) Community. This Handbook is designed to complement those more in-depth materials, combining key lessons into a one-stop, easy-to-read resource for parliaments looking to get started on a cybersecurity plan.

In addition to taking indirect inspiration from many wonderful resources compiled by the community, we have directly copied useful language from a handful of existing resources as well throughout this Handbook, particularly the Electronic Frontier Foundation's Surveillance Self Defense Guide, Tactical Tech's Holistic Security Manual, and a range of explainers from the Center for Democracy and Technology and the Freedom of the Press Foundation. You can find specific citations to these resources throughout the sections below, and complete links, author, and license information within Appendix A.

Who are We?

The National Democratic Institute for International Affairs (NDI) is a nonprofit, nonpartisan organization, based in Washington D.C., that works in partnership around the world to strengthen and safeguard democratic institutions, processes, norms and values to secure a better quality of life for all.

NDI believes all people have the right to live in a world that respects their dignity, security, and political rights—and that the digital world is no exception.

Within NDI, the Democracy and Technology team seeks to foster a global digital ecosystem in which democratic values are protected, promoted, and can thrive; governments are more transparent and inclusive; and all citizens are empowered to hold their government accountable. We do this work by supporting a global network of activists committed to digital resilience, and through collaboration with partners on tools and resources like this Handbook. You can learn more about our work on our website, by following us on Twitter, or by reaching out directly to cyberhandbook@ndi.org. We are always happy to hear from you and answer questions about our team and our work on cybersecurity, technology, and democracy.

The House Democracy Partnership (HDP) works with legislatures around the world to promote responsive, effective government and strengthen democratic institutions. Central to our work is peer-to-peer cooperation to build technical expertise in partner legislatures that will enhance accountability, transparency, legislative independence, access to information, and government oversight. HDP currently has partnerships with more than 20 national legislatures around the world. Areas of cooperation with HDP partner parliaments include addressing budgetary issues, ensuring more effective committee operations, enhancing constituent services, providing tools for stronger oversight, strengthening legislative ethics, and improving IT, library and research, and legislative processes and procedures. HDP programs are implemented by the National Democratic Institute (NDI) and the International Republican Institute (IRI) through a cooperative funding agreement with the U.S. Agency for International Development (USAID).

Who Manages Parliamentary Cybersecurity?

An effective and secure parliament requires staff with the skill and proper authority to implement the recommendations included in this Handbook. With that said, those responsible for cybersecurity in parliaments can vary widely, and there is no one "right" model for who should handle cybersecurity. In some cases it may be a dedicated cybersecurity team within your IT unit, and in others a group of different administrative staff and members alike. Regardless, keep in mind that while it is important to have a good team in charge of your parliament's cybersecurity, it is also the responsibility of everyone in and around parliament to follow the policies and procedures necessary to keep parliament safe. Below are a few examples of different staffing models for managing parliamentary cybersecurity:

United States House of Representatives
In the United States House of Representatives, some individual member offices hire a systems administrator who is responsible for managing all of the computer hardware and software systems used by the office – including managing cybersecurity considerations – and trains staff members on best practices. On an institutional level, the House of Representatives' Chief Administrative Officer houses an Information Resources team, which includes a department dedicated to information security.

National Assembly of Zambia
The National Assembly of Zambia counts on its Information and Communications Technology (ICT) Department for a variety of functions, including managing the parliament's software, hardware, and information infrastructure, training members or parliament and staff on technology systems, and securing the parliament's information infrastructure from internal and external cybersecurity threats.

Parliament of Malaysia
The parliament of Malaysia houses its Information Technology division under the parliament's chief administrator, which allows it to serve both houses of parliament. This division includes a specific post for network security, which allows it to ensure that network systems, data centers, and ICT infrastructure are up-to-date and as secure as possible.

Who is this Handbook for?

This Handbook was written with a simple goal in mind: to help your parliament develop an understandable and implementable cybersecurity plan.

As the world increasingly moves online, cybersecurity is not just a buzzword but a critical concept for the success of parliaments, and the security of information (both online and off) is a challenge that requires focus, investment and vigilance.

Your parliament will likely find itself – if it has not already – the target of a cybersecurity attack. This is not intended to be alarmist; it is reality even for parliaments that do not consider themselves to be particular targets.

In an average year, the Center for Strategic and International Studies, which maintains a running list of what they term "Significant Cyber Incidents", catalogs hundreds of serious cyber attacks, many of which target dozens if not hundreds of organizations at once. In addition to such reported attacks, there are likely hundreds of other smaller attacks each year that go undetected or unreported, many aimed at governmental institutions, legislative bodies, and political organizations.

Cyberattacks like these have significant consequences. Whether their aim is to disrupt parliamentary operations, damage your reputation, or even steal information that can lead to psychological or physical harm to your members or staff, such threats need to be taken seriously.

The good thing is that you do not need to become a coder or a technologist to defend yourself and your parliament against common threats. However, you do need to be prepared to invest effort, energy, and time in developing and implementing a strong parliamentary security plan.

If you have never thought about cybersecurity for your parliament, have not had time to focus on it, or know some basics about the topic but think your parliament could enhance its cybersecurity, this Handbook is for you. **Regardless of where you are coming from, this Handbook aims to give your parliament the essential information it needs to put a strong security plan in place - a plan that goes beyond simply putting words on paper and enables you to put best practices into action.**

What is a security plan and why should my parliament have one?

A security plan is the set of written policies, procedures, and instructions your parliament has agreed upon to achieve the level of security you and your team think is appropriate to keep your people, partners, and information safe.

A well-crafted and updated organizational security plan can both keep you safe and make you more effective by providing the peace of mind needed to focus on your parliament's important day-to-day work. Without thinking through a comprehensive plan, it is very easy to be blind to some types of threats, focusing too much on one risk or ignoring cybersecurity until there is a crisis. When you start developing a security plan there are some important questions to ask yourself that form a process called a **risk assessment.** Answering these questions helps your parliament understand the unique threats that you face and allows you to step back and think comprehensively about what you need to protect and from whom you need to protect it. Trained assessors, aided with systems like Internews' SAFETAG auditing framework, can help lead your parliament through such a process. If you can get access to that level of professional expertise it is well worth it, but even if you cannot undergo a full assessment, you should meet with your stakeholders across parliament to thoughtfully consider these key questions:

1 What assets does your parliament have and what do you want to protect?

You can start answering these questions by creating a catalog of all your parliament's assets. Information such as messages, emails, contacts, documents, calendars, and locations are all possible assets. Phones, computers and other devices can be assets. And people, connections, and relationships might be assets too. Make a list of your assets and try to catalog them by their importance to the organization, where you keep them (perhaps multiple digital or physical places), and what prevents others from accessing, damaging, or disrupting them. Keep in mind that not everything is equally important. If some of the parliament's data is a matter of public record, or information you already publish, they are not secrets that you need to protect.

2 Who are your adversaries and what are their capabilities and motivations?

"Adversary" is a term commonly used in organizational security. In simple terms, adversaries are the actors (individuals or groups) that are interested in targeting your parliament, disrupting your work, and gaining access to or destroying your information: the bad guys. Examples of potential adversaries could include financial scammers, adversarial governments, or ideologically or politically motivated hackers. It is important to make a list of your adversaries and think critically about who might want to negatively impact your parliament and staff. While it is easy to envision external actors (like a foreign government or a particular political group) as adversaries, also keep in mind that adversaries can be people that you know, such as disgruntled employees, former staff, and unsupportive family members or partners. Different adversaries pose different threats and have different resources and capabilities to disrupt your operations and gain access to or destroy your information. For example, governments often have lots of money and powerful capabilities including shutting down the internet or using expensive surveillance technology; mobile networks and internet providers likely have access to call records and browsing histories; skilled hackers on public Wi-Fi networks have the capability to intercept poorly secured communications or financial transactions. You can even become your own adversary, for example, by accidentally deleting important files or sending private messages to the wrong person.

The motives of adversaries are likely to differ along with their capacity, interests, and strategies. Are they interested in discrediting your parliament? Perhaps they are intent on silencing your message or disrupting parliament's work? It is important to understand an adversary's motivation because doing so can help your parliament better assess the threats it might pose.

3 What threats does your parliament face? And how likely and high-impact are they?

As you identify possible threats, you are likely to end up with a long list which can be overwhelming. You may feel any efforts would be pointless, or not know where to begin. To help empower your parliament to take productive next steps, it is helpful to analyze each threat based upon two factors: the likelihood that the threat will take place; and the impact if it does.

To measure the likelihood of a threat (perhaps "low, medium or high," based on if a given event is unlikely to take place, could happen, or frequently happens), you can use information you know about your adversaries' capacity and motivation, analysis of past security incidents, other similar parliaments' experiences, and of course the presence of any existing mitigation strategies you have put in place.

To measure the impact of a threat, think about what your world would look like if the threat actually did occur. Ask questions like "How has the threat harmed us as a parliament and as people, physically and mentally?", "How long-lasting is the effect?", "Does this create other harmful situations?", and "How does it hamper our ability to achieve our goals now and in the future?" As you answer these questions, consider if the threat is low, medium, or high impact.

Once you have categorized your threats by likelihood and impact, you can begin to make a more informed plan of action. By focusing on those threats that are most likely to happen AND that will have significant negative impacts, you will be channeling your limited resources in the most efficient and effective way possible.

Your goal is always to mitigate as much risk as possible, but no one – not the most well-resourced government or company on earth – can ever fully eliminate risk. And that is OK: You can do a lot to protect yourself, your colleagues, and your parliament by taking care of the biggest threats.

To help you manage this risk assessment process, consider using a worksheet, like **this one** developed by the Electronic Frontier Foundation. Keep in mind that the information you develop as part of this process (such as a list of your adversaries and the threats they pose) might itself be sensitive, so it is important to keep it secure.

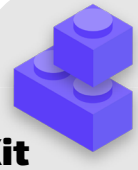
Creating your Parliament's Cybersecurity Plan

While every parliament's security plan will look a little bit different based upon its risk assessment and organizational dynamics, certain core concepts are nearly universal.

This Handbook addresses these essential concepts in a way that will help your parliament build a concrete security plan based upon practical solutions and real-world applications.

This Handbook endeavors to provide options and suggestions that are free or very low cost. Keep in mind that the most significant cost associated with implementing an effective security plan will be the time you and the staff, members, and teams across parliament need to talk about, learn, and implement your new plan. Given the risks your parliament is likely to face, though, this investment will be more than worth it.

In each section, you will find an explanation of a key topic that your parliament and its staff should be aware of - what it is and why it is important. Each topic is paired with essential strategies, approaches, and recommended tools to limit your risk and tips and links to additional resources that can help you implement such recommendations across your parliament.



Security Plan Starter Kit

To help your parliament process the Handbook's lessons and turn them into a real plan, make use of this starter kit. You can either print out the kit or fill it in digitally while you read the Handbook online. As you take notes and begin to update or craft your security plan, be sure to reference the "Security Plan Building Blocks" detailed in each section. No security plan is complete without, at minimum, addressing these essential elements.

Take advantage of other resources that can help you build and implement your plan as well.
Make use of free training resources like Consumer Reports' Security Planner, the Umbrella app from Security First, the Totem Project from Free Press Unlimited and Greenhost, and the Global Cyber Alliance Cybersecurity Toolkit for Mission Based-Organizations, which include resources on many of the best practices mentioned in this Handbook and links to dozens of training tools to help you implement many core basics.

Building a Culture of Security

Security is all about people, and to protect your parliament you need to make sure that everyone involved – including members of parliament (MPs), legislative support staff and research service personnel, and administrative staffers in finance, human resources and IT among many others – takes cybersecurity seriously. Changing culture is hard, but a few simple steps and important conversations can go a long way towards creating an atmosphere that will build the resilience of your staff and parliament in the face of security threats. One of the simplest but most important steps to take to build this parliamentary security culture is to communicate about it within and across your parliament, and for leaders to always model and invest in good behavior.

Building a Culture of Security in Parliaments

In February 2019, Australia suffered a cyberattack that compromised the networks of the Australian national parliament and three leading political parties. The attackers were able to gain access to policy papers and private email correspondence between MPs, their staff, and their constituents. The attack took place just three months before elections were scheduled to take place, highlighting the vulnerability of insecure networks during elections.

In response to this significant and successful attack, the parliament undertook efforts to enhance its cybersecurity preparedness. Such investment included the Joint Committee of Public Accounts and Audits' inquiry into the Commonwealth's cyber resilience. The inquiry built upon findings from audits conducted over several years that found cybersecurity risk mitigation processes to be lacking within parliament and other government agencies. For instance, Australia's National Audit Office highlighted a failure of parliament to focus on long-term strategic objectives and to develop a risk-based approach when it came to cybersecurity. And while the inquiry and audits were not flattering, the parliament's willingness to identify cybersecurity problems and invest in addressing them is an example of creating a culture conducive to effective parliamentary cybersecurity. One that starts with recognizing problems and investing in technical and human solutions, where security is not avoided but rather prioritized. For example, through the recruitment of a "cybersecurity uplift" team and budgetary investment for a "Cybersecurity Response Fund", the parliament (and other government entities) should be better equipped to mitigate future attacks if such resources are properly deployed, sustained, and the focus on cybersecurity as a regular element of parliamentary operations remains. With that said, it is of course better to build this commitment to security within your parliament *before* a significant security breach occurs.

Integrate Security into your Regular Operating Structure

As is described in detail in Tactical Tech's Holistic Security Guide, it is essential to create regular, safe spaces to talk about the different aspects of security.

This way, if staff and members have concerns around security, they will be less anxious about seeming paranoid or wasteful of other people's time. **Scheduling regular conversations about security** also normalizes the frequency of interaction and reflection on matters relating to security, so that the issues are not forgotten, and staff across teams are more likely to bring at least a passive awareness of security to their ongoing work. It does not need to be every week, but make it a recurring reminder. These discussions should not only leave space for topics of technical security, but also issues that impact staff comfort and safety, such as online (and offline) harassment, or issues with using and implementing digital tools within parliamentary offices. Conversations can even include topics like offline information-sharing habits and the ways staff do or do not secure information outside of parliament. After all, it is important to remember that a parliament's security is only as strong as its weakest link. One way to accomplish consistent engagement is by adding security to the agenda of a regular meeting. You can also rotate the responsibility for organizing and facilitating a discussion on security between different staff, which can help develop the idea that security is everyone's responsibility and not just that of a select few or the "IT Team". As you begin to formalize discussion about security, staff will likely feel more comfortable discussing these important issues amongst themselves as well in less formal settings.

It is also important to incorporate security elements into the normal functioning of parliament, such as during member and staff onboarding – and thinking about cutting off access to systems during off-boarding. Security should not be some "extra thing" to worry about, but rather an ***integral part of your strategy and operations.***

Remember that all security plans should be considered living documents, and should be re-evaluated and discussed regularly, especially when your security context changes.

Plan to revisit your strategy and make updates annually, or if there are major changes in strategy, tools, or the threats you face.

Get Organizational Buy-In

Part of a successful security culture is also ensuring buy-in across parliament to your security plan.

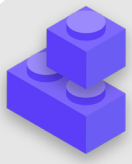
Critically this must include strong, vocal support and guidance from leadership who will, in many cases, be the ones making the final decision to allocate time, resources, and energy towards developing and implementing an effective security plan. If they do not take it seriously, no one else will. To achieve this buy-in, think carefully about when and how to introduce your plan, do so in a clear manner, make sure leadership reinforces the messages, and walk everyone through all the elements and steps of the plan so that there is no mystery or confusion about what you are trying to achieve. Make sure to budget appropriately for cybersecurity across the parliament as well. Although finances might be limited, it is essential to invest appropriately in cybersecurity, otherwise other investments are likely to be put at risk. When talking about security, avoid scare tactics. Sometimes the threats that your parliament and staff face can be scary, but try to focus on sharing facts and creating a calm space for questions and concerns. Making the dangers seem too threatening can cause people to dismiss you as sensationalist or simply give up, thinking nothing they do matters – and nothing could be further from the truth.

Establish a Training Plan

Once you have developed and committed to a plan, think about how you will train all members, staff, and volunteers on these new best practices.

Requiring regular training - and making attendance of training mandatory - can be a helpful tactic. Avoid creating harsh, negative consequences for staff who struggle with security concepts. Keep in mind that certain staff may adapt to and learn about technology differently than others based upon varying levels of familiarity with digital tools and the internet. A fear of failure only further disincentivizes staff from reporting problems or seeking help. However, creating positive accountability and rewards for successful training and adoption of policies can help incentivize improvement across parliament. You may find additional valuable support through local or international digital security training networks and free training resources such as the Umbrella app from Security First, the Totem Project from Free Press Unlimited and Greenhost, and the Global Cyber Alliance Learning Portal.

Consider how your training plan can reach MPs, parliamentary staff, and the parliamentary administration as well. Keep in mind that prominent members often require even more training and attention when it comes to security due to their high profile.Ensure that your training plan and security plan apply to all these different types of individuals and any assets they may have both inside and outside of parliament.



Building a Culture of Security

- **Schedule regular conversations and trainings about security and your security plan.**
- **Get everyone involved - distribute responsibility for implementing your security plan across the entire parliament.**
- **Ensure leadership models good security behavior and a commitment to your plan.**
- **Avoid fear tactics or punishment - reward improvement and create a comfortable space for staff to report problems and seek help.**
- **Update your security plan annually or after major changes in parliamentary staffing, structure, or operating environment.**

A Strong Foundation: Securing Accounts and Devices

Why the focus on accounts and devices? Because they form the foundation of everything that your parliament does digitally.

You almost certainly access sensitive information, communicate internally and externally, and save private information on them. Just consider members' participation in plenary sessions, voting (including virtual), the legislative drafting processes, and communicating with staff members and the general public. Without secure accounts and devices, these crucial parliamentary operations and more can be put at risk. For example, if hackers are watching your keystrokes or listening to your microphone, private conversations with colleagues will be captured no matter how secure your messaging apps are. Or, if an adversary gains access to your parliament's social media accounts, they could easily harm your reputation and credibility, undermining trust with the public. Therefore, it is essential as a parliament to ensure that everyone is taking some simple but effective steps to keep their devices and accounts secure. It is important to note that these recommendations include personal accounts and devices as well, as those are often easy targets for adversaries. Hackers will gladly go after the easiest target and break into a personal account or home computer if your members and staff are using them to communicate and access important information.

Secure Accounts and Parliaments

The widely publicized SolarWinds hack revealed in late 2020, which compromised over 250 organizations, including most United States government departments, technology vendors like Microsoft and Cisco, and NGOs, was partly a result of hackers guessing poor passwords that were used on important administrator accounts. Overall, about 80 percent of all hacking-related breaches occur because of weak or reused passwords.

With the increasing prevalence of password breaches like this and easier access for all kinds of adversaries to sophisticated password hacking tools, password best practices and two-factor authentication are security must-haves for all organizations, including parliaments. No incident more clearly illustrates this than the 2017 attack against the British parliament's email system. In this incident, poor password practices from a small but meaningful number of MPs led to exposed email accounts and conversations, thousands of leaked credentials, and tremendous disruption to parliamentary operations. According to the British parliament's press office, the breached accounts were "compromised as a result of weak passwords that did not conform to guidance issued by the Parliamentary Digital Service."

Secure Accounts: Passwords and Two-Factor Authentication

In today's world, it is likely that your parliament and its staff have dozens if not hundreds of accounts that, if breached, could expose sensitive information or even get at-risk individuals hurt.

Think about the different accounts that individual staff and parliament as a whole may have: email, chat apps, social media, online banking, cloud data storage, as well as clothing stores, the local restaurants, newspapers, and many other websites or apps that you log into. Good security in today's world requires a diligent approach to protecting all of these accounts from attacks. That starts with ensuring good password hygiene and the use of two-factor authentication by everyone.

WHAT MAKES A GOOD PASSWORD?

There are three keys to a good, strong password: length, randomness, and uniqueness.

LENGTH	The longer the password is, the harder it is for an adversary to guess it. Most password hacks are done by computer programs these days, and it does not take those nefarious programs long to crack a short password. As a result, it is essential that your passwords are at minimum 16 characters, or at least five words, and preferably longer.
RANDOMNESS	Even if a password is long, it is not very good if it is something that an adversary can easily guess about you. Avoid including information like your birthday, hometown, favorite activities, or other facts that someone could find out about you from a quick internet search.
UNIQUENESS	Perhaps the most common password "worst practice" is using the same password for multiple sites. Repeating passwords is a big problem because it means that when just one of those accounts is compromised, any other accounts using that same password are vulnerable too. If you use the same passphrase on multiple sites, it can greatly increase the impact of one mistake or data breach. While you may not care about your password for the local library, if it is hacked and you use the same password on a more sensitive account, important information could be stolen.

One easy way to achieve these goals of length, randomness, and uniqueness is picking three or four common but random words. For example, your password could be "flower lamp green bear" which is easy to remember but hard to guess. You can take a look at this website from Better Buys to see an estimate of just how quickly bad passwords can be cracked.

USE A PASSWORD MANAGER TO HELP

So you know it is important for everyone in parliament to use a long, random, and different password for each of their personal and parliamentary accounts, but how do you actually do that? Memorizing a good password for dozens (if not hundreds) of accounts is impossible, so everyone has to cheat. The wrong way to do it is to reuse passwords. Luckily, we can turn to digital password managers to make our lives much easier (and our password practices much safer) instead. These applications, many of which can be accessed via computer or mobile device, can create, store, and manage passwords for you and your entire organization. Adopting a secure password manager means that you will only ever have to remember one very strong, long password called the primary password (historically referred to as a "master" password), while being able to get the security benefits of using good, unique passwords across all of your accounts. You will use this primary password (and ideally a second factor of authentication (2FA), which will be discussed in the next section) to open your password manager and unlock access to all your other passwords. Password managers can also be shared across multiple accounts to facilitate secure password sharing throughout parliament.

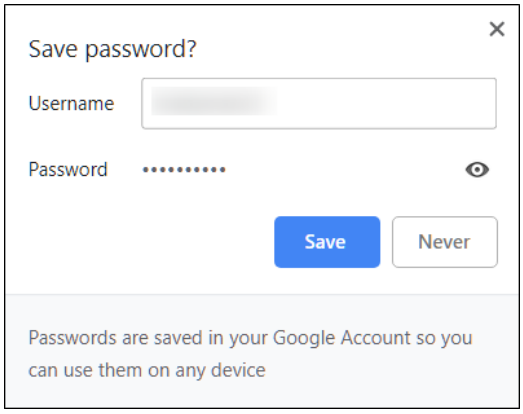
Why do we need to use something new? Can we not just write them down on paper or in a spreadsheet on the computer?

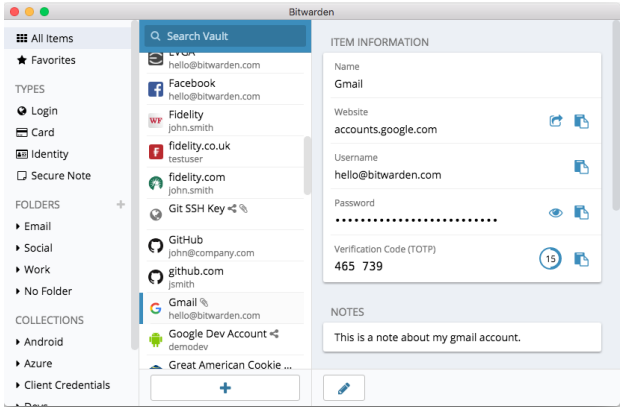
Unfortunately, there are many common approaches to managing passwords that are not secure. Storing passwords on sheets of paper (unless you keep them locked away in a safe) can expose them to physical theft, prying eyes, and easy loss and damage. Saving passwords on a document on your computer makes it much easier for a hacker to gain access – or for someone who steals your computer to not only have your device but also access to all of your accounts. Using a good password manager is just as easy as that document, but far more secure.

Why should we trust a password manager?

Quality password managers go to extraordinary lengths (and employ excellent security teams) to keep their systems secure. Good password management apps (a few are recommended below) are also set up so that they do not have the ability to "unlock" your accounts. This means that in most cases, even if they were hacked or legally compelled to hand over information, they would not be able to lose or give up your passwords. It is also important to remember that it is infinitely more likely that an adversary guesses one of your weak or repeated passwords, or finds one in a public data breach, than that a good password manager would have its security systems broken. It is important to be skeptical, and you definitely should not blindly trust all software and applications, but reputable password managers have all the right incentives to do the right thing.

Instead of using your browser (such as Chrome, shown at left) to save your passwords, use a dedicated password manager (like Bitwarden, shown at right). Password managers have features that make life both more secure and convenient for your parliament.





What about storing passwords in the browser?

Saving passwords in your browser is not the same as using a secure password manager. In short, you should not use Chrome, Firefox, Safari or any other browser as your password manager. Although it is definitely an improvement over writing them on paper or saving them in a spreadsheet, the basic password-saving features of your web browser leave something to be desired from a security perspective. These shortcomings also rob you of much of the convenience that a good password manager brings. Losing this convenience makes it more likely that people across parliament will continue poor password creation and sharing practices.

For example, unlike dedicated password managers, browsers' built-in "save this password" or "remember this password" features do not provide simple mobile compatibility, cross-browser functionality, and strong password generation and auditing tools. These features are a big part of what makes a dedicated password manager so useful and beneficial to your parliament's security. Password managers also include organization-specific features (such as password sharing) that provide not just individual security value, but value to your parliament as a whole. If you have been saving passwords with your browser (intentionally or unintentionally), take a moment to remove them.

What password manager should we use?

Many good password management tools exist that can be set-up in less than 30 minutes. If you are looking for a trusted online option for your parliament that people can access from multiple devices at any time, 1Password (starts at $2.99 USD per user per month) or the free, open-source Bitwarden are both well supported and recommended. An online option like Bitwarden can be great for both security and convenience. Bitwarden, for example, will help you create strong unique passwords and access passwords from multiple devices through browser extensions and

a mobile app. With the paid version ($10 USD for a full year) Bitwarden also provides reports on reused, weak, and possibly breached passwords to help you stay on top of things. Once you set up your primary password (referred to as a master password), you should also turn on two-factor authentication to keep your password manager's vault as secure as possible.

It is essential to **practice good security when using your password manager too.** For instance, if you use your password manager's browser extension or log in to Bitwarden (or any other password manager) on a device, remember to log out after use if you are sharing that device or believe that you might be at heightened risk of physical device theft. This includes logging out from your password manager if you leave a computer or mobile device unattended. If sharing passwords across teams or parliament as a whole, also be sure to revoke access to passwords (and change the passwords themselves) when people leave.

You do not want a former staffer to keep access to your parliament's Facebook password, for example.

What if someone forgets their primary password?

It is essential to remember your primary password. Good password management systems like the ones recommended above will not remember your primary password for you or allow you to reset it directly via email the way you might be able to for websites. This is a good security feature, but also makes it essential to commit your primary password to memory when you first set up your password manager. To help with this, consider setting up a daily reminder to recall your primary password when you first create a password manager account.

Using a Password Manager for Your Parliament

You can strengthen your parliament's password practices and ensure all individual staff have access to (and use) a password manager by implementing one across the entire organization. Instead of having each individual staff member set up their own, consider investing in a "team" or "business" plan. For example, Bitwarden's "teams organization" plan costs $3 per user per month. With it (or other team plans from password managers like 1Password), you have the ability to manage all shared passwords across the "organization". The features of a parliament or team-wide password manager not only provide greater security but also convenience for staff. You can securely share credentials within the password manager itself to different user accounts. And Bitwarden, for example, also provides a convenient end-to-end encrypted text and file sharing feature called "Bitwarden Send" within its team plan. Both of these features give your parliament more control over who can see and share which passwords, and provides a more secure option for sharing credentials for team-wide or group accounts. If you do set up a parliament-wide password manager, be sure that someone is specifically in charge of removing staff accounts and changing any shared passwords when someone leaves the team.

WHAT IS TWO-FACTOR AUTHENTICATION?

However good your password hygiene, it is all too common for hackers to get around passwords. Keeping your accounts secure from some common threat actors in today's world requires another layer of protection. That is where multi-factor or two-factor authentication comes into play – referred to as MFA or 2FA.

There are many great guides and resources explaining two-factor authentication, including Martin Shelton's Two-Factor Authentication for Beginners article and the Center for Democracy & Technology's Election Cybersecurity 101 Field Guide. This section borrows heavily from both of those resources to help explain why 2FA is so important to implement across parliament.

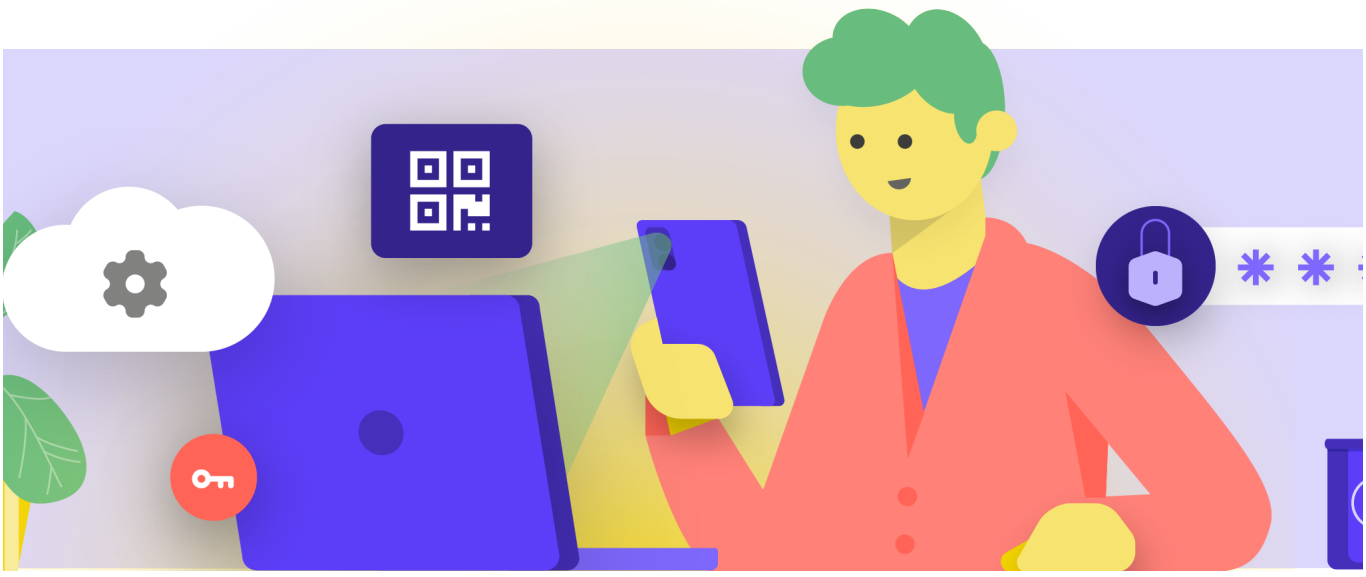
In short, 2FA strengthens account security by requiring a second piece of information – something more than just a password – to gain access. The second piece of information is usually something that you have, like a code from an app on your phone or a physical token or key.
This second piece of information acts as a second layer of defense. If a hacker steals your password or gains access to it via a dump of passwords from a major data breach, effective 2FA can keep them from accessing your account (and therefore away from private and sensitive information). Ensuring that everyone in parliament puts 2FA in place on their accounts is critically important.

HOW CAN WE SET UP 2FA?

There are three common methods for 2FA: security keys, authentication apps, and one-time SMS codes.

Security Keys

Security keys are the best option, in part because they are almost completely phishing-proof. These "keys" are hardware tokens (think mini USB drives) that can attach to your keychain (or stay in your computer) for easy access and safekeeping. When it is time to use the key to unlock a given account, you simply insert it into your device and physically tap it when prompted during login. There are a wide range of models that you can purchase online ($20-50 USD), including highly regarded YubiKeys. The New York Times' Wirecutter has a helpful guide with some recommendations for which keys to purchase. Keep in mind that the same security key can be used for as many accounts as you would like.



Authentication Apps

The **second-best option for 2FA is authentication apps.** These services allow you to receive a temporary two-factor login code through a mobile app or push notification on your smartphone. Some popular and trusted options include Google Authenticator, Authy, and Duo Mobile. Authenticator apps are also great because they work when you do not have access to your cellular network and are free to use for individuals. However, authenticator apps are more susceptible to phishing than security keys because users can be tricked into entering security codes from an authentication app into a fake website. Take care to only enter login codes on legitimate websites. And do not "accept" login push notifications unless you are sure that you are the one who made the login request. It is also essential when using an authenticator app to be prepared with backup codes (discussed below) in case your phone is lost or stolen.

Codes Via SMS

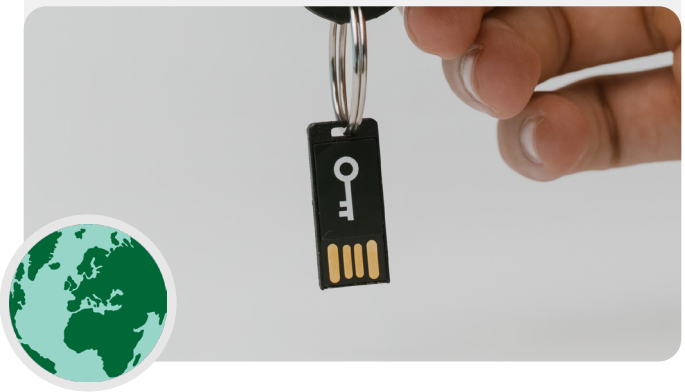
The least secure but unfortunately still most common form of 2FA are codes sent via SMS. Because SMS can be intercepted and phone numbers can be spoofed or hacked via your mobile carrier, SMS leaves a lot to be desired as a method for requesting 2FA codes. It is better than only using a password, but authenticator apps or a physical security key are recommended when at all possible. A determined adversary can get access to SMS 2FA codes, usually just by calling the phone company and swapping your SIM card. When you are ready to start enabling 2FA for all of your parliament's various accounts, make use of this website (https://2fa.directory/) to quickly look up information and instructions for specific services (like Gmail, Office 365, Facebook, Twitter, etc.) and to see which services allow for which types of 2FA.

2FA and Parliaments

According to reports in the year 2020, hackers infiltrated Norway's parliamentary email system, compromising email accounts belonging to several parliamentary officials and even downloading some information from parliamentary systems. While full details of the hack were not released to the public, Norway did attribute the intrusion to APT28, a hacking group affiliated with Russia's security services. While highly sophisticated, APT28 and other hackers often use less complex tactics such as "brute-force attacks" (wherein the attacker uses tools to try many passwords with the hope of eventually guessing the right one) to gain account access. This tactic allows hackers to guess even solid passwords - such as was believed to be the case in Norway. The good news? The types of attacks are much less likely to succeed with proper key or app-based two factor authentication in place!

Security Keys in the Real World

By providing physical security keys for two factor authentication to all 85,000+ of its employees, Google (a very high risk, highly targeted organization) effectively eliminated any successful phishing attacks against the organization. This case shows just how effective security keys can be for even the most at-risk organizations.



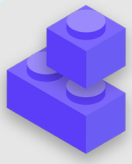
WHAT IF SOMEONE LOSES A 2FA DEVICE?

If using a security key, treat it the same way you would treat a key for your house or apartment, if you have one. In short, do not lose it. Just like your house keys though, it is always a good idea to have a backup key registered to your account that stays locked away in a safe place (like a safe at home or a safe deposit box) just in case of loss or theft. Alternatively you should create backup codes for accounts that allow it. You should keep these codes saved in a very secure place, like your password manager or a physical safe. Such backup codes can be generated within most sites' 2FA settings (the same place where you enable 2FA in the first place), and can act as a backup key in case of emergency. The most common 2FA mishap occurs when people replace or lose phones which they use for authentication apps. If using Google Authenticator, you are out of luck if your phone is stolen, unless you save the backup codes that are generated at the time you connect an account to Google Authenticator. Therefore, if you are using Google Authenticator as a 2FA app, be sure to save the backup codes for all accounts that you connect in a secure place. If using Authy or Duo, both apps have built-in backup features with strong security settings that you can enable. If you choose either of those apps, you can configure those backup options in case of device breakage, loss, or theft. See Authy's instructions here, and Duo's here. Be sure that everyone is aware of these steps as they start to enable 2FA across all of their accounts.

Enforcing 2FA Across Your Parliament

If your parliament provides email accounts to all staff through Google Workspace (formerly known as GSuite) or Microsoft 365 using your own domain (for example, @ndi.org), you can enforce 2FA and strong security settings for all accounts. Such enforcement not only helps protect these accounts, but it also acts as a way to introduce and normalize 2FA to your members and staff so that they are more comfortable with adopting it for personal accounts as well. As a Google Workspace administrator, you can follow these instructions to enforce 2FA for your domain. You can do something similar in Microsoft 365 following these steps as a domain admin.

Consider also enrolling your parliament's accounts in the Advanced Protection Program (Google) or AccountGuard (Microsoft) to enforce additional security controls and require physical security keys for two-factor authentication.



Secure Accounts

- **Require strong passwords for all parliamentary accounts; encourage the same for member, staff and volunteer's personal accounts.**
- **Implement a trusted password manager for the parliament (and encourage use in staff's personal lives as well).**
  - Require a strong primary password and 2FA for all password manager accounts.
  - Remind everyone to log out of a password manager on shared devices or when at heightened risk of device theft or confiscation.
- **Change shared passwords when staff and members leave parliament.**
- **Only share passwords securely, such as through your parliament's password manager or end-to-end encrypted apps.**
- **Require 2FA on all parliament accounts, and encourage staff to set up 2FA on all personal accounts as well.**
  - If possible, provide physical security keys to all members and staff.
  - If security keys are not in your budget, encourage the use of authenticator apps instead of SMS or phone calls for 2FA.
- **Hold regular training to ensure everyone is aware of password and 2FA best practices, including what makes a strong password and the importance of never reusing passwords, only accepting legitimate 2FA requests, and generating backup 2FA codes.**

Secure Devices

In addition to accounts, it is essential to keep all devices – computers, phones, USBs, external hard drives, etc. – well protected.

Such protection starts with being careful about what type of devices your parliament and staff purchase and use. Any vendors or manufacturers that you select should have a demonstrated track record of adhering to global standards regarding the secure development of hardware devices (like phones and computers). Any devices you procure should be manufactured by trusted companies that do not have an incentive to hand over data and information to a potential adversary. It is important to note that the Chinese government requires Chinese companies to provide data to the central government. Therefore, despite the ubiquitous and inexpensive presence of smartphones like Huawei or ZTE, they should be avoided. Although the cost of cheap hardware can be very attractive, the potential security risks for parliaments should steer you towards other device and equipment options.

Your adversaries can compromise the security of your devices - and everything you do from those devices - by either gaining physical access or "remote" access to your device.

Device Security and Parliaments

Some of the world's most advanced malware has been developed and deployed across the globe to target MPs, other government officials, and their staff. In India, for example, a consortium of journalists revealed that multiple MPs and government ministers were targeted by the Pegasus spyware, a type of malicious software that captured headlines in 2020. Pegasus is infamous for its ability to infect mobile devices and give the perpetrator the ability to record audio, intercept keystrokes and messages, and in effect put the victim under full surveillance. without requiring the victim's interaction. However, the vast majority of spyware succeeds in compromising its victims.

PHYSICAL DEVICE ACCESS THROUGH LOSS OR THEFT

To prevent physical compromise, it is essential to keep your devices physically secure. In short, do not make it easy for an adversary to steal or even temporarily take your device from you. Keep devices locked away if left at home or in an office. Or if you think it is safer, keep them on your person. This of course means that part of device security is the physical security of your workspaces (whether in an office setting or at home). You will need to install strong locks, security cameras, or other monitoring systems. Remind staff to treat devices the same way they would treat a large stack of cash - do not leave them lying around unattended or unprotected.

What if a device is stolen?

To limit the impact if someone does manage to steal a device – or even if they just gain access to it for a short period of time – be sure to **mandate the use of strong passwords or passcodes on everyone's computers and phones.** The same password tips from the Passwords section of this Handbook apply to a good password for a computer or laptop. When it comes to locking your phone, use codes that are at least six to eight digits, and avoid using "swipe patterns" to unlock the screen. For additional tips on screen locks, check out Tactical Tech's Data Detox Kit. Using good device passwords makes it much harder for an adversary to quickly access information on your device in the case of theft or confiscation. Be sure any devices issued by parliament are also enrolled in a **mobile device or endpoint management system.** While not inexpensive, these systems allow your parliament to enforce security policies across all devices and locate one, and wipe its potentially sensitive contents, should it be stolen, lost, or confiscated. While many different solutions for mobile device management exist, a few trusted options that work across platforms (iPhones, Android, Mac, and Windows) include Hexnode, Cisco's Meraki Systems Manager, IBMs MDM, and the Google Workspace built-in Mobile Device Management feature. If cost is a limiting factor, at the very least encourage members and staff to use built-in "Find my Device" features on their parliamentary-issued and personal smartphones, such as iPhone's Find My iPhone and Android's Find My Device.

What about device encryption?

It is important to use encryption, scrambling data so that it is unreadable and unusable, on all devices, especially computers and smartphones. You should set up all devices across parliament with something called **full-disk encryption** if possible. Full-disk encryption means that the entirety of a device is encrypted so that an adversary, if they were to physically steal it, would be unable to extract a device's contents without knowing the password or key you used to encrypt it. Many modern smartphones and computers offer full-disk encryption. Apple devices like iPhones and iPads, quite conveniently, turn on full-disk encryption when you set a normal device passcode. Apple computers using macOS provide a feature called FileVault that you can turn on for full-disk encryption. Windows computers running pro, enterprise, or education licenses offer a feature called BitLocker that you can turn on for full-disk encryption. You can turn on BitLocker by following these instructions from Microsoft, which may have to first be enabled by your organization's administrator. If staff only have a home license for their Windows computers, BitLocker is not available. However, they can still turn on full-disk encryption by going to 'Update & Security' > 'Device encryption' under the Windows OS settings.

Android devices, as of version 9.0 and later, ship with file-based encryption turned on by default. Android's file-based encryption operates differently from full-disk encryption but still provides strong security. If you are using a relatively new Android phone and have set a passcode, file-based encryption should be enabled. However, it is a good idea to check your settings just to make sure, especially if your phone is more than a couple of years old. To check, go to Settings > Security on your Android device. Within the security settings, you should see a subsection for "encryption" or "encryption and credentials" which will indicate if your phone is encrypted and, if not, allow you to turn encryption on.

For computers (whether Windows or Mac), it is particularly important to store any encryption keys (referred to as recovery keys) in a safe place. These "recovery keys" are in most cases essentially long passwords or passphrases. In case you forget your normal device password or something unexpected happens (such as device failure), recovery keys are the only way to recover your encrypted data and, if necessary, move it to a new device. Therefore, when turning on full-disk encryption, be sure to save these keys or passwords in a safe place, like a secured cloud account or your parliament's password manager.

REMOTE DEVICE ACCESS – ALSO KNOWN AS HACKING

In addition to keeping devices physically secure, it is important to keep them free from malware. Tactical Tech's Security-in-a-Box gives a helpful description of what malware is and why it is important to avoid, which is adapted slightly in the rest of this section.

Understanding and avoiding malware

There are many ways to classify malware (which is a term meaning malicious software). Viruses, spyware, worms, trojans, rootkits, ransomware and cryptojackers are all types of malware. Some types of malware spread over the internet through email, text messages, malicious web pages, and other means. Some spread through devices like USB memory sticks that are used to exchange and steal data. And, while some malware requires an unsuspecting target to make a mistake, others can silently infect vulnerable systems without you doing anything wrong at all.

In addition to general malware (which is released widely and aimed at the general public), targeted malware is typically used to interfere with or spy on a particular individual, organization, or network. Regular criminals use these techniques, but so do military and intelligence services, terrorists, online harassers, abusive spouses, and shady political actors.

Whatever they are called, however they are distributed, malware can ruin computers, steal and destroy data, disrupt parliamentary operations, invade privacy, and put users at risk. In short, malware is really dangerous. However, there are some simple steps that your parliament can take to protect itself against this common threat.

Will an anti-malware tool protect us?

Anti-malware tools are unfortunately not a complete solution. However, it is a very good idea to use some basic, free tools as a baseline. Malware changes so quickly, with new risks in the real world so frequently, that relying on any such tool cannot be your only defense.

If you are using Windows, you should have a look at the built-in Windows Defender. Macs and Linux computers do not come with built-in anti-malware software, nor do Android and iOS devices. You can install a reputable, free-to-use tool like Bitdefender or Malwarebytes for those devices (and Windows computers as well). **But do not rely on that as your only line of defense** as they will certainly miss some of the most targeted, dangerous new attacks.

Additionally, be very careful to only download reputable anti-malware or anti-virus tools from legitimate sources (such as the websites linked above). Unfortunately, many fake or compromised versions of anti-malware tools exist that do much more harm than good.

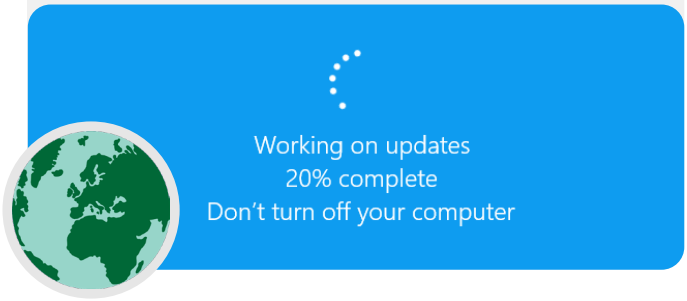
To the extent that you do use Bitdefender or another anti-malware tool across your parliament, be sure not to run two of them at the same time. Many of them will identify the behavior of another anti-malware program as suspicious and stop it from running, leaving both malfunctioning. Bitdefender or other reputable anti-malware programs can be updated for free, and the built-in Windows Defender receives updates along with your computer. Ensure that your anti-malware software updates itself regularly (some trial versions of commercial software that ship with a computer will be disabled after the trial period expires, leaving it more dangerous than helpful.) New malware is written and distributed every day, and your computer will quickly become even more vulnerable if you do not keep up with new malware definitions and anti-malware techniques. If possible, you should configure your software to install updates automatically. If your anti-malware tool has an optional "always on" feature, you should enable it, and consider occasionally scanning all of the files on your computer.

Keep devices up to date

Updates are essential. Use the latest version of whatever operating system runs on a device (Windows, Mac, Android, iOS, etc), and keep that operating system up to date. Keep other software, browser, and any browser plugins up to date as well. Install updates as soon as they become available, ideally by turning on automatic updates. The more up to date a device's operating system, the less vulnerabilities you have. Think of updates kind of like putting a band-aid on an open cut: it seals up a vulnerability and greatly reduces the chance that you will get infected. Also uninstall software that you no longer use. Outdated software often has security issues, and you may have installed a tool that is no longer being updated by the developer, leaving it more vulnerable to hackers.

Malware in the Real World: Updates Are Essential

In 2017, the WannaCry ransomware attacks infected millions of devices around the world, shutting down hospitals, government entities, large and small organizations and businesses in dozens of countries. Why was the attack so effective? Because of out of date, "unpatched" Windows operating systems, many of which were initially pirated. Much of the damage – human and financial – could have been avoided with better automated updating practices and the use of legitimate operating systems.



Be careful about USBs

Be cautious when opening files that are sent to you as attachments, through download links, or by any other means. Also **think twice before inserting removable media like USB sticks,** flash memory cards, DVDs and CDs into your computer, as they can be a vector for malware. USBs that have been shared for a while are very likely to have viruses on them. For alternative options to share files securely across your parliament, take a look at the File Sharing section of the Handbook.

Be cautious as well about what other devices you connect to through Bluetooth. It is fine to sync up your phone or computer to a known and trusted Bluetooth speaker to play your favorite music, but be careful about linking to or accepting requests from any devices that you do not recognize. Only allow connections to trusted devices and remember to turn off Bluetooth when it is not in use.

Be smart while browsing

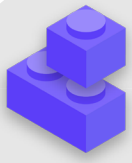
Never accept and run applications that come from websites you do not know and trust. Rather than accepting an "update" offered in a pop-up browser window, for example, check for updates on the relevant application's official website. As discussed in the Phishing section of the Handbook, it is essential to stay alert when browsing websites. Check the destination of a link (by hovering over it) before you click, and glance at the website address after you follow a link and make sure it looks appropriate before entering sensitive information like your password. Do not click through error messages or warnings, and watch for browser windows that appear automatically and read them carefully instead of just clicking Yes or OK.

Malware in the Real World: Malicious Mobile Apps

Hackers in multiple countries have been using fake applications in the Google Play store to distribute malware for years. One particular case targeted at users in Vietnam came to light in April 2020. This spying campaign used fake applications, which supposedly helped users find nearby pubs or look up information about local churches. Once installed by unwitting Android users, the malicious applications collected call logs, location data, and information about contacts and text messages. This is just one of many reasons to be careful about what apps you download to your devices.

What about smartphones?

As with computers, keep your phone's operating system and applications up to date, and turn on automatic updates. Install only from official or trusted sources like Google's Play Store and Apple's App Store (or F-droid, a free, open-source app store for Android). Apps can have malware inserted into them and still appear to work normally, so you will not always know if one is malicious. Be sure that you are downloading the legitimate version of an app as well. Especially on Androids, "fake" versions of popular applications exist. So be sure an app is created by the proper company or developer, has good reviews, and has the expected number of downloads (for example, a fake version of WhatsApp might only have a few thousand downloads, but the real version has over five billion). Pay attention to the permissions that your apps request. If they seem excessive (like a calculator requiring access to your camera or Angry Birds asking for access to your location, for example) deny the request or uninstall the app. Uninstalling apps that you no longer use can also help protect your smartphone or tablet. Developers sometimes sell ownership of their apps to other people. These new owners may try to make money by adding malicious code.



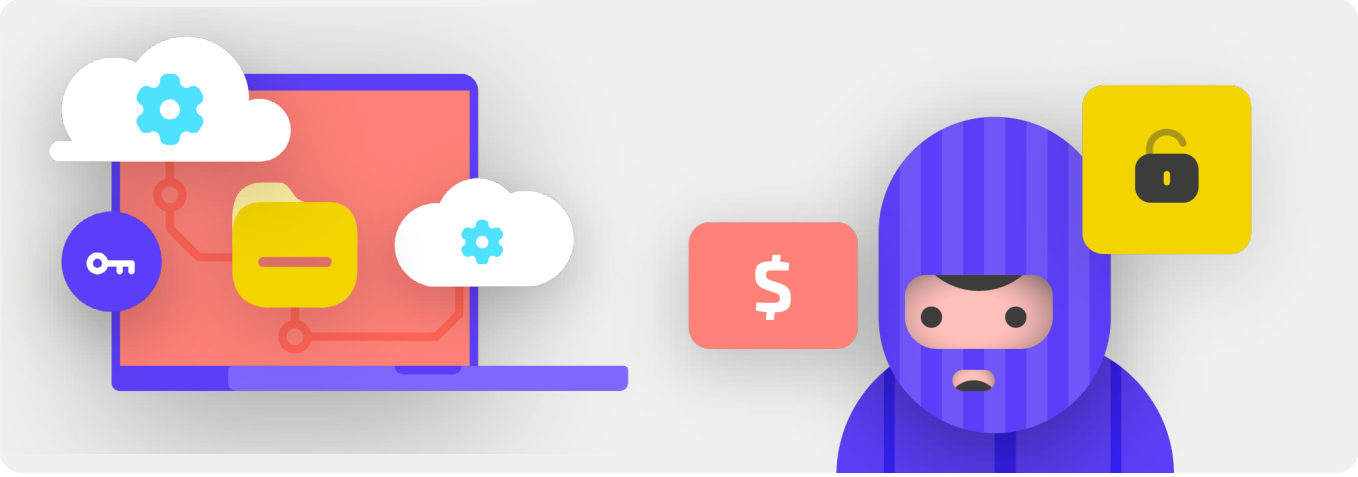
Keeping Devices Secure

- **Train member and staff on the risks of malware and the best practices to avoid it.**
  - Provide policies about connecting external devices, clicking on links, downloading files and apps, and checking software and app permissions.
- **Mandate that devices, software, and applications are kept fully updated.**
  - Turn on automatic updates where possible.
- **Enroll all parliamentary devices in a mobile device or endpoint management system.**
- **Ensure all devices are using licensed software.**
- **Require password protection of all parliamentary devices, including personal mobile devices which are used for parliament-related communications.**
- **Enable full-disk encryption on devices.**
- **Frequently remind members and staff to keep their devices physically secure - and manage your office security with appropriate locks and ways to secure computers.**
- **Do not share files using USBs or plug USBs into your computers.**
  - Use alternative secure file sharing options instead.

Phishing: A Common Threat to Devices and Accounts

Phishing is the most common and effective attack on organizations, parliaments included, around the world. The technique is used by the most sophisticated nation-state militaries as well as petty fraudsters.

Phishing, put simply, is where an adversary attempts to trick you into sharing information that could be used against you or your organization. Phishing can happen via emails, text messages/SMS (often referred to as SMS phishing or "smishing"), messaging apps like WhatsApp, social media messages or posts, or phone calls (often referred to as voice phishing or "vishing"). The phishing messages may try to get you to type sensitive information (like passwords) into a fake website in order to gain access to an account, ask you to share private information (like a credit card number) via voice or text, or convince you to download malware (malicious software) that can infect your device. For a non-technical example, every day millions of people get fake automated phone calls telling them that their bank account was compromised or that their identity has been stolen - all of which are designed to trick the unaware into sharing sensitive information.



HOW CAN WE IDENTIFY PHISHING?

Phishing can sound sinister and impossible to catch, but there are some simple steps that everyone in parliament can take to protect against the majority of attacks. The following phishing defense tips are modified and extended from the in-depth phishing guide developed by the Freedom of the Press Foundation, and should be shared with everyone in and around parliament and integrated into your security plan:

Sometimes, the "from" field is lying to you

Be aware that the "from" field in your emails can be faked or forged to trick you. It is common for phishers to set up an email address that looks a lot like a legitimate one that you are familiar with, misspelled just a bit to trick you. For example, you may receive an email from someone with the address "john@gooogle.com" as opposed to "john@google.com". Notice the extra Os in google. You may also know someone with an email address "john@gmail.com", but receive a phishing email from an impersonator who set up "johm@gmail.com" - the only difference being a subtle change of letters at the end. Always be sure to double-check that you know the sending address of an email before proceeding. A similar concept applies to phishing via text, calls, or messaging apps. If you get a message from an unknown number, think twice before responding to or interacting with the message.

Phishing and Parliaments

Thu 4/8/2021 8:48 AM

<[redacted]@aop.gov.af>

Kindlty mention this email Most Urgent.

To [redacted]@nsc.gov.af

Message | NSC Press conference.rar (38 KB)

Yesterday I called your office and no one answered it. We have received your file and modified it. There is an error in the third line of the second page. Please confirm whether the error exists.
File Pass: nsc2021
Press conference by 5:00PM.

Regards | [redacted]

Press office | Spokesman
Presidential Palace (ARG) | Islamic Republic of Afghanistan
Mobile: [redacted] | ocs.gov.af
Mail: [redacted]

Sophisticated, personalized phishing attacks target parliaments and other government actors around the world regularly.

Federal and local parliamentary officials in Germany were targeted by phishing emails in the run-up to elections in the fall of 2021. Just a few months prior in Afghanistan, a hacking group **used phishing techniques to successfully infiltrate** the former National Security Council by taking on the identity of former Afghan President Ashraf Ghani's press spokesman. The hackers sent phishing emails (shown above) that asked victims to open an attached file that the "spokesman" claimed contained an error. When the victims downloaded and opened the file to "confirm the error," the malicious attachment deployed malware that granted the hackers sustained access to the computers. Such access enabled the hackers to upload and download files, run commands on the devices at will, and steal highly sensitive government data.

Beware of attachments

Attachments can carry malware and viruses, and commonly accompany phishing emails. **The best way to avoid malware from attachments is to never download them.** As a rule, do not open any attachments immediately, especially if they come from people you do not know. If possible, ask the person that sent you the document to copy-paste the text in an email or to share the document via a service like Google Drive or Microsoft OneDrive, which have built-in virus scanning of most documents uploaded to their platforms. Build an organizational culture where attachments are discouraged.

If you absolutely have to open the attachment, it should only be opened in a safe environment (see the Advanced section below) where potential malware cannot be deployed to your device.

If you use Gmail and receive an attachment in an email, instead of downloading it and opening it on your computer, simply click on the attached file and read it in "preview" within your browser. This step allows you to view the text and contents of a file without downloading it or allowing it to load possible malware onto your computer. This works well for word documents, PDFs, and even slideshow presentations. If you need to edit the document, consider opening the file in a cloud program like Google Drive and converting the file to a Google Doc or Google Slides.

If you use Outlook, you can similarly preview attachments without downloading them from the Outlook web client. If you need to edit the attachment, consider opening it in OneDrive if that's available to you. If you use Yahoo Mail, the same concept applies. Do not download attachments, but rather preview them from within the web browser.

Regardless of what tools you have at your disposal, the best approach is simply to never download attachments that you do not know or trust, and regardless of how important an attachment might seem, never open something with a file type you do not recognize or have no intention of ever using.

Phishing Defense for Your Parliament

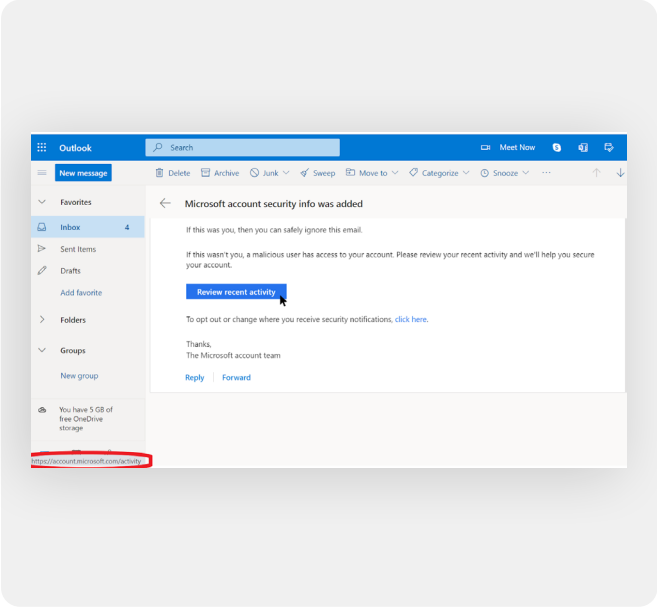
If your parliament uses enterprise Microsoft 365 for email and other applications, your domain administrator should configure the Safe Attachments policy to protect against dangerous attachments. If using enterprise Google Workspace (formerly known as GSuite), there is a similarly effective option that your administrator should configure called Google Security Sandbox. More advanced individual users can consider setting up sophisticated sandbox programs, such as Dangerzone or, for those with the Pro or Enterprise version of Windows 10, Windows Sandbox. Another advanced option to consider implementing across parliament is a secure domain name system (DNS) filtering service.

Parliaments can use this technology to block staff from accidentally accessing or interacting with malicious content, providing an additional layer of protection against phishing. New services like Cloudflare's Gateway provide such capabilities to organizations without requiring large sums of money. Additional free tools, including Quad9 from the Global Cyber Alliance Toolkit, will help block you from accessing known sites that have viruses or other malware and can be implemented in less than five minutes.

Click with caution

Be skeptical of links in emails or other text messages. Links can be disguised to download malicious files or take you to fake sites that might ask you to provide passwords or other sensitive information. When on a computer, there is a simple trick for making sure a link in an email or message will send you to where it is supposed to: Use your mouse to hover over any link before clicking on it, and look in the bottom of your browser window to see what the actual URL is (see image below).

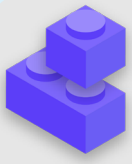
It is more difficult to check links in an email on a mobile device without accidentally clicking on them - so be careful. You can check the destination of a link on most smartphones by long-pressing (holding down) on a link until the full URL pops up.
In phishing via SMS and messaging apps, shortened links are a very common practice used to disguise the destination of a URL. If you see a short link (e.g., bit.ly or tinyurl.com) instead of the full URL, do not click on it. If the link is important, copy it into a URL expander, such as https://www.expandurl.net/, to see the actual destination of a shortened URL. Furthermore, do not click on links to websites you are unfamiliar with. If in doubt, perform a search for the site, with the site name in quotation marks (e.g. "www.badwebsite.com") to see if it is a legitimate website. You can also run potentially suspicious links through VirusTotal's URL scanner. This is not 100 percent accurate, but it is a good precaution to take.



Finally, if you click on any link from a message and are asked to log in to something, do not do it unless you are 100 percent sure that the email is legitimate and is sending you to the appropriate site. Many phishing attacks will provide links that send you to fake login pages for Gmail, Facebook, or other popular sites. Do not fall for them. You can always open a new browser, and go directly to a known site like Gmail.com, Facebook.com, etc. yourself if you want or need to login. That will also take you to the content, safely – if it was legitimate in the first place.

What should we do when we get a phishing message?

If anyone within parliament receives an unsolicited attachment, link, image, or an otherwise suspicious message or call, it is important that they immediately report it to the IT security point-person(s) or team. If you do not have such an individual or team, you should identify them as part of developing your security plan. Staff and members can also report the email as spam or phishing directly in Gmail or Outlook.
Having a plan in place for what staff, members or volunteers should do if/when they receive a possible phishing message is crucial. In addition, we recommend taking these phishing best practices - not clicking on suspicious links, avoiding attachments, and checking the "from" address - and sharing them with others that you work with, preferably through a widely-used communication channel. This illustrates that you care about the people you are in communication with, and encourages a culture across your networks that is alert and aware of the dangers of phishing. Your security depends on those organizations you trust, and vice versa. Better practices protect everyone.
In addition to sharing the tips above with everyone, you can also practice identifying phishing with the Google Phishing Quiz. We also strongly recommend setting up regular phishing training with staff to test awareness and keep people vigilant. Such training can be formalized as part of regular team and parliamentary meetings, or held more informally. What is important is that everyone involved in parliamentary operations feels comfortable asking questions about phishing, reporting phishing (even if they feel they might have made a mistake such as by clicking a link), and that everyone is empowered to help defend parliament against this high impact and high likelihood threat.



Phishing

- **Regularly train members and staff on what phishing is and how to spot it and defend against it, including phishing on text messages, messaging apps, and phone calls, not just email.**
- **Frequently remind members and staff of best practices such as:**
  - Do not download unknown or potentially suspicious attachments.
  - Check the URL of a link before you click. Do not click unknown or potentially suspicious links.
  - Do not provide sensitive or private information via email, text, or phone call to unknown or unconfirmed addresses or people.
- **Encourage reporting of phishing.**
  - Establish a reporting mechanism and point-person for phishing within parliament.
  - Reward reporting, and do not punish failure.

Communicating and Storing Data Securely

Communications and Sharing Data

To make the best decisions for your parliament about how to communicate, it is essential to understand the different types of protection that our communications can have, and why such protection is important.

One of the most important elements of communications security relates to keeping private communications private - which in the modern era is largely taken care of by encryption. Without proper encryption, internal parliamentary communications could be seen by any number of adversaries. Insecure communications can expose sensitive or embarrassing information and messages, reveal passwords or other private data, and possibly put your members or staff at risk depending upon the nature of your communications and content that you share. As a parliament, it is also important to ensure that members and staff's official governmental communications comply with all relevant open government obligations (such as freedom of information requests) and data security commitments. Therefore, when designing and implementing secure communications systems and policies across parliament, be sure to keep these factors in mind so that relevant messages can both be properly secured and, when necessary under law, preserved.

Secure Communications and Parliaments

There have been many incidents in recent years in which the communications systems of parliaments and accounts of MPs and their staff have been compromised, leading to disruption in parliamentary operations and in some cases the theft of sensitive communications. In July 2021, for instance, Polish authorities announced that the email accounts of nearly a dozen local MPs were hacked, including a personal account of the prime minister's top aide and accounts of members from almost every parliamentary opposition grouping. This report came just months after similar news came to light about a cyberattack against the information and communication systems of the Finnish parliament. Authorities in Finland described that attack as "aggravated espionage and message interception" aimed at its parliament.

WHAT IS ENCRYPTION AND WHY IS IT IMPORTANT?

Encryption is a mathematical process used to scramble a message or a file so that only a person or entity with the key can "decrypt" it and read it. The Electronic Frontier Foundation's Surveillance Self-Defense Guide provides a practical explanation (with graphics) of what encryption means:

Unencrypted Messaging

Without any encryption in place, our messages are left open to being read by potential adversaries, including unfriendly foreign governments, or hackers on the web. Such encryption is important not just for internal parliamentary communications but also for external communications in which privacy and integrity need to be protected.

As you can see in the image above, a smartphone sends a green, unencrypted text message ("hello") to another smartphone on the far right. Along the way, a cellphone tower (or in the case of something sent over the internet, your internet service provider, known as an ISP) passes the message along to company servers. From there it hops through the network to another cellphone tower, which can see the unencrypted "hello" message, and is finally then routed to the destination. It is important to note that without any encryption, everyone involved in relaying the message, and anyone who can sneak a peek as it goes by, can read its content. This might not matter much if all you are saying is "hello", but it could be a big deal if you are communicating something more private or sensitive that you do not want your telecom, ISP, an unfriendly government, or any other adversary to see. Because of this, it is essential to avoid using unencrypted tools to send any sensitive messages (and ideally any messages at all.) Keep in mind that some of the most popular communication methods - such as SMS and phone calls - practically operate without any encryption (like in the image above).

There are two ways to encrypt data as it moves: ***transport-layer encryption*** and ***end-to-end encryption.*** The type of encryption a service provider supports is important to know as your parliament makes choices to adopt more secure communications practices and systems. Such differences are described well by the Surveillance Self-Defense guide, which is adapted again here:

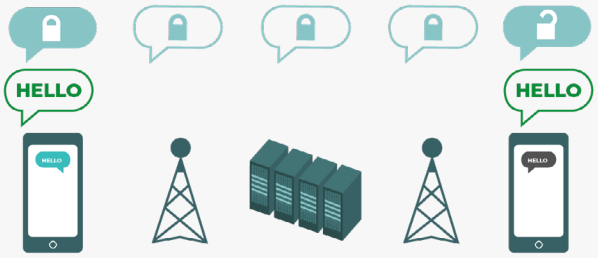
Transport-layer Encryption

Transport-layer encryption, also known as transport layer security (TLS), protects messages as they travel from your device to the messaging app/service's servers and from there to your recipient's device. This protects them from the prying eyes of hackers sitting on your network or your internet or telecommunications service providers. However, in the middle your messaging/email service provider, the website you are browsing, or the app you are using can see unencrypted copies of your messages. Because your messages can be seen by (and are often stored on) company servers, they may be vulnerable to law enforcement requests or theft if the company's servers are compromised.

The image above shows an example of transport-layer encryption. On the left, a smartphone sends a green, unencrypted message: "Hello." That message is encrypted, and then passed along to a cellphone tower. In the middle, the company servers are able to decrypt the message, read the contents, decide where to send it, re-encrypt it, and send it along to the next cellphone tower towards its destination. At the end, the other smartphone receives the encrypted message, and decrypts it to read "Hello."

End-to-End Encryption

End-to-end encryption protects messages in transit all the way from sender to receiver. It ensures that information is turned into a secret message by its original sender (the first "end") and decoded only by its final recipient (the second "end"). No one, including the app or service you are using, can "listen in" and eavesdrop on your activity.



The image above shows an example of end-to-end encryption. On the left, a smartphone sends a green, unencrypted message: "Hello." That message is encrypted, and then passed along to a cellphone tower and then to the app/service's servers, which cannot read the contents, but will pass the secret message along to its destination. At the end, the other smartphone receives the encrypted message, and decrypts it to read "hello." Unlike with transport-layer encryption, your ISP or messaging host is not able to decrypt the message. Only the endpoints (the original devices sending and receiving encrypted messages) have the keys to decrypt and read the message.

WHAT TYPE OF ENCRYPTION DO WE NEED?

When deciding whether your parliament needs transport-layer encryption or end-to-end encryption for your communications (or some combination of the two for different systems and activities), the big questions you should ask involve trust. For instance, do you trust the app or service you are using? Do you trust its technical infrastructure? Are you concerned about the possibility that an unfriendly foreign government could force the company to hand over your messages – and if so, do you trust the company's policies to protect against foreign law enforcement requests?

If you answer "no" to any of these questions, then you need end-to-end encryption. If you answer "yes" to them, then a service that supports only transport-layer encryption may suffice - but it is generally better to go with services that support end-to-end encryption when possible.

Another set of questions to consider is whether you as a parliament are required by law to maintain sole access to any parliamentary communications, whether there are any data localization requirements in your country, and/or if certain communications need to be preserved (e.g. not permanently deleted by staff) in order to comply with open government laws and commitments. If so, you might consider an end-to-end encryption-enabled enterprise-grade communications system in which you, as a parliament, are able to control the encryption keys yourself. Such systems (which will be discussed in more detail in the **"Storing Data Securely"** section of the Handbook) can be powerful, but do require advanced technical skills to implement.

Also, when messaging with groups, keep in mind that the security of your messages is only as good as the security of everyone receiving the messages. In addition to carefully choosing secure apps and systems, it is important that everyone in the group follows other best practices regarding account security and device security. All it takes is one bad actor or one infected device to leak the contents of an entire group chat or call.

WHAT SHOULD WE DO ABOUT EMAIL?

In general, email is not the best option when it comes to security. Even the best end-to-end encrypted email options typically leave something to be desired from a security perspective, for example, not encrypting subject lines of emails and not protecting metadata (an important concept which will be described below). If you need to communicate highly sensitive information that does not need to be retained for the public record, keep in mind that email (both the parliament's system and especially someone's personal account) is best avoided in favor of secure messaging options (which will be highlighted in the next section).

However, as a parliament, you may still want or need for members and staff to communicate sensitive or private content through a system that is centrally managed as part of their day-to-day operations. A parliament-wide email system, with proper account controls of course, can be useful here. If, according to your analysis above, transport-layer encryption will suffice, then standard business offerings from email providers such as Google Workspace (Gmail) and Microsoft 365 (Outlook) could be solid options for your parliament. However if you are worried that your email provider could be legally required to provide information about your communications to a foreign government or another adversary, or if local data residency requirements may be a concern, you will want to consider using an end-to-end encrypted email option. A few such options include adding your own encryption key management to Google Workspace or Microsoft 365 (as described in the **"Storing Data Securely"** section of this Handbook), or adopting end-to-end encrypted email services designed for large organizations such as **ProtonMail** Business or **Tutanota** Business.

WHAT IS METADATA AND SHOULD WE BE CONCERNED ABOUT IT?

Who you and your staff, members, and teams talk to and when and where you talk to them can often be just as sensitive as what you talk about. It is important to remember that end-to-end encryption only protects the contents (the "what") of your communications. This is where metadata comes into play. EFF's Surveillance Self-Defense Guide provides an overview of metadata and why it matters (including an illustration of what metadata looks like):

Metadata is often described as everything except the content of your communications. You can think of metadata as the digital equivalent of an envelope. Just like an envelope contains information about the sender, receiver, and destination of a message, so does metadata. Metadata is information about the digital communications you send and receive.

Some examples of metadata include:

- who you are communicating with
- the subject line of your emails
- the length of your conversations
- the time at which a conversation took place
- your location when communicating

While transparency of applicable parliamentary operations is essential, limiting unauthorized access to metadata (in addition to protecting the content of communications) is important as well. After all, metadata can reveal sensitive information to hackers, foreign governments, companies, or others whom you might not want to have access. A couple examples of how revealing metadata can be include:

They know an MP or staffer called a journalist and spoke with them for an hour before that journalist published a story with an anonymous quote. However, they do not know what you talked about.

They know you got an email from a COVID testing service, then called your doctor, then visited the World Health Organization's website in the same hour. However, they do not know what was in the email or what you talked about on the phone.

Recommended End-to-End Encrypted Communications Tools

TEXT MESSAGING (INDIVIDUAL OR GROUP)	• **Signal** • **WhatsApp (only with specific setting configurations detailed below)**
AUDIO AND VIDEO CALLS	• **Signal (up to 40 people)** • **WhatsApp (up to 32 people on audio, eight on video)**
FILE SHARING	• **Signal** • **Keybase / Keybase Teams** • **Tresorit**

WHAT END-TO-END ENCRYPTED MESSAGING TOOLS SHOULD WE USE (AS OF 2022)?

If you need to use end-to-end encryption, or just want to adopt the best practice regardless of your parliament's threat context, here are some trusted examples of services that, **as of 2022,** offer end-to-end encrypted messaging and calls. This section of the Handbook will be regularly updated online, but please note that things change quickly in the world of secure messaging, so these recommendations may not be up to date at the time you are reading this section. Keep in mind that your communications are only as secure as your device itself. In addition to adopting secure messaging practices, it is essential to implement the best practices described in the "Secure Devices" section of this Handbook.

Metadata is not protected by the encryption provided by most message services. If you are sending a message on WhatsApp, for example, keep in mind that while the contents of your message are end-to-end encrypted, it is still possible for others to know who you are messaging, how frequently, and, with phone calls, for how long. As a result, you should keep in mind what risks exist (if any) if certain adversaries are able to find out who you talk to, when you talked to them, and (in the case of email) the general subject lines of your parliament's communications.

One of the reasons that **Signal** is so highly recommended is that, in addition to providing end-to-end encryption, it has **introduced features and made commitments to reduce the amount of metadata that it records and stores.** For instance, Signal's Sealed Sender feature encrypts the metadata about who is talking to whom, so that Signal only knows the recipient of a message but not the sender. By default this feature only works when communicating with existing contacts or profiles (people) with whom you have already communicated or whom you have stored in your contacts list. However you can enable this "Sealed Sender" setting to "Allow from anyone" if it is important for you to eliminate such metadata across all Signal conversations, even those with people unknown to you.

This may not be critical for the majority of parliamentary communications, but it is important to be aware of the risks posed by metadata and to select appropriate communication tools and policies accordingly.

CAN WE REALLY TRUST WHATSAPP?

WhatsApp is a popular choice for secure messaging, and can be a good option given its ubiquity. Some people are concerned that it is owned and controlled by Facebook, which has been working to integrate it with its other systems. People are also concerned about the amount of metadata (i.e. information about with whom you communicate and when) that WhatsApp collects. If you choose to use WhatsApp as a secure messaging option, be sure to read the above section on metadata. There are also a few settings that you need to ensure are properly configured. Most critically, be sure to turn off cloud backups or, at the very least, enable WhatsApp's new end-to-end encrypted backups feature using a 64 digit encryption key or long, random, and unique passcode saved in a secure place (like your password manager). Also be sure to show security notifications and verify security codes. You can find simple how-to guides for configuring these settings for Android phones here and iPhones here. **If your staff *and those with whom you all communicate* do not properly configure these options, then you should not consider WhatsApp to be a good option for sensitive communications that require end-to-end encryption.** Signal still remains the best option for such end-to-end encrypted messaging needs given its secure default settings and protection of metadata.

WHAT ABOUT TEXTING?

Basic text messages are highly insecure (standard SMS is effectively unencrypted), and should be avoided for anything that is not meant for public knowledge. While Apple's iPhone-to-iPhone messages (known as iMessages) are end-to-end encrypted, if a non-iPhone is in the conversation the messages are not secured. It is best to be safe and **avoid text messages for anything remotely sensitive, private, or confidential.**

WHY AREN'T TELEGRAM, FACEBOOK MESSENGER, OR VIBER RECOMMENDED FOR SECURE CHATS?

Some services, like Facebook Messenger and Telegram, only offer end-to-end encryption if you deliberately turn it on (and only for one-to-one chats), so they are not good options for sensitive or private messaging, especially for teams. Do not rely on these tools if you need to use end-to-end encryption, because it is quite easy to forget to change away from the default, less secure settings. Viber claims to offer end-to-end encryption, but has not made its code available for review to outside security researchers. Telegram's code has also not been made available for a public audit. As a result, many experts fear that Viber's encryption (or Telegram's "secret chats") may be substandard and therefore not suitable for communications that require true end-to-end encryption.

OUR PARLIAMENTARY COLLEAGUES AND CONSTITUENTS ARE USING OTHER MESSAGING APPS AND SYSTEMS FOR COMMUNICATION - HOW CAN WE CONVINCE THEM TO DOWNLOAD A NEW APP TO COMMUNICATE WITH US?

Sometimes there is a tradeoff between security and convenience, but a little extra effort is worth it for sensitive communications. Set a good example for your contacts - whether they be in other government agencies, institutions, across parliament or external constituents. If you have to use other less secure systems, be very conscious of what you are saying. Avoid discussion of sensitive topics. Some parliaments may have different protocols for general chatting or public facing communications compared to confidential discussions with leadership, for example. Classify your parliamentary communications (internal and external) based upon sensitivity and be sure members and staff are using appropriate communication mechanisms accordingly! Of course, it is simplest if everything is just automatically encrypted all the time - nothing to remember or think about.

Luckily, end-to-end encrypted apps like Signal are becoming increasingly popular and user-friendly - not to mention that they have been localized in dozens of languages for global use. If your partners or other contacts need help switching communications over to an end-to-end encrypted option like Signal, take some time to talk them through why it is so important to properly protect your communications. When everyone understands the importance, the few minutes required to download a new app and the couple days it might take to get used to using it will not seem like a big deal.

ARE THERE OTHER SETTINGS FOR END-TO-END ENCRYPTED APPS THAT WE SHOULD BE AWARE OF?

In the Signal app, verifying security codes (which they refer to as Safety Numbers) is also important. To view a safety number and verify it in Signal, you can open up your chat with a contact, tap their name at the top of your screen, and scroll down to tap "View Safety Number." If your safety number matches with your contact, you can mark them as "verified" from that same screen. It is especially important to pay attention to these safety numbers and to verify your contacts if you receive a notification in a chat that your safety number with a given contact has changed. If you or other staff need help configuring these settings, Signal itself **provides helpful instructions.** If using Signal, which is widely considered to be the best user-friendly option for secure messaging and one-to-one calls, be sure to **set a strong pin.** Use at least six digits, and not something easy-to-guess like your birth date. For more tips on how to properly configure **Signal** and **WhatsApp**, you can check out the **tool guides** for both developed by EFF in their **Surveillance Self-Defense Guide.**

WHAT ABOUT LARGER GROUP VIDEO CALLS? ARE THERE END-TO-END ENCRYPTED OPTIONS?

With the increase in remote work, it is important to have a secure option for your office's large group video calls or virtual town halls for MPs. Unfortunately, no great options currently exist that check all the boxes: user-friendly, support large numbers of attendees and collaboration features, and enable end-to-end encryption by default.

The specific needs of plenary sessions and committee meetings will be discussed later in this Handbook, but for your other more general meetings that do not require collaboration features like screen sharing or breakout rooms, there are a couple of options.

For groups of up to eight people, Signal is highly recommended. Group video calls on Signal can be joined either from a smartphone or the Signal desktop app on a computer. Keep in mind, however, that only your contacts who already use Signal can be added to a Signal group.

If you are looking for other options, one platform that recently added an end-to-end encrypted option is **Jitsi Meet.** Jitsi Meet is a web-based audio and video conferencing solution that can work for large audiences (up to 100 people) and requires no app download or special software. Note that if you use this feature with large groups (more than 15-20 people) the call quality may decrease. To set up a meeting on Jitsi Meet, you can go to meet.jit.si, type in a meeting code and share that link (via a secure channel such as Signal) with your desired participants. To use end-to-end encryption, take a look at these instructions outlined by Jitsi. Note that all individual users will need to enable end-to-end encryption themselves in order for it to work. When using Jitsi, be sure to create random meeting room names and to use strong passcodes to protect your calls.

If this option does not work for your teams, you can consider using a popular commercial option like Webex or Zoom with end-to-end encryption enabled. Webex has long allowed for end-to-end encryption; however this option is not turned on by default and requires participants to download Webex to join your meeting. To get the end-to-end encrypted option for your Webex account you must open a Webex support case and follow these instructions to ensure end-to-end encryption is configured. Only the host of the meeting needs to enable end-to-end encryption. If they do so, the entire meeting will be end-to-end encrypted. If using Webex for secure group meetings and workshops, be sure to also enable strong passcodes on your calls.

After months of negative press, Zoom developed an end-to-end encryption option for its calls. However, that option is not turned on by default, requires that the call host associate their account with a phone number, and only works if all participants join via the Zoom desktop or mobile app instead of dialing in. Because it is easy to accidentally misconfigure these settings, it is not ideal to rely on Zoom as an end-to-end encrypted option. However, if end-to-end encryption is required and Zoom is your only option, you can follow Zoom's instructions to configure it. Just be sure to check any call before it starts to ensure it is indeed end-to-end encrypted by clicking the green lock in the upper left-hand corner of the Zoom screen and seeing "end-to-end" listed next to the encryption setting. You should also set a strong passcode for any Zoom meeting.

It is worth noting, however, that certain popular features of the above tools only work with transport-layer encryption. For example, turning on end-to-end encryption in Zoom disables breakout rooms, polling capabilities, and cloud recording. In Jitsi Meet, breakout rooms can disable the end-to-end encryption feature, leading to an unwitting decrease in security.

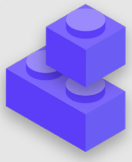
A NOTE ABOUT FILE SHARING

In addition to securely sharing messages, sharing files safely is likely an important part of your parliament's security plan. Most file-sharing options are built-in to messaging applications or services that you might already be using. For instance, sharing files via Signal is a great option if end-to-end encryption is needed. If transport-layer encryption is enough, using Google Drive or Microsoft SharePoint might be a good option for your parliament. Just be sure to configure sharing settings properly so that only the appropriate people have access to a given document or folder, and ensure that these services are connected to staff's organizational (not personal) email accounts. If you can, prohibit sharing sensitive files via email attachments or physically with USBs. Using devices like USBs within your parliament greatly increases the likelihood of malware or theft and relying on email or other forms of attachments weakens your parliament's defenses against phishing attacks.

WHAT IF WE REALLY DO NOT NEED END-TO-END ENCRYPTION FOR ALL OUR COMMUNICATIONS?

If end-to-end encryption is not needed for all of your parliament's communications based upon your risk assessment, you can consider using applications protected by transport-layer encryption. Remember, this type of encryption requires that you trust the service provider, such as Google for Gmail, Microsoft for Outlook/Exchange, or Facebook for Messenger, because they (and anyone they might be compelled to share information with) can see/hear your communications. Once again, the best options will depend upon your threat model (for example, if you do not trust Google or if the U.S. government is your adversary, then Gmail is not a good option), but a few popular and generally trusted options include:

EMAIL	• **Gmail (via Google Workspace)** • **Outlook (via Office 365)** • Do not host your own Microsoft Exchange server for your parliament's email. If you are currently doing so, you should migrate to Office 365.
TEXT MESSAGING (INDIVIDUAL OR GROUP)	• **Google Hangouts** • **Slack** • **Microsoft Teams** • **Mattermost** • **Line** • **KaKao Talk** • **Telegram**
GROUP CONFERENCING, AUDIO AND VIDEO CALLS	• **Jitsi Meet** • **Google Meet** • **Microsoft Teams** • **Webex** • **GotoMeeting** • **Zoom**
FILE SHARING	• **Google Drive** • **Microsoft Sharepoint** • **Dropbox** • **Slack** • **Microsoft Teams**



Communicating Data Securely

- **Classify communications based upon their sensitivity.**
  - Determine the appropriate systems and tools for communication accordingly.
  - Set a policy on how long you will retain messages accordingly, keeping in mind both security and commitments to parliamentary transparency.
- **Require the use of trusted end-to-end encrypted messaging services for your parliament's sensitive communications.**
  - Take time to explain to staff and external partners why secure communications are so important; this will enhance the success of your plan.
- **Ensure proper settings are in place for secure communications apps, including:**
  - Ensure all staff are paying attention to security notifications and, if using WhatsApp, not backing up chats.
  - If using an app where end-to-end encryption is not enabled by default (e.g. Zoom or Webex), ensure the required users have turned on the proper settings at the outset of any call or meeting.
- **Do not attempt to host your own email server - use cloud-based email services such as Office 365 or Google Workspace as alternatives.**
  - Do not allow staff to use personal email accounts for work.
- **Frequently remind staff and members about security best practices related to group messaging and metadata.**
  - Be aware of who is included in group messages,chats, and email threads.

Digital Parliaments (e-Parliament)

As a parliament, it is important to pay particular attention to the communications and operational security policies of your most essential functions, including those that occur online and in the digital space.

Whether your parliament is considering a full "e-Parliament" system that can digitize everything from the drafting of bills through debate and electronic voting (such as Nextsense, Propylon, or Granicus to name a few examples), or you are using simpler, less-expensive tools to facilitate your parliamentary operations, it is essential to consider how any tool (or tools) and process (or processes) take into account the security, integrity, and availability of information.

Security and Digital Parliaments

As evidenced by a series of incidents in South Africa, the transition of parliamentary operations to the digital world necessitates attention to cybersecurity to avoid not just the loss or theft of sensitive data, but also potential embarrassment, insult, and harm to members and staff. In May 2020, pornographic images popped up a few minutes before the start of a virtual meeting of the country's National Assembly. Following the display of the offensive images, the "hacker" or "zoom bomber" then hurled sexist and racial insults at the speaker of the assembly who was hosting the session, forcing the meeting to adjourn. A similar incident occurred a month prior when a meeting chaired by the minister of women, youth and persons with disabilities was disrupted with pornographic images.

REMOTE PLENARY SESSIONS AND COMMITTEE MEETINGS

Chief among those processes are the plenary sessions and committee meetings. These sessions and the conversations, decisions, and votes that occur within them are at the core of much of your parliament's work and as such can be a particular target for adversaries. In a modern, pandemic-impacted world, such sessions and meetings are taking place in increasingly diverse fashion depending upon your country's context, both in-person, completely online, and in a "hybrid" fashion.

As outlined in the House Democracy Partnership's recent **Parliaments Responding to a Pandemic** guide, the typical parliamentary debate structure is different from a normal conference discussion or standard organizational meeting. Needs for remote voting, the submission of official proposals and amendments, structured debate, and even simultaneous interpretation to ensure inclusion of all constituencies often require additional features not found in most standard technology solutions. As a result, when hosting a virtual or hybrid session, it is likely that your parliament may need to develop (or already has developed) custom software, or purchase expensive, enterprise solutions (such as **Cisco's Webex Legislate**) designed specifically to manage parliamentary sessions remotely. Whatever option your parliament chooses, it is important to give thought, as outlined in the **Parliaments Responding to a Pandemic** guide, to how all members and staff will be able to access such a system. It's also crucial to ensure such a system is properly secured.

When building and implementing technical solutions for parliamentary sessions, it's important to ensure basic security fundamentals are in place. These include steps to ensure data is secured "at-rest" within the system itself, properly encrypted while in transit, and that only authorized users are able to access the system. There are many approaches that can be taken to ensure such security, including many of the fundamentals outlined throughout the rest of this Handbook. End-to-end encryption on any data sharing and communications systems used, strong password and two-factor authentication requirements and/or IP address restriction for users to access such systems (unless they are intended to be open to the public), the requirement of virtual private networks (which will be discussed later in the Handbook), and the limitation of access to only trusted, clean devices are all helpful steps.

REMOTE VOTING

The need for robust security is perhaps most critical when dealing with remote voting. As the aforementioned **Parliaments Responding to a Pandemic** guide highlights, MPs are elected to parliament for the specific purpose of voting on behalf of their constituents. The ability to trust and verify these votes is crucial not only to the functioning of your parliament itself but to the democratic system as a whole. Such votes are relatively easily verified when an MP votes in person, but when participating virtually, technical authentication becomes a greater challenge that requires significant care and focus. As outlined in expert **testimony** given to the Canadian House of Commons' Standing Committee on Procedure and House Affairs, parliaments typically choose one of four options for remote voting:

- Email voting: where members receive a ballot form electronically and submit their vote via email. This option is generally considered insecure, in part due to its lack of end-to-end encryption, and should be avoided.
- Web-based voting: where members access and cast ballots via a website on either a computer or mobile phone. This approach requires investment in secure infrastructure, including secured devices with strong authentication controls as mentioned above.
- Application-based voting: where members download an application to access and cast ballots. Similar to web-based voting, but uses a specific app, which can be downloaded to a phone or tablet as opposed to being accessed through a browser.
- Video voting: where members vote on-screen by a show of hands or a voice vote. For non-anonymous voting this can be the least technically complicated and least technically sophisticated to set-up and secure. It does still require robust encryption and authentication systems, however, to avoid impersonation or interruption during voting sessions.

Whatever option your parliament chooses to implement for remote voting - if it uses remote voting at all - it is important to address cybersecurity basics throughout the voting process as well. Such fundamentals include ensuring the devices that MPs use to cast votes are properly secured physically and free from malware, that members' internet access is properly secured when voting (and when conducting other parliamentary business as well), and that members have stable internet connections and are able to vote when called upon. As outlined in the **Parliaments Responding to a Pandemic** guide,

when adopting remote voting, there is a need for extensive testing of the system before it goes live and a need to provide support and training to MPs to ensure they can use the system effectively. It is important to remember that part of security is *availability*. There is also a need in particular to ensure that women MPs and staff are able to use online systems safely, including remote voting, and have access to the technology to do so. When women, particularly elected women, go online they face greater levels of intimidation and harassment, and this factor should be considered when developing and using technology like remote voting to ensure that all MPs are able to fulfill their functions effectively. Further, it is critical to ensure adequate remote multi-language access in countries where multiple formal languages are spoken by members and staff.

E-PARLIAMENT VENDOR AND SOFTWARE SECURITY

Any software that you procure - whether used for remote voting or a broader range of parliamentary needs - **should come from a secure and accredited source, be audited for security by independent teams, and receive appropriate certifications.** It is important to remember that software developers, those whom you hire to build an application or tool, are not always security experts themselves. Therefore, bringing in security experts to test the application for potential security gaps via an audit is critical to reducing the risk that your platform, tool, or app could be hacked or compromised. Even the best software developers make mistakes without a second (or third) set of expert eyes checking their work!

Remote Voting in the Real World

Various parliaments have implemented remote voting systems and, in doing so, taken considerable steps to ensure the security and integrity of members' votes. One element in this process, among others mentioned above, is to ensure proper authentication. A few examples include in the U.K. House of Commons where members use a single sign-on process to log in to their parliamentary accounts before voting, which requires a password to be used on a specific, assigned device. In Spain, MPs are assigned personal codes that must be entered via a smartphone app before a vote can be recorded remotely. In Chile, senators who vote remotely via the chamber's carefully designed remote voting app must be visible on screen in order to cast a vote.

Storing Data Securely

For most parliaments, one of the most important decisions to make is where to store their data.

Is it "more secure" to store data on staff computers, on a local server, on external storage devices, or in the cloud? In 99 percent percent of situations, the easiest and most secure option is to keep data stored in trusted cloud storage services. Perhaps the most common examples include Microsoft 365 and Google Drive. Without a comprehensive cloud storage plan, it is likely that your parliament's data is stored in a variety of places - including staff and MPs' computers, external hard drives, and even a few local servers. While it is possible to secure data on all these devices, it is very hard to do so successfully without spending a lot of money and hiring significant IT staff.

Data Storage and Parliaments

The advent of affordable (sometimes free) cloud-based data storage has made life easier (and more secure) for many parliaments and other organizations. Unfortunately, many still attempt to host their own servers with relatively limited IT budget, staffing, and support. In March 2021, the threat of such organizational infrastructure became real for tens of thousands of organizations, including parliaments, across the world when a Chinese government-affiliated threat actor, called Hafnium, unleashed a global cybersecurity catastrophe with a sophisticated attack on self-hosted Microsoft Exchange servers. The attack compromised local servers, including that of Norway's parliament, enabling the hackers to gain access to parliamentary email accounts, install additional malware on the victim's servers and connected systems, and ultimately extract sensitive data. While Microsoft quickly published an update and instructions to identify and remove potential intruders once the hacks became public, many organizations lacked the IT capacity to quickly apply such updates, leaving them exposed for extended periods of time. The scope and impact of this global hack reveals the danger of parliaments and other organizations choosing to self-host email servers and other types of sensitive data, particularly without significant investment in dedicated cybersecurity staff.

BENEFITS OF CLOUD STORAGE

Even if you take all the right steps to protect your computers against malware and physical theft, it is still possible for a determined adversary to hack into your computer or local parliamentary server. It is much harder for them to defeat the security defenses of, for example, Google or Microsoft. Good cloud storage companies have unparalleled security resources and have a strong business incentive to provide maximum security to their users. In short: a trusted cloud storage strategy will be much easier to implement and keep secure over time. So instead of trying to identify (and retain) the number of dedicated and highly skilled cybersecurity staff required to protect local servers in your parliament, focus your energy on a handful of simpler tasks. These include choosing the right cloud storage option for your data privacy and localization needs, implementing good account security, training staff to properly share (and not share) folders and documents (in general, you should set up folders within your cloud storage drive that limit access to only the staff that need it for given files), and routinely auditing your system to make sure that staff and members are not "oversharing" any files (such as by turning on universal link sharing for files that should instead be limited to just a few people). Keeping the bulk of your information in the cloud helps with a range of common risks. Was someone's computer left in a restaurant or their phone on the bus? Did your child tip a glass of juice onto your keyboard, leaving your device inoperable? Do you need to compartmentalize data that belongs to an MP herself from information she generates for parliament itself? Does a staffer have malware and need to erase their computer and start fresh? If most documents and data are in the cloud, it is easy to re-synchronize and start fresh on a cleaned or entirely new computer. Also if malware gets into a computer or if a thief scans a hard drive, there is nothing to steal if most documents are accessed through the web browser.

CAN WE REALLY TRUST CLOUD STORAGE?

In short, there is nothing inherently untrustworthy about cloud storage. As mentioned above, most major cloud storage providers have teams of the world's best security engineers working to protect their products every day, and offer security support to their customers beyond what most small IT departments might be able to provide on their own.

Keep in mind, however, that traditional cloud storage services usually require granting access to sensitive data to a third-party company that provides the service. **With that said, every individual parliament will have its own political considerations and legal requirements (such as data localization mandates) to consider when choosing whether it can trust and use a given cloud storage provider.**

WHAT CLOUD STORAGE PROVIDER SHOULD WE CHOOSE?

If your parliament does not have to consider any data localization requirements, and has no issue with a trusted third-party company sharing access to data, the two most popular cloud storage options are Google Workspace (formerly known as GSuite) and Microsoft 365. If your parliament already uses Gmail, signing up for Google Workspace and storing data in Google Drive with its built-in Google Docs, Sheets, and Slides apps for word processing, spreadsheets, and presentations make a lot of sense. Similarly, if your parliament is reliant on Excel and Word, the easy choice is to sign up for Microsoft 365, which grants access to Outlook for email and licensed versions of Microsoft Word, Excel, PowerPoint, and Teams.

WHAT IF WE NEED TO CONTROL OUR OWN DATA OR COMPLY WITH DATA LOCALIZATION LAWS?

For many parliaments, such a simple option might not be feasible given either data localization requirements or specific expectations that require exclusive parliamentary control over its own data. The good news is that recently, secure cloud storage providers have developed options that allow enterprise customers to either choose the location of their data (note that this is mostly limited to European customers for now), or to control their own encryption keys. **In practice, this means that your parliament has options to control its own data while still benefiting from the infrastructure and security of cloud storage.**

If your parliament is currently using or interested in Google Workspace for cloud data storage and sharing, Google introduced a feature enabling Client-side encryption for Enterprise Plus organizations. While currently in a testing phase and available only to the most expensive Google Workspace plans, this feature provides an option to take advantage of Google Drive's full suite of data storage and sharing functions - and the security features built into them - while limiting Google's ability to access your parliament's sensitive or private information. With client-side encryption, you can choose to integrate an additional key management service, such as Virtru, and allow users to manage their own encryption keys without allowing access to Google itself. Such a service requires everyone to take great care in protecting those keys to properly protect access to whichever key management system you choose to integrate into Google Workspace. Account administrators can learn more about how to enable client-side encryption on Google Workspace's support page.

If your parliament is currently using or interested in Microsoft 365 for cloud data storage and sharing, it offers a slightly more complex but well established option for managing your own encryption keys known as Microsoft 365 Double Key Encryption. This security option requires Microsoft 365 E5, but allows you to keep control of any sensitive or private parliamentary data and limit access even to Microsoft itself.

Tresorit is another option that is simpler to implement if your parliament is concerned about allowing a third-party to access your internal information. Tresorit provides end-to-end encryption for cloud storage and file sharing, and offers a range of data residency options.

WHAT IF WE CANNOT TRUST ANY CLOUD STORAGE SOLUTION?

If you do opt to go it alone and rely on local servers to store your parliament's data instead, it is crucial that you invest substantial time and resources into strengthening the digital defenses of your parliament's devices, and ensure such servers are properly configured, encrypted, and kept physically safe. As stated above, such an approach requires identifying, hiring, and retaining a number of dedicated and highly skilled cybersecurity staff to maintain the security of your local server infrastructure.

Enhancing the Security of Parliamentary Cloud Accounts

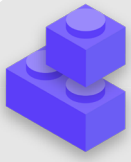
If your parliament chooses to set up a domain in Google Workspace or Microsoft 365, be aware that both companies offer higher levels of security for at-risk accounts. Google's Advanced Protection Program and Microsoft's AccountGuard provide even more robust security to eligible organizations' cloud accounts, and help you greatly reduce the likelihood of effective phishing and account compromise. If you believe that your parliament qualifies and are interested in enrolling your members and staff in either plan, visit the websites linked above or contact cyberhandbook@ndi.org for further assistance.

BACKING UP DATA

Whether your parliament stores data on physical devices and servers or in the cloud, it is important to have a backup. Keep in mind that if you rely on physical device storage, it is quite easy to lose access to your data. You could spill coffee on your computer and destroy the hard drive. Staff computers could be hacked and all local files locked with ransomware. Someone could lose a device on the train or have it stolen along with their briefcase. As mentioned above, this is another reason why using cloud storage can be a benefit, because it is not tied to a specific device that can be infected, lost, or stolen. Macs come with built-in backup software called Time Machine which is used together with an external storage device; for Windows devices, File History offers similar functionality. iPhones and Androids can automatically back up their most important contents to the cloud if enabled under your phone's settings.

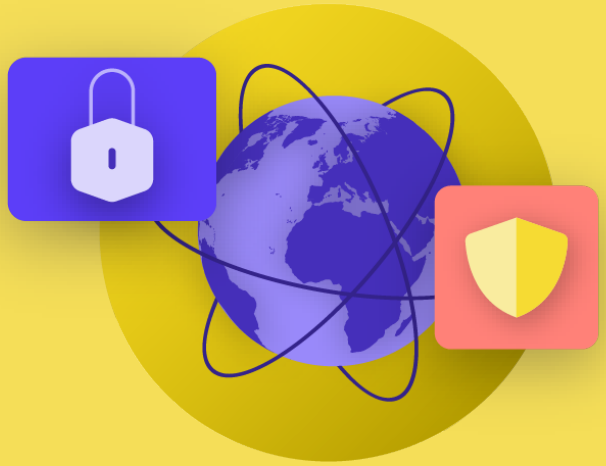
If your parliament is using cloud storage (like Google Drive) the risk of Google being taken down or your data destroyed in a disaster is quite low, but human error (like accidentally deleting important files) is still a possibility. Exploring a cloud backup solution like Backupify or SpinOneBackup may be worthwhile.

If data is stored on a local server and/or local devices, a secure backup becomes even more critical. You can backup your parliament's data to an external hard drive or series of drives, but be sure to encrypt such drives with a strong password. Time Machine can encrypt hard drives for you, or you can use trusted encryption tools for the whole hard drive like VeraCrypt or BitLocker. Be sure to keep any backup devices in a separate location from your other devices and files. Remember, a fire that destroys both your computers and their backups means you do not have backups at all. Consider keeping a copy in a very secure location, such as a safe deposit box.



Storing Data Securely

- **Store sensitive data exclusively in a trusted cloud storage service.**
  - Ensure any connected accounts used to access such a service have strong passwords and 2FA.
- **Set and enforce a policy to limit sharing settings within the cloud.**
  - Train all members and staff on how to properly share (and not overshare) documents.
- **If your parliament opts to store data locally, invest in skilled IT staff.**
- **Keep your data backups secure - encrypt backup hard drives or other backup devices.**



Staying Safe on the Internet

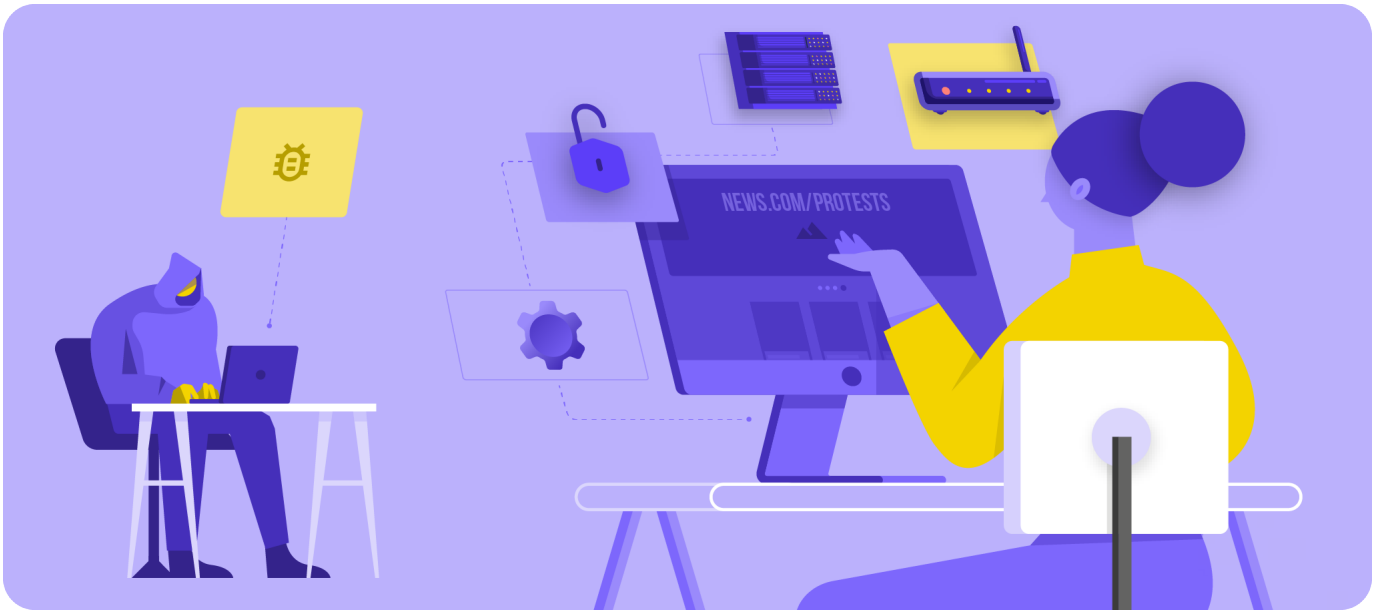
When using the internet on your phone or computer, your activity can say quite a bit about you and your organization.

It is important to keep sensitive information – like usernames and passwords that you type into a website, your social media posts, or in certain contexts even the names of the websites that you visit – out of the view of prying eyes. Having your access to certain sites or apps blocked or restricted is also a common concern. These two problems – internet surveillance and internet censorship – go hand in hand, and the strategies to reduce their impacts are similar.

Browsing Securely

USING HTTPS

The most important step to limiting an adversary's ability to surveil your parliament online is to minimize the amount of information available about you and your colleagues' internet activity. Always make sure you are connecting to websites securely: make sure the URL (location) starts with "https" and shows a small lock icon in the address bar of your browser. When you browse the internet **without encryption,** the information you type into a site (like passwords, account numbers, or messages), and the details of the site and pages you are visiting are all exposed. This means that (1) any hackers on your network, (2) your network administrator, (3) your ISP and any entity they might share data with (like governmental authorities), (4) the ISP of the site you are visiting and any entity they might share data with, and of course (5) the site you are visiting itself all have access to quite a bit of potentially sensitive information.



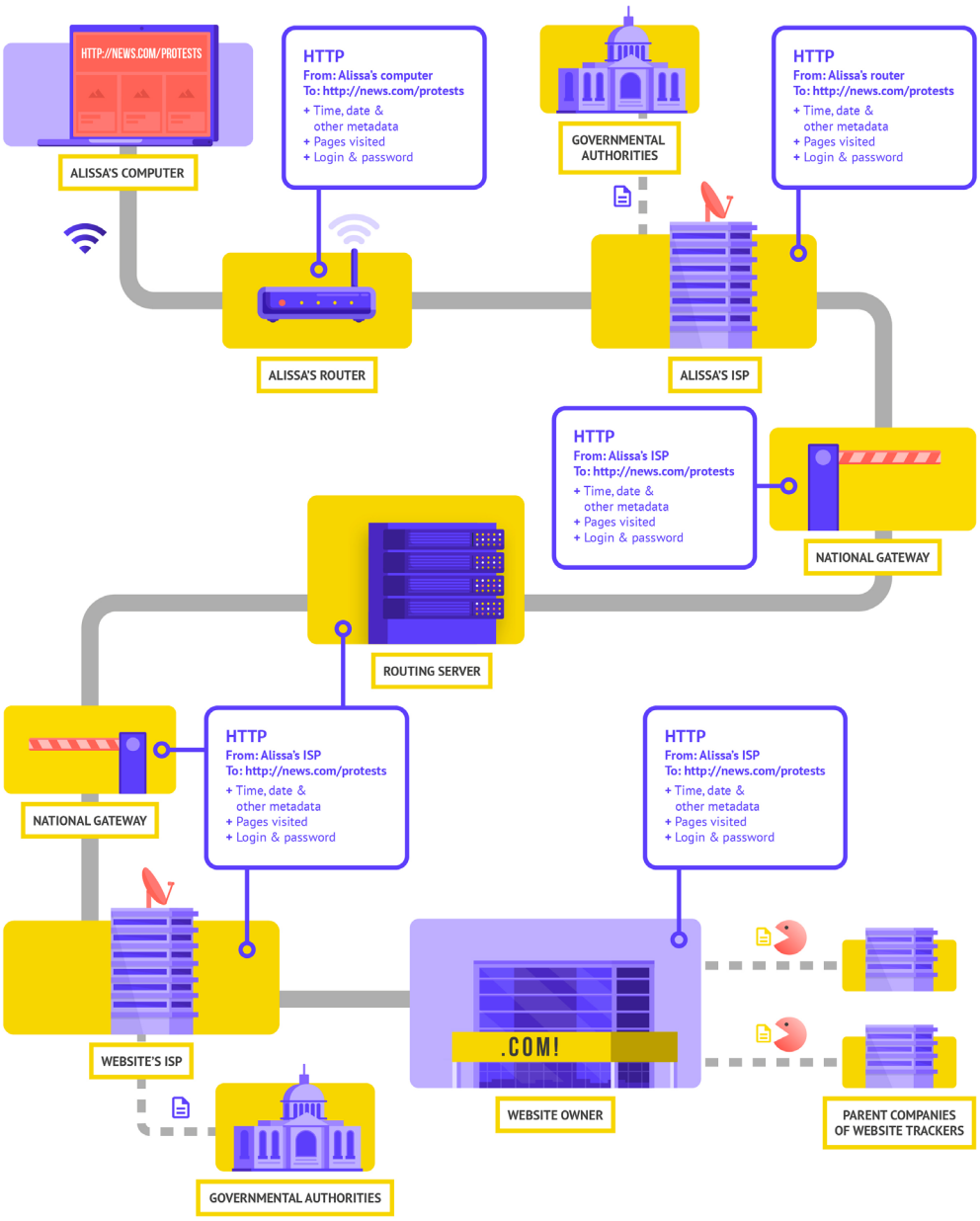
Surveillance, Censorship, and Parliaments

Unfriendly governments and other threat actors across the globe are using increasingly accessible surveillance technology, and in some cases simple Wi-Fi hacking, to monitor the online activity of MPs and others working in parliament. For instance, hackers stole data from European parliamentary staff and visitors by **spoofing the Parliament's public Wi-Fi network** in 2013. A preview of much more sophisticated attacks in years to follow.

In addition to hijacking internet traffic and stealing data, adversaries also disrupt critical parliamentary operations by blocking internet access and systems. In Brussels, Belgium's parliament was knocked offline by a **massive denial of service attack** in May 2021. The attack forced the postponement of some debates and committee meetings, as users could not access the virtual services required to take part in the session.

The increasing frequency of such attacks on access to and reedom of information online highlight just how essential it is for parliaments to understand the risks of operating on the internet and develop plans for how to connect when connectivity is impacted.

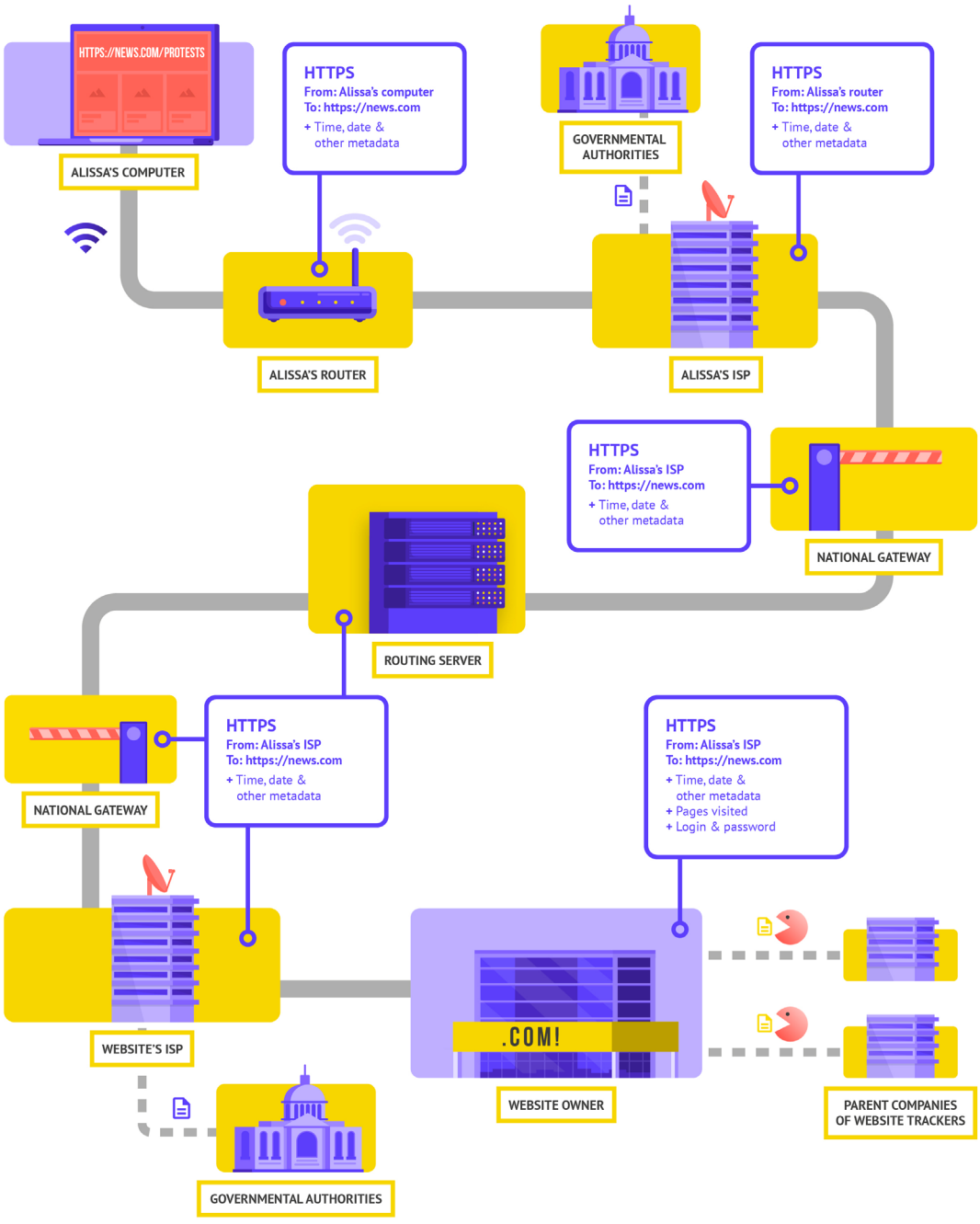
Let's take a real-world example of what browsing without encryption looks like:



Adapted from the Totem Project's How the Internet Works (CC–BY–NC–SA)

When browsing without encryption, all of your data is exposed. As shown above, an adversary can see where you are, that you are going to news.com, looking specifically at the page on protests in your country, and perhaps most importantly as an MP or member of parliamentary staff, see your password that you share to log in to the site itself. Such information in the wrong hands not only exposes your account but also gives potential adversaries, wherever they may be in the world, a good idea of what you might be doing or thinking about.

Using **HTTPS (the "s" stands for secure) means that encryption is in place.** This offers you much more protection. Let's take a look at what browsing with HTTPS (aka with encryption) looks like:



Adapted from the Totem Project's How the Internet Works (CC–BY–NC–SA)

With HTTPS in place, a potential adversary can no longer see your password or other sensitive information that you might share to a website. They can, however, still see what domains (for example, news.com) you are visiting. And while HTTPS also encrypts information about the individual pages within a site (for example, website.com/protests) that you visit, sophisticated adversaries can still see this information by inspecting your internet traffic. With HTTPS in place, an adversary might know that you are going to news.com, but they would not be able to see your password, and it would be more difficult (but not impossible) for them to see that you are looking up information about protests (to use this one example). That is an important difference. Always check that HTTPS is in place before navigating through a website or entering sensitive information. You can also use the **HTTPS Everywhere browser extension** to ensure you are using HTTPS at all times, or if you use Firefox, turn on **HTTPS only mode** in the browser.

If you are presented with a warning from your browser that a website might be insecure, do not ignore it. Something is wrong. It might be benign – like the site has an expired security certificate – or the site might be maliciously spoofed or faked. Either way, it is important to heed the warning and not proceed to the site. HTTPS is essential and encrypted DNS provides some extra protection against snooping and site blocking, but if your parliament is concerned about highly targeted surveillance regarding your online activities and faces sophisticated censorship online (such as websites and apps being blocked), you might want to use a trusted virtual private network (VPN).

Using Encrypted DNS

If you want to make it more difficult (but not impossible) for an ISP to know the details of the websites that you visit, you can use encrypted DNS.

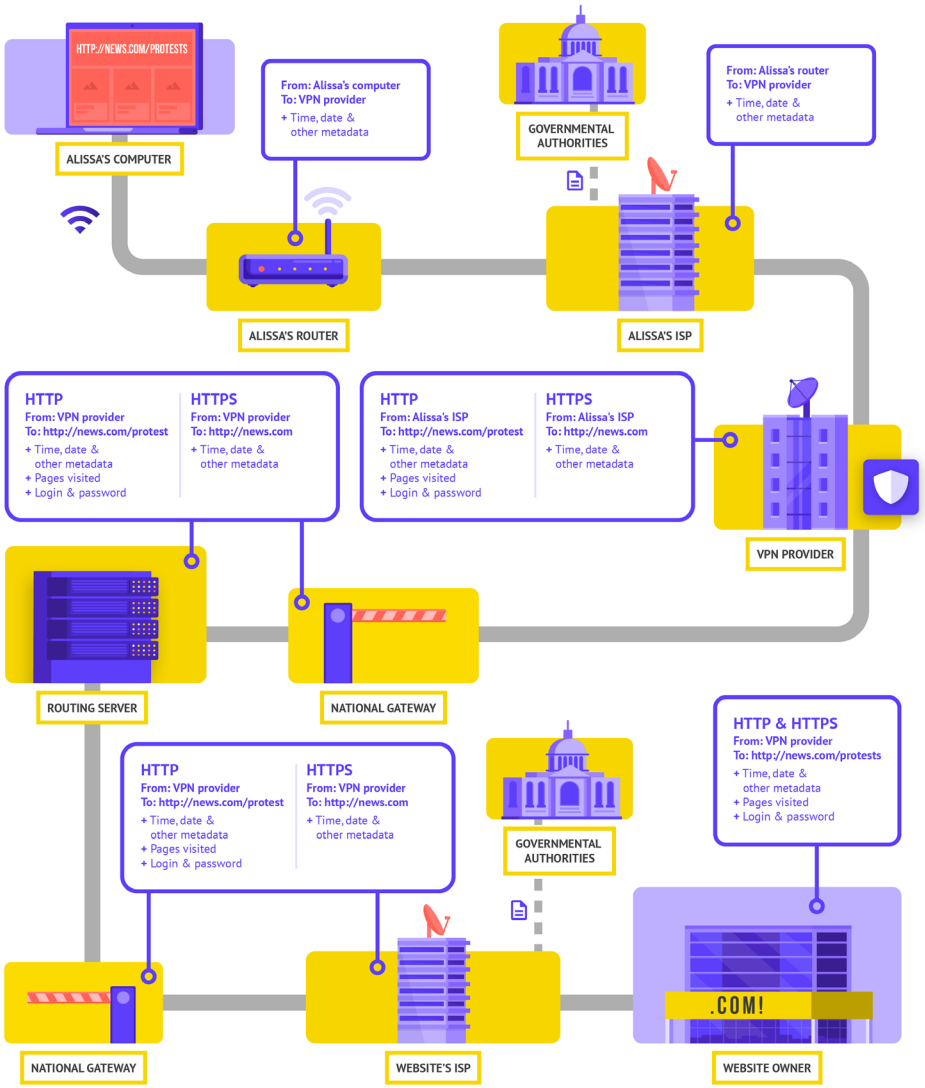
If you are **wondering**, DNS stands for Domain Name System. It is essentially the phonebook of the Internet, translating human-friendly domain names (like ndi.org) to web-friendly internet protocol (IP) addresses. This allows people to use web browsers to easily look up and load Internet resources and visit websites. By default though, DNS is not encrypted.

To use encrypted DNS and add a bit of protection to your internet traffic at the same time, one easy option is to download and turn on **Cloudflare's 1.1.1.1 app** on your computer and mobile device. Other encrypted DNS options, including Google's 8.8.8.8, are available but require **more technical steps** to configure. If you use Firefox browser, encrypted DNS is now turned on by default. Users of Chrome or Edge browsers **can turn on encrypted DNS** through the browser's advanced security settings by turning on "use secure DNS" and selecting "With: Cloudflare (1.1.1.1)" or the provider of their choice.

Cloudflare's 1.1.1.1 with WARP encrypts your DNS and encrypts your browsing data - providing a service similar to a traditional VPN. While WARP does not fully protect your location from all websites that you visit, it is an easy-to-use feature that can help your parliament's staff take advantage of encrypted DNS and additional protection from your ISP in situations where a full VPN is either not functional or required given the threat context. In the 1.1.1.1 with WARP advanced DNS settings, staff can also turn on 1.1.1.1 for Families to provide additional protection against malware while accessing the internet.

WHAT IS A VPN?

A VPN is essentially a tunnel that protects against the surveillance and blocking of your internet traffic from hackers on your network, your network administrator, your ISP, and anyone they might share data with. In a large organization - like a parliament - "business" or "corporate" VPNs are often used to help to protect the integrity of access to internal systems and applications (such as those used for remote voting) as well. Whether using a personal VPN or one designed for business purposes, the concept of protecting your internet traffic against snooping works generally the same, and it remains essential to continue using HTTPS (even with the VPN in place.) It is also critical to ensure that you trust the VPN that your parliament uses. Here is an example of what browsing with a VPN looks like:



Adapted from the Totem Project's How the Internet Works (CC–BY–NC–SA)

To describe VPNs in more depth, this section references EFF's [Surveillance Self-Defense Guide]:

Traditional VPNs are designed to disguise your actual network IP address and create an encrypted tunnel for the internet traffic between your computer (or phone or any networked "smart" device) and the VPN's server. Because traffic in the tunnel is encrypted and sent to your VPN, it is much harder for third parties like ISPs or hackers on public Wi-Fi to monitor, modify, or block your traffic. After going through the tunnel from you to the VPN, your traffic then leaves the VPN to its ultimate destination, masking your original IP address. This helps to disguise your physical location for anyone looking at traffic after it leaves the VPN. This offers you more privacy and security, but using a VPN does not make you completely anonymous online: your traffic is still visible to the operator of the VPN. Your ISP will also know that you are using a VPN, which might raise your risk profile.

This means that **choosing a trustworthy VPN provider is essential.** In some places like Iran, hostile governments have actually set up their own VPNs to be able to track what citizens are doing. To find the VPN that is right for your parliament and its staff, you can evaluate VPNs based on their business model and reputation, what data they do or do not collect, and of course the security of the tool itself.

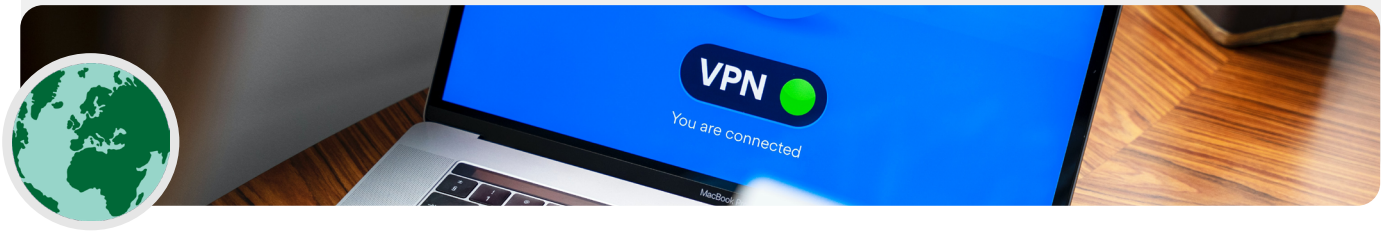
Why should you not just use a free VPN? The short answer is that most free VPNs, including those that come pre-installed on some smartphones, come with a big catch. Like all businesses and service providers, VPNs have to sustain themselves somehow. If the VPN does not sell its service, how is it keeping its business afloat? Does it solicit donations? Does it charge for premium services? Is it supported by charitable organizations or funders? Unfortunately, many free VPNs make their money by collecting and then selling your data.

A VPN provider that does not collect data in the first place is the best choice. If the data is not collected, it cannot be sold or handed over to a foreign government if requested. When looking through a VPN provider's privacy policy, see whether the VPN actually collects user data. If it does not explicitly state that user connection data is not being logged, chances are that it is. Even if a company claims not to log connection data, this may not always be a guarantee of good behavior.

It is worthwhile to do a search on the company behind the VPN. Is it endorsed by independent security professionals? Does the VPN have news articles written about it? Has it ever been caught misleading or lying to its customers? If the VPN was established by people known in the information security community, it is more likely to be trustworthy. Be skeptical of a VPN offering a service that no one wants to stake their reputation on, or one that is run by a company that no one knows about.

Fake VPNs in the Real World

In late 2017, following a surge in protests in the country, [Iranians started discovering a "free" (but fake) version of a popular VPN being shared via text messages]. The free VPN (which did not actually work) promised to grant access to Telegram, which at that time was blocked locally. Unfortunately the fake application was nothing more than malware that allowed authorities to track the movement and monitor the communications of those who downloaded it.



So what VPN should we use?

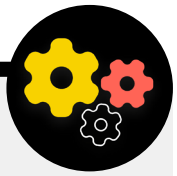
If, in addition to ensuring the security of parliamentary internet traffic, you also need a solution to securely limit access to only those on your parliamentary network (even while working remotely) to internal parliamentary systems and applications, you may want to implement a "business" or "corporate" VPN. A range of options using varying technologies exist that you may consider, including Cisco's **AnyConnect**, PaloAlto's **Global Protect**, or Cloudflare's **Access** (technically a Zero Trust Access System, not a VPN) just to name a few. Either way, such systems require skilled IT staff to implement and effectively manage.

If an advanced "corporate" VPN system is either out of budget or unnecessarily complicated for your parliament, you can also consider using personal VPN options like **ProtonVPN** or **TunnelBear** (which also offers a Teams plan to make account management simpler) for all parliamentary members and staff.

Another trustworthy option is to configure your own server using Jigsaw's **Outline**, where there is not a company managing your account, but in return, you have to set up your own server.

Although most modern VPNs have improved in regard to performance and speed, it is worth keeping in mind that using a VPN might slow down your browsing speed if you are on a very low-bandwidth network, suffer from high latency or network delays, or experience intermittent internet outages. If you are on a faster network, you should default to using a VPN all the time.

If you do recommend that staff use a VPN, it is also important to ensure that people keep the VPN turned on. It might sound obvious, but a VPN that is installed but not running does not provide any protection.



Anonymity through Tor

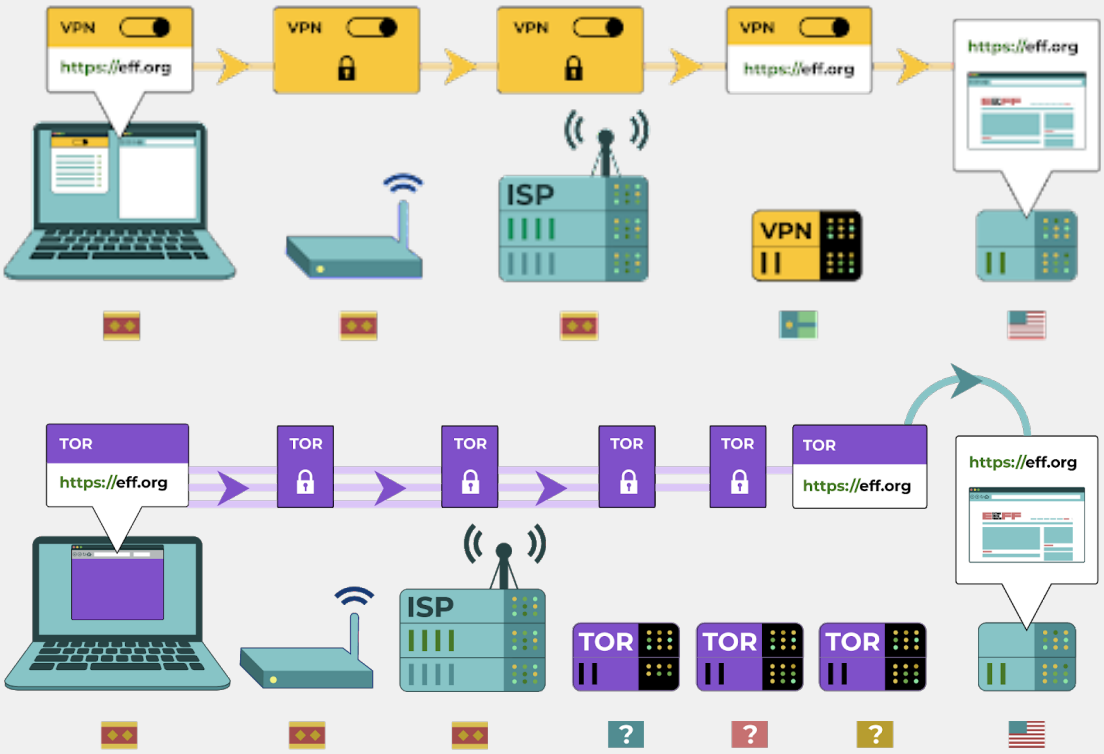
In addition to VPNs, you may have heard of Tor as another tool for more securely using the internet. It is important to understand what both are, and why you might use one or the other.

Tor is a protocol for transmitting data anonymously over the internet by routing messages or data through a decentralized network. You can learn more about how Tor works **here**, but in short, it routes your traffic through multiple points along the way to its destination so that no single point has enough information to expose who you are and what you are doing online at once.

Tor is different from a VPN in a few ways. Most fundamentally, it differs because it does not rely on the trust of any one specific point (like a VPN provider).
This graphic, developed by EFF, shows the difference between a traditional VPN and Tor.

The easiest way to use Tor is through the **Tor web browser**. It operates like any normal browser except that it routes your traffic through the Tor network. You can download the Tor browser on Windows, Mac, Linux or Android devices. Keep in mind that when using Tor Browser, you are only protecting the information you access **while in the browser.** It does not provide any protection to other apps or downloaded files that you might open separately on your device. Also keep in mind that Tor does not encrypt your traffic, so - much like when using a VPN - it is still essential to use best practices like HTTPS when browsing.

If you would like to extend the anonymity protections of Tor to your entire computer, more tech savvy users can install Tor as a systemwide internet connection, or consider using the **Tails** operating system, which routes all traffic through Tor by default. Android users can also use the **Orbot** app to run Tor for all internet traffic and apps on their device. Regardless of how you use Tor, it is important to know that



when using it, your internet service provider cannot see what websites you are visiting but they *can* see that you are using Tor itself. Much like when using a VPN, this could raise your risk profile considerably, because Tor is not a very common tool and therefore stands out to adversaries that may be monitoring your internet traffic.

So, while there are likely very few instances where Tor would be necessary to use within a parliamentary context, if you either cannot afford a trustworthy VPN or find your parliament operating in an environment where VPNs are routinely blocked, Tor can be a good option, if legal, for limiting the impact of surveillance and avoiding censorship online.

Are there any reasons we should not use a VPN or Tor?

Apart from concerns around non-reputable VPN services, the biggest thing to consider is whether using a VPN or Tor might attract unwanted attention or, locally, be against the law. Although your ISP will not know what sites you are visiting while using these services, they can see that you are connected to Tor or a VPN. If that is illegal where your parliament or its staff operate or might cause more attention or risk than simply navigating the web with standard HTTPS and encrypted DNS, perhaps a VPN or especially Tor (which is much less commonly used and therefore a bigger "red flag") is not the right choice.

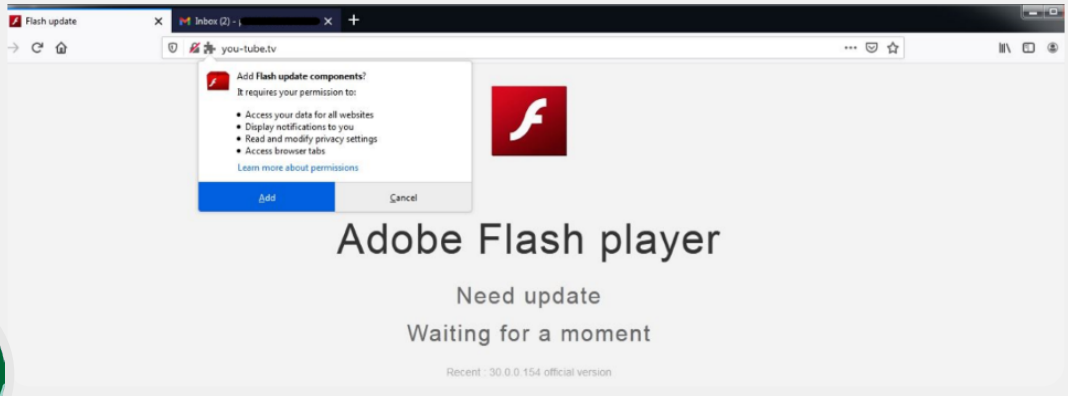
WHAT BROWSER SHOULD WE BE USING?

Use a reputable browser such as Chrome, Firefox, Brave, Safari, Edge, or Tor Browser. Both Chrome and Firefox are very widely used and do a great job with security. Some people prefer Firefox given its privacy focus. Either way, it is important that you restart them and your computer relatively frequently to keep your browser up to date. If you are interested in comparing browser features, check out this resource from the Freedom of the Press Foundation. Regardless of browser, it is also a good idea to use an extension or add-on like Privacy Badger, uBlock Origin, or DuckDuckGo's Privacy Essentials that stops advertisers and other third-party trackers from tracking where you go and what sites you visit. And when browsing the internet, consider switching your default web searches away from Google to DuckDuckGo, Startpage, or another privacy-protecting search engine. Such a switch will help limit advertisers and third-party trackers as well.

Browser Security in the Real World

Browser extension or add-on attacks can be just as damaging as malware shared directly through phishing downloads or other software. For example, a cleverly designed malicious add-on titled "Flash update components" targeted Tibetan political organizations in early 2021. The add-on was presented to users who visited websites linked to phishing emails, and when installed, it enabled hackers to steal email and browsing data.

Browser add-ons can also be a vector for infecting parliamentary resources such as websites, which in turn can spread malware to a wide range of site visitors (including the general public, parliamentary staff and members themselves). Take, for example, hackers' exploitation of the popular browser add-on Browsealoud (now known as ReachDeck), a program that converts website text to audio for visually impaired users. In 2018, hackers inserted malicious code into the browser add-on, which had been in use on websites of various government entities, including the state of Victoria's parliament in Australia. With the infected browser add-on in place and improperly configured, website visitors' devices were infected with malware upon visiting the site. In this case, the malware was used to leverage the devices to mine cryptocurrency, but such tactics could be used by hackers to spread malware for the purposes of data theft or espionage as well.



Social Media Safety

Parliamentary staff and MPs can reveal a lot – and sometimes more than they intend – by posting and commenting on social media.

Whether it is Facebook, Twitter, Instagram, YouTube or region-specific social media sites such as VKontakte and Odnoklassniki, you should always think carefully about what you post, and properly configure any privacy settings that may be available. This is true not only for parliaments' official pages, but also in some cases for staffs' personal accounts and those of their family and friends too.

Social Media Security and Parliaments

Even low risk organizations can be targeted and harassed on social media without proper security policies in place. In this example from 2018, a non-profit animal shelter lost thousands of dollars and alienated supporters after an unauthorized account administrator set up a fake fundraising effort, and fake accounts impersonating employees appeared on the platform. If hackers will go to those lengths to make a few thousand dollars off of an animal shelter, you can imagine the damage sophisticated adversaries might be able to inflict if they were to gain access to your parliament's accounts or successfully impersonate a prominent MP or staff person online.

In addition to hacking social media accounts, parliament's websites are also common targets given their public visibility and reputational significance. In one example from 2017, Austria's parliamentary website was taken down by a hacking group that was supposedly angry at the country's souring relations with Turkey at the time.

DEVELOP A PARLIAMENTARY SOCIAL MEDIA POLICY

Assume that anything posted on social media could become public knowledge, and craft a parliamentary social media policy accordingly. Given the public nature of most parliamentary work, it's likely that you will want to share most posts and messages publicly, but it is still crucial to ask and answer questions such as: Who has access to your social media accounts? Who is allowed to post and who needs to approve posts? What about comments and replies? What information should/should not be shared on social media? If you post photos, location information, or other identifying information about your staff, members, or partners have you asked for their permission, and have they considered any possible risks? Such questions are especially important if your parliament engages publicly with citizens through social media or similar online portals for public engagement.

In addition to developing your policy and making it clear to staff, be sure to properly configure your privacy and security (often referred to as "safety") settings. Some key questions to ask yourself as you decide what privacy and safety settings make the most sense for parliamentary and personal accounts, include:

- Do you want to share your posts with the public, or only with a specific group of people internally or externally?
- Should anybody be able to comment, reply, or interact with your messages or posts?
- Should people be able to find you using your email address or (personal or professional) phone number?
- Do you want your location shared automatically when you post?
- Do you want to block or mute hostile accounts?
- Do you want to block specific words or hashtags?

Each social media site will have different privacy and safety settings, but these general concepts apply universally. As you consider these questions, take advantage of helpful privacy guides from the major platforms: **Facebook**, **Twitter**, **Instagram**, and **YouTube**. For Facebook in particular, be cautious about your privacy choices regarding Groups. Facebook Groups are a popular spot for engagement, advocacy, and information sharing, but unrestricted groups can be joined by anyone. It is not uncommon for "fake" accounts to pose as real people in an effort to infiltrate private social media groups or pages. Therefore, accept "friend" and "follow" requests carefully.

Remember that your parliament's social media accounts are only as secure as the accounts that are "linked" to it. This is especially important to remember for Facebook, where your pages may be managed by someone's linked personal account.

ONLINE HARASSMENT

Unfortunately, many parliaments and affiliated groups face significant harassment online, especially on social media. Such harassment is **often directed with even more intensity at women and marginalized populations.** Online violence against women in particular can create a hostile environment that leads to self-censorship or withdrawal from political or civic discourse. As identified in NDI's Gender, Women, and Democracy team's **Tweets That Chill** report, when attacks against politically active women are channeled online, the expansive reach of social media can magnify the effect of harassment and psychological abuse, undermining women's sense of personal security in ways not experienced by men.

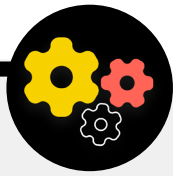
As your parliament develops its social media policy, it is important to be cognizant of these dynamics. Build into your security plan structured support for members and staff who face negative messages, insults, and threats on social media, both as part of their jobs and in their personal lives. Develop an anti-harassment infrastructure within parliament, including surveying your staff to understand how online harassment impacts them and create a rapid response team to help staff face challenging situations. PEN America's **Online Harassment Field Manual** also provides detailed recommendations on how you can support staff who face such harassment. You might consider, if your staff are comfortable doing so, **reporting incidents** of harassment and/or problematic accounts directly to the platforms as well.

When engaging with members or staff who have been the victim of harassment online (and in the physical world as well), it is important to be sensitive. As outlined by the Association for Progressive Communications' Women's Rights Programme's **Take Back the Tech**, understand that a survivor may be dealing with trauma, and recognize that violence (online or offline) is never the fault of the survivor. Ensure such issues can be raised and discussed (if staff are comfortable doing so) in a confidential and safe environment, with the option of anonymity. And include in your parliament's security plan a list of local professionals, organisations, and law enforcement agencies that you can connect staff to for legal, medical, mental health, and technical assistance if needed. For additional ideas, check out Feminist Frequency's **Online Safety Guide**.

Keep your Websites Online

In addition to protecting your ability to access the internet safely, it is also important to do what you can to ensure others can access your parliament's websites or web properties.

For social media pages, this means protecting those accounts with strong, unique passwords and two-factor authentication. For your website, this means protecting it against hacking and denial of service attacks. Distributed Denial of Service (DDoS) attacks are where a large group of computers simultaneously drown your server in malicious traffic. A few options for DDoS protection - which makes it much harder for an adversary to take your website down - include Cloudflare, Amazon's AWS Shield, or eQualitie's Deflect service.



Hosting Your Parliament's Website Securely

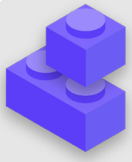
Websites are hosted on computers - and those are vulnerable to hacking just like your own devices. If possible, your parliament should take advantage of existing hosting services like WordPress, Wix, or others that manage all the site security for you. If your website needs are more complex and/or you need to host your website yourself, then be sure to focus on keeping your operating system and web hosting software up to date, just like you would for your personal computer. Consider using well-established cloud hosting providers such as Amazon Web Services (AWS), Microsoft Azure, or Greenhost's eclips.is, which provide enhanced security options for hosted websites. Regardless of what tools you use to host your website, ensure that any accounts used to access content editing and configuration settings are protected with strong passwords and two-factor authentication.

If your parliament has the technical savvy to host its own website, you should consider choosing a so-called "static-site" or flat website. As opposed to dynamic websites, these types of sites reduce the attack surface for hackers and will make your website more attack resistant.

Protect your WiFi Network

All these steps to protect web traffic from surveillance and censorship are important, but they are not a substitute for basic network security in parliament and at home.

Do not forget the basics like using a strong password (not the default password) on your Wi-Fi router(s), ensuring that only authorized users have access to your network by frequently changing the password, and enabling your wireless routers' built-in firewall. Consider creating a guest network on parliamentary premises as well if you have visitors coming in and out of the building who use the internet.



Staying Safe on the Internet

- **Conduct regular training for members and staff on the importance of following basic web security measures.**
- **Remind staff to always browse with HTTPS and encrypted DNS.**
- **Require staff to regularly restart their browsers to install updates.**
- **Encourage the use of privacy protecting browsers and extensions.**
- **If a VPN is appropriate, choose a reputable one, train staff on its use, and ensure it is consistently used.**
- **Develop and distribute a clear parliamentary policy on social media use.**
- **Enable privacy and security settings on all social media accounts.**
- **Understand the impacts of online harassment and be prepared to support members and staff who are affected.**
- **Develop a list of local professionals, organizations, and law enforcement agencies that you can connect members and staff to for legal, mental health, and technical assistance in response to online harassment.**
- **Sign up for DDOS protection for your websites.**
- **Use a trusted, reliable web hosting provider.**
- **Use a strong password and a guest network for your on-premises Wi-Fi.**

Protecting Physical Security

It is essential to keep your devices physically secure. Keep in mind that physical security goes beyond just devices, and should include strategies to protect everything else in your world. This includes hard-copy documents; parliament's offices; chambers, or work spaces; and of course you, your staff, and members.

Physical Security and Parliament

Unfortunately, physical attacks on parliaments and other legislative bodies are not uncommon, and often have significant implications for both physical and information security. On January 6, 2021, insurrectionists stormed the United States' Capitol Building - home to both houses of the U.S. legislature - in an effort to stop the certification of presidential election results. The physical attack tragically led to five deaths and caused significant psychological distress for Congressional members and staff. However that was not the only negative impact. The attackers also destroyed IT equipment, gained access to sensitive materials in members' offices and perhaps most damagingly, stole computers and other devices with potentially confidential information from the U.S. Capitol.

Sensitive Compartmented Information Facilities (SCIFs)

To hold highly sensitive conversations, some parliaments have secured physical rooms called SCIFs in place. These spaces are established so that sensitive information, such as issues related to national security or intelligence, can be viewed by and discussed between MPs and their staff without concern of outside surveillance or spying. In addition to proper physical construction, a proper SCIF necessitates that people leave devices (such as their cell phones) outside the room prior to entering for discussion.

Protecting Physical Assets

An essential component of information security is the physical security of your devices.

In addition to mitigating the impact of a stolen device by using lockscreens and passwords, implementing full disk encryption, and turning on remote wipe features, you should also consider how to keep those devices from being stolen in the first place. To make theft more difficult, be sure to install strong locks (and rotate them whenever staff change) at parliamentary premises and/or home. In addition, consider buying a laptop safe or lockable cabinet to keep devices protected overnight. Security cameras or motion sensor systems around the premises can detect and hopefully deter physical break-ins and theft. Look for a privacy-respecting option available in your country, and be sure to select cameras and security systems provided by trusted companies that do not have an incentive to hand over data and information to a potential adversary.

If old devices have information still stored on them but are no longer in use, consider wiping them - this guide from Wirecutter is a great resource on how to do this for most modern devices. If wiping your devices is not possible, you can physically destroy them too. The easiest, if not most environmentally sensitive, way to do that is to break up the devices and their hard drives with a hammer. Sometimes the oldest solutions still work the best!

Even before these technical steps, take a moment to create an inventory of all the equipment across parliament. If you do not have a list of all your devices, it is harder to keep track of what might be missing if one gets stolen.

WHAT DO WE DO WITH ALL THIS PAPER?

It is likely that your parliament has a lot of information that is printed on paper, written in notebooks, or scribbled down on Post-it notes. Some of this can be very sensitive - notes from confidential testimony or private meetings, for example. It is essential to think about the security of this information as well. If you absolutely need to keep hard copies of sensitive information, ensure that it is stored safely in a locked cabinet or another safe place. Do not keep any private or sensitive information (including passwords) laying around on a desk or written up on a white-board. Keep highly sensitive information in a less targeted, well protected location.

To the extent possible, endeavor to dispose of unneeded hard-copy information. Remember: if you do not have it, it cannot be stolen. Set a parliamentary policy regarding ownership of hard-copy notes, and be sure to collect any paper notes from staff if they decide to leave or are let go from the organization, just like you would collect a parliament-issued computer or phone. To get rid of sensitive paper, purchase a quality shredder. A fun end-of-week activity can be taking a 15-minute break with your teams to shred any leftover, sensitive print-outs or notes from the prior week.

THE PARLIAMENTARY POLICY

Although for many the realities of "the office" have changed significantly since the beginning of the COVID-19 pandemic, it is still important for your parliament to set a clear policy regarding access to the premises. Such a policy should address key questions including who is allowed inside the parliamentary premises (and when), who can access what office resources (like the WiFi network), and what to do about guests.

A simple yet important question to answer is who gets an office key or access badge. Only trusted staff should have keys or badges, and locks should be changed when staff leave and/or on a semi-regular basis. During the day, any doors that are left unlocked should be in constant view of someone trusted and/or a security guard. In addition, ensure that your parliament has a trusted relationship with service providers such as cleaning staff and external technicians that have access to the premises. Think about what information or devices such people might have access to and ensure that it is protected, particularly if you do not have that trusted relationship. Whoever has access, someone trusted should always be designated to lock up offices and buildings and ensure devices are properly secured before leaving at the end of the day.

Are constituents allowed inside your parliament? Perhaps the public has a right to access parts of the parliamentary premises? If so, ensure they do not have access (or at least unattended access) to devices or sensitive hard-copy data. If it is a requirement or expectation that the visiting public or guests have internet access when they visit, you should set up a "guest" network so that such guests do not have the ability to monitor your regular traffic.
In general, only trusted personnel should be able to access the network and network devices such as printers. It is also usually a good idea to require guest registration so that you have a log of who has visited.

As you develop an office policy, the goal should be to allow only trusted people access to sensitive devices, documents, spaces, and systems.

SUPPORTING STAFF AND VOLUNTEERS

Physical security threats to your parliament can impact your staff too. Similar to harassment on social media, these physical security threats often disproportionately impact women and marginalized communities. It is not just about broken windows and stolen laptops. Intimidation, threats or instances of physical or sexual violence, domestic abuse, and fear of attack can have a serious negative impact on the lives of members and staff. NDI's **#Think10** Safety Planning Tool is a useful resource to provide to politically active women who might be at increased personal risk as a result of their participation in parliament and politics more generally.

The well-being of staff is obviously an important asset to them as individuals, but it is also a crucial element to a healthy and well-functioning parliament. To that end, consider what additional resources you can provide to staff to keep them protected and, in the case of physical or digital attack, help them recover. As mentioned earlier in the Handbook, this means at a bare minimum developing a list of resources that you can connect staff to for legal, medical, mental health, and technical assistance if needed. Once again PEN America's **Online Field Harassment Manual** includes ideas for how organizations can support staff during and after crises.

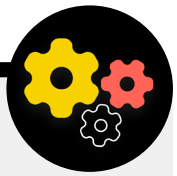
SECURITY WHILE TRAVELING

Traveling - whether to another country or the town down the road - often intensifies physical information security risks. It is generally safe to assume that you and your devices have no privacy rights when crossing borders. As such, it is a good idea to include parliamentary travel policy within your security plan that includes reminders about key security best practices.
Your parliament's travel policy should include a lot of the information covered in other sections of the Handbook including using the internet securely and keeping devices and other information sources physically secure and with you at all times when travelling. If possible, leave your sensitive information behind and just use a fresh, cleanly erased computer, access the files you absolutely need from the cloud, and then erase it when getting home again.

In addition to preparing for travel and minimizing the data shared when you do travel, there are a few essential operational tips that you should think through and include in your parliamentary travel policy.

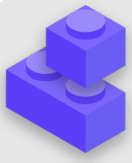
Consider using travel-specific laptops or phones that have little to no sensitive data stored on them. If most of your parliament's work is done in the cloud, a relatively inexpensive Chromebook can be a good option for such a device. Factory reset, or "wipe", these devices upon their return before connecting to common WiFi networks at home or the office.
Provide staff with contact information and a plan of action for what they should do if something goes wrong on their trip. This includes information about local hospitals, clinics, or pharmacies should they need medical assistance while travelling.

Staff should also keep all devices on their person while travelling. For example, keep your laptop at your feet (not the overhead compartment or in checked luggage) when on a bus, train, or plane. Do not assume a hotel room – or even the hotel safe – is a "safe place" to keep sensitive devices and items. Do not trust public USB charging ports. USB charging ports in airports, stations, and vehicles are becoming an increasingly common sight, and a very convenient way to power up devices. However, they can be an easy vector for picking up malware. So be sure to either charge devices the traditional way through a plug in the wall, or purchase **USB data blockers** to allow travelling staff to safely charge up their devices via USB.



Booking Travel Securely for Your Parliament

When putting together a travel policy, keep in mind what information might be exposed when you organize or book travel. This can be particularly important if you are organizing large events, or conferences for which you are handling sensitive information from a variety of staff, members, or attendees. Think carefully about how you will securely share and store (if needed) personal information like passport details, travel itineraries, and medical records.



Protecting your Physical Security

- **Remind members and staff to keep devices physically protected at all times.**
- **Check and secure all the ways people can get onto your premises.**
- **Develop a guest and access policy.**
- **Use strong locks, ID/badge systems, and rotate/change them when needed.**
- **Consider setting up cameras or other on-premises security systems.**
- **Have and use paper shredders.**
  - Set up dedicated staff time to dispose of hard-copy documents that contain sensitive information.
- **Develop a list of local professionals, organisations, and law enforcement agencies that you can connect members and staff to for legal, medical, and mental health assistance in response to physical attacks or threats.**
- **Develop a parlamentary travel policy.**
- **Ensure staff know what to do in case of emergency during travel.**
- **Be mindful of the additional data that is created and shared when organizing travel or events.**

What To Do When Things Go Wrong

So, you know the right things to do. You have put the policies in place and trained everybody across parliament on all the best practices. Even with all this hard work, it is very likely that something will eventually go wrong.

Stuff happens. When it does, it is essential to have an incident response plan in place. Incident response is a crucial, and often underrated, part of your parliament's security plan because it can be the difference between an attack destroying your reputation or being an unpleasant bump in the road. Keep in mind that you can only respond to an incident if you know about it. Having a strong security culture and encouraging members and staff to report problems is very important. This is why it is better to reward good security behavior rather than punish security lapses or mistakes. It is also important to express empathy and check on the wellbeing of staff when they report an incident. You want staff to immediately report a clicked link in a phishing message, a stolen phone, or a hacked social media account - not hesitate for fear of retribution or lack of support. After all, incident response, just like the mitigation strategies mentioned in other sections of the Handbook, is a parliament-wide effort.

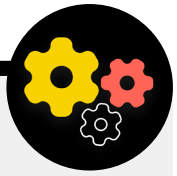
What should you plan for? In short, anything that is somewhat likely to happen. That will look different for every parliament, but common questions that an incident response plan will help answer include:

- What do we do if our accounts or websites get hacked?
- What do we do if someone clicks on a phishing email or if a device is acting suspiciously?
- What do we do if our emails or most sensitive documents are stolen and leaked?
- What do we do if one of our staff is put in physical danger? Or if they are struggling with stress and anxiety due to such threats?
- What do we do if our office is damaged in a fire, flood, or natural disaster?
- What do we do if a member's computer or phone is lost or stolen?

The answers to these questions and others will differ by parliament, but it is important to think through them together and clearly articulate and share a plan so that everyone is prepared to take action immediately to limit the damage.

Borrowing from Tactical Tech's Holistic Security Guide, a good place to start with an incident response plan is **defining an incident or an emergency** in the context of your parliament. Decide what an "emergency" is – i.e, the point at which we should begin to implement the actions and contingency measures planned. This is important as sometimes it will be unclear – if you imagine a scenario such as losing contact with a colleague on a field mission; how long would you wait before declaring an emergency? One does not want to jump too early, but waiting too long can in some circumstances be disastrous. It is also important to think through any **operations** steps as well. Assign each person a clear role that they are aware of and have agreed to in advance – this will reduce disorganisation and panic in the event of an incident. In the case of each threat, consider the different roles that you may have to assume and the practicalities involved in responding to an emergency. Within this important strategy for emergencies is the activation of a support network – a broad network of allies, which may include different branches of your own government, other friendly governments, technology companies, security vendors, and multilateral institutions to name just a few examples. How can your allies support you? Should you contact them in advance to verify that they will be willing to help you in an emergency and let them know what you expect of them?

When responding to an incident, effective **communications** become increasingly important. Decide what the most secure and effective means of communicating with each actor is in different scenarios and identify a back up means. Be aware that for emergencies, it might be useful to have clear guidelines on what to (and what not to) communicate, when to communicate, which channels to use to communicate, and with whom you should communicate. Also, consider the reputational impact of an incident on your parliament, and be prepared to respond accordingly. Make sure that the parliament's communications lead is aware of the incident and can watch social media or other media for potential impact. They should also be prepared to field possible public or media inquiries about an incident if relevant. This is especially important for getting ahead of any potential negative stories or reputational damage. While every incident and context is different, honest and transparent communications often help build trust in the aftermath of an incident.



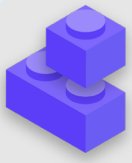
Creating an Early Alert and Response System

Consider establishing an Early Alert and Response System. Such a system sounds fancy, but it is essentially just a centralised document (electronic or otherwise) to be opened in the event of an emergency. In the document, you should record all the details about the security indicators and incidents which have occurred on a timeline, provide a clear description of the actions and sequence for the planned response, and indicate what needs to be achieved to signify that the risk has once again decreased. It should also include actions to be taken after an incident in order to protect those involved from further harm and help them to recover physically and emotionally. An Early Alert and Response System can provide useful documentation for sharing with law enforcement (if applicable), subsequent analysis of what has happened, and guidance on how to improve your prevention tactics and responses to threats in the future.

In addition to these important incident response concepts, your parliament should also prepare for any specific **technical** response. In some cases a technical response can be managed by internal IT staff or system administrators. For example, if an email account appears to have been hacked, your account administrator should be prepared and able to shut down or disable the impacted account. Some technical incidents, however, might require expertise that you do not have within your parliament. For situations like these, it is important to identify a trusted list of external technical experts who can assist you in your incident response. In some cases, you may want to pre-negotiate terms with service providers (such as your website host or an IT security firm) to ensure that they are available (and would not charge extra) for such technical incident response.

Last but certainly not least, you should consider **legal** steps. Understanding the legal protections you might have, as well as the legal obligations or consequences your parliament might face as a result of a data breach or other security incident, is important. As a parliament, you are in a position of particular power and prominence when it comes to both understanding and respecting local data security and privacy regulations. Take time to review possible incidents with relevant legal counsel if necessary and make a plan for what you would do in response. It is a good idea to make an agreement with this trusted counsel to represent you and your interests if needed in the aftermath of an incident. As part of this legal preparation, make sure that you understand the legal obligations of any vendors or partners. Are they required to notify you in the case of their own data breach? What support (if any) are they required to provide you in the case of an incident? As you develop contracts and agreements with external vendors, keep the possibility of a data breach or other incident in mind.

While there is no one-size-fits-all approach to incident response, having clear operational, communications, technical, and legal plans in place is essential. As you put together your incident response plan, we strongly encourage you to make use of some excellent existing resources, designed to help organizations navigate incident response. Although not all of these resources are designed specifically for parliaments, their content is still very relevant. These resources include the Digital First Aid Kit developed by Rarenet and CiviCERT, PEN America's Online Harassment Field Manual, the Belfer Center's Cybersecurity Campaign Playbook and Cyber Incident Communications Plan Template, and Access Now's Digital Security Helpline.



Incident Response

- **Develop a parliamentary incident response plan, and practice it.**
  - Brainstorm possible incidents and prepare for your response before it happens.
- **Ensure everyone across parliament is aware of how you will communicate and what technical steps will be taken in the case of an incident.**
- **Take time to understand your legal protections and obligations.**
- **Be prepared to provide members and staff the emotional and social support they need in the aftermath of an incident.**

Appendix A: Recommended Resources

- Tactical Tech's Holistic Security Manual ; Creative Commons Attribution-ShareAlike 4.0 International License
  - Chapter 2.4 - Understanding and Cataloguing Our Information
  - Chapter 1.5 - Communicating About Threats in Teams and Organizations
  - Chapter 3.4 - Security in Groups and Organizations
- The Electronic Frontier Foundation's Security Education Companion ; Creative Commons Attribution 3.0 US License
  - Threat Modeling Activity Handout
- Freedom of the Press Foundation's Phishing Prevention and Email Hygiene Guide ; Creative Commons Attribution 4.0 International License
- Freedom of the Press Foundation's Locking Down Signal Guide ; Creative Commons Attribution 4.0 International License
- Electronic Frontier Foundation's Surveillance Self-Defense (SSD) Guide ; Creative Commons Attribution 3.0 US License
  - What Should I Know About Encryption
  - Communicating with Others
  - Choosing the VPN That's Right for You
- Front Line Defenders' Guide to Secure Group Chat and Conferencing Tools
- Tactical Tech's Data Detox Kit
  - Let the Right One In: Make Your Passwords Stronger
  - Strengthen Your Screen Locks
- Center for Democracy & Technology's Elections Security Guide on Passwords ; Creative Commons Attribution 4.0 International License
- Center for Democracy and Technology's Elections Security Guide on Two Factor Authentication ; Creative Commons Attribution 4.0 International License
- Martin Shelton's Two Factor Authentication for Beginners ; Creative Commons Attribution 4.0 International License
- Tactical Tech and Frontline Defender's Security in a Box ; Creative Commons Attribution-ShareAlike 3.0 Unported License
  - Protect your device from malware and phishing attacks
  - Protect against physical threats
- SANS' OUCH! Newsletter: Stop That Malware
- Apple's Device and Data Access When Personal Safety is at Risk
- Global Cyber Alliance Cybersecurity Toolkit for Mission-Based Organizations
- Ford Foundation's Cybersecurity Assessment Tool

Appendix B: Security Plan Starter Kit

Use the following starter kit to take notes as you and your parliament read through the Handbook and digest the material, and consider the accompanying questions with your colleagues to help generate productive discussion.

Be sure to reference the key "building blocks" in each section of the Handbook to ensure that you are covering the important topics as you build your security plan. By the end of the Handbook, the building blocks, answers to these discussion questions, and your notes should form the foundation of a successful security plan.

Building a Culture of Security

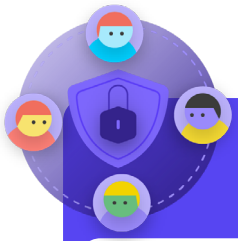
A Strong Foundation: Securing Accounts and Devices

Communicating Data Securely

Staying Safe on the Internet

Protecting Physical Security

What To Do When Things Go Wrong



Building a Culture of Security

QUESTIONS TO CONSIDER:

- When can you schedule a conversation to review your security plan with the entire parliament?
- What days or times work well for the parliament to schedule regular conversations and training about security?
- What steps can leadership take to model good security behavior and a commitment to a security plan? How can others in the parliament play a role in security?

YOUR NOTES AND IDEAS:

A Strong Foundation: Securing Accounts and Devices

QUESTIONS TO CONSIDER:

- How will you implement account security measures - like a password manager and 2FA - across parliament? What obstacles might you encounter during implementation?
- How will your parliament ensure that devices are kept secure and updated? As part of this, will the parliament need a plan to address unlicensed software or computers?
- When is a good time to set up training for all staff on the dangers of phishing, malware, and device security best practices?

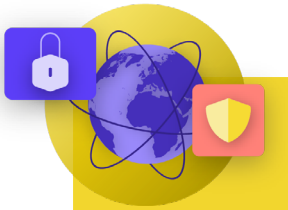
YOUR NOTES AND IDEAS:

Communicating and Storing Data Securely

QUESTIONS TO CONSIDER:

- How will your parliament implement end-to-end encrypted messaging for secure communication? What obstacles might you encounter during implementation?
- How will your parliament enforce a secure file sharing solution both internally and externally? What obstacles might you encounter during implementation?
- How will your parliament implement a secure data storage and backup solution? What obstacles might you encounter during implementation?

YOUR NOTES AND IDEAS:



Staying Safe on the Internet

QUESTIONS TO CONSIDER:

- How will your parliament implement secure browsing requirements such as HTTPS, a trusted browser, and, if appropriate, a VPN for staff?
- What will be the key elements of your parliament's social media policy? How will it be enforced?
- How will your parliament protect its websites and web properties?

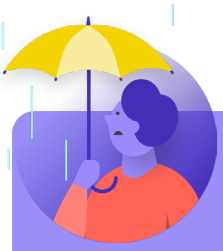
YOUR NOTES AND IDEAS:

Protecting Physical Security

QUESTIONS TO CONSIDER:

- How will the parliament distribute and enforce its office guest and access policy?
- Who is responsible for preparing staff for the physical and digital security challenges that they might face while on travel for work?
- What steps can staff take to keep their devices safe and secure both at the office and while on travel?

YOUR NOTES AND IDEAS:



What to Do When Things Go Wrong

QUESTIONS TO CONSIDER:

- How will the parliament distribute and practice its incident response policy?
- Are there resources available for staff who might need emotional and social support in the aftermath of an incident? If not, how might the parliament be able to provide those resources in case of an incident?

YOUR NOTES AND IDEAS:

Appendix C: Image Citations

Page 14: New York Times, "Australian Parliament Reports Cyberattack on Its Computer Network", 2019, digital image, Getty Images, https://www.nytimes.com/2019/02/07/world/australia/cyberattack-parliament-hack.html.
Page 18: CNP Collection, "Security Protection Anti-Virus Software cms", 2014, digital image, Alamy Stock Photo, https://www.alamy.com/security-protection-anti-virus-software-cms-image67114038.html?irclickid=2oWTxrXnOxyIRKXzgq3HowdNUkDzCPSFpyViRI0&utm_source=77643&utm_campaign=Shop%20Royalty%20Free%20at%20Alamy&utm_medium=impact&irgwc=1.
Page 24: Bleeping Computers, "Norway parliament data stolen in Microsoft Exchange attack", 2021, digital image, https://www.bleepstatic.com/content/hl-images/2021/03/10/storting.jpg.
Page 25: Cottonbro, "Person Holding Black and Silver Key", 2020, digital image, Pexels, https://www.pexels.com/photo/person-holding-black-and-silver-key-5474292/?utm_content=attributionCopyText&utm_medium=referral&utm_source=pexels.
Page 27: Blogtrepreneur, "Malware Infection", 2016, digital image, Flickr, https://www.flickr.com/photos/143601516@N03/.
Page 30: "Microsoft Loading Screen," digital image, Kompass, September 23, 2019, https://asset.kompass.com/crops/kYVdzylbrYB5lIpuKDDwJLNFMV4=/164x49:679x393/750x500/data/photo/2018/07/02/4208974652.png.
Page 30: Mateuz Dach, "Turned-on iPhone and Displaying Icons," 2017, digital image, Pexels, https://www.pexels.com/photo/turned-on-iphone-and-displaying-icons-365194/.
Page 33: ZDNet, "Chinese hacking group impersonates Afghan president to infiltrate government agencies," 2021, digital image, https://www.zdnet.com/article/chinese-hacking-group-impersonates-afghan-president-to-infiltrate-government-agencies/
Page 38: Andrew Keymaster, "People Gathering on Street During Daytime Photo," 2020, digital image, Unsplash, https://unsplash.com/photos/JXQ2bizu7kc.
Page 39: Surveillance Self-Defense, "No Encryption in Transit," digital image, Electronic Frontier Foundation, January 17, 2019. https://ssd.eff.org/en/module/what-should-i-know-about-encryption.
Page 40: Surveillance Self-Defense, "4.Transport-layer-alternate," digital image, Electronic Frontier Foundation, January 17, 2019, https://ssd.Surveillance Self-Defense.org/files/2018/11/26/4.transport-layer-alternate.png. ; Surveillance Self-Defense, "6. End-to-end Alternate", digital image, Electronic Frontier Foundation, January 17, 2019, https://ssd.Surveillance Self-Defense.org/files/2018/11/26/6.end-to-end-alternate.png.
Page 42: Surveillance Self-Defense, "9._endtoendencryptionmetadata," 2019, digital image, Electronic Frontier Foundation, https://ssd.eff.org/en/module/what-should-i-know-about-encryption.
Page 49: African News Agency, "Parliament meeting falls victim to hacking as MPs greeted by pornographic images," 2020, digital image, Reuters, https://www.iol.co.za/news/politics/parliament-meeting-falls-victim-to-hacking-as-mps-greeted-by-pornographic-images-47657120
Page 51: UK Parliament, digital image, Jessica Taylor, https://e3.365dm.com/20/04/768x432/skynews-parliament-house-of-commons_4974709.jpg?20200422191547
Page 52: Brett Sayles, "Server Racks on Data Center," 2020, digital image, Pexels, https://www.pexels.com/photo/server-racks-on-data-center-4508751/.
Page 58: PhotoMIX Company, 2016, "White 2 Cctv Cameras Mounted on Black Post Under Clear Blue Sky," digital image, Pexels, https://www.pexels.com/photo/white-2-cctv-camera-mounted-on-black-post-under-clear-blue-sky-96612/.
Page 63: Stefan Coders, "laptop-screen-vpn-cyber-security," 2020, digital image, Unsplash, https://pixabay.com/photos/laptop-screen-vpn-cyber-security-5534556/.
Page 65: Surveillance Self-Defense, "Using the Tor Browser," digital image, Electronic Frontier Foundation, April 25, 2020. https://ssd.eff.org/files/2020/04/25/circumvention-tor_0.png
Page 67: Nathan Dumlao, "White Samsung Android Smartphone on Brown Wooden Table," 2020, digital image, Unsplash, https://unsplash.com/photos/kLmt1mpGJVg.
Page 72: Matt Artz, "Two Broken 6-Pane On White Painted Wall Photo," digital image, Unsplash, October 1, 2017, https://unsplash.com/photos/vT684iB7Ejg.


NDI
NATIONAL
DEMOCRATIC
INSTITUTE


HOUSE
DEMOCRACY
PARTNERSHIP


IRI
INTERNATIONAL
REPUBLICAN
INSTITUTE
Advancing Democracy Worldwide


USAID
FROM THE AMERICAN PEOPLE