Implementing the Paris Call Principles
Principle #7: Advancing Cyber Hygiene

THE COMPENDIUM ON CYBER HYGIENE

THE CYBERSECURITY TECH ACCORD'S GUIDE TO ADVANCING CYBER HYGIENE AND PRACTICING SAFE ONLINE HABITS

Over the last decade, increasing connectivity and advancements in digital technologies have led to cyberspace playing a central role in seemingly every aspect of our lives. However, the growth in both frequency and impact of cyberattacks has jeopardized the benefits of these advancements. These attacks are often carried out by skilful hackers, as well as states, creating new and evolving threats to personal data, company resources, and entire industries. While it may be impossible to protect against every threat, organizations can significantly improve their security posture by educating their user base on best practices for secure digital engagement.

The Cybersecurity Tech Accord, the largest industry commitment to international cybersecurity, and an early supporter of the Paris Call, was launched in 2018 to help the technology industry take greater responsibility for cybersecurity challenges. Promoting better cyber hygiene among organizations, governments and individuals is a key part of this commitment, and core to protecting users and customers everywhere. To this end, the Cybersecurity Tech Accord has made strides to ensure that its 140 plus signatories implement cyber hygiene best practices in their daily operations, support like-minded organizations in the promotion of effective cyber hygiene protocols, and launch and support initiatives that raise consumer awareness.

In November 2018, the **Paris Call for Trust and Security in Cyberspace**, a landmark agreement led by the French government between public and private sector actors, united its supporters around nine foundational principles to help secure cyberspace. As early and vocal proponents of the Paris Call, the Cybersecurity Tech Accord has been dedicated to helping implement principles where we have unique expertise. Through collaboration with our signatories, and with multistakeholder groups over the last two years, the Cybersecurity Tech Accord has helped to make the Paris Call principle on cyber hygiene operational, available and accessible at scale, particularly in communities with limited financial and technical resources.

This compendium presents a **collection of resources and initiatives on cyber hygiene** that we have developed and implemented over the past three years with the objective of supporting the Paris Call principle. It is intended to help businesses and consumers take the necessary steps to protect against evolving cyber threats and practice secure online habits. Some of these initiatives have been developed in partnership with like-minded organizations, including the Global Cyber Alliance, Internet Society, and Consumers International, based on common values and a shared commitment to promote a safer cyberspace.

In today's always-on, always-connected world, these challenges can no longer be a concern for cybersecurity professionals alone. Protecting our online environment is in everyone's interest, and must be a shared responsibility. This means that everyone must hold themselves accountable for adhering to cybersecurity best practices; no individual, business, or government entity can be solely responsible nor fully exempt from helping to keep the internet safe and secure. And the technology industry has a responsibility for helping to develop and share these best practices to help keep secure the products and services we provide. We hope this compendium on cyber hygiene will serve as a starting point for businesses and consumers seeking a clear overview of the ways they can contribute to helping keep the online environment safe while protecting themselves and their assets online.

Contents

LEARN ABOUT
WHO WE ARE

About the Cybersecurity Tech Accord

Founded in 2018, the Cybersecurity Tech Accord is a coalition of over 140 global technology firms committed to advancing trust and security in cyberspace based on four foundational cybersecurity principles.

By combining the resources and expertise of the global technology industry, the Cybersecurity Tech Accord creates a starting point for dialogue and decisive action.
Through a shared commitment signatories aim to:

1. *Provide their customers, users and the developer ecosystem with information and tools that enable them to understand current and future threats and better protect themselves.*
2. *Protect their customers and users everywhere by designing, developing and delivering products and services that prioritize security, privacy, integrity and reliability, and in turn reduce the likelihood, frequency, exploitability and severity of vulnerabilities.*
3. *Work with each other and likeminded groups to enhance cybersecurity best practices, such as improving technical collaboration, coordinated vulnerability disclosure and threat sharing, as well as ensuring flexible responses for the wider global technology ecosystem.*
4. *Oppose efforts to attack citizens and enterprises by protecting against exploitation of technology products and services during their development, design, distribution and use.*

About the Paris Call for Trust and Security in Cyberspace

In 2018, French President Emmanuel Macron launched the Paris Call for Trust and Security in Cyberspace.

This landmark agreement set a new standard for multistakeholder cooperation in promoting stability, security, and resilience in the online world. As cyberspace is an inherently shared domain, the Paris Call is based on the belief that governments, along with civil society and private industry, all have unique and overlapping roles and responsibilities when it comes to cybersecurity and promoting a rules-based international order online. In this multistakeholder community, the technology industry in particular, as the owners and operators of the majority of what we consider "cyberspace," has unique responsibilities for its security.

PRINCIPLE #7

SUPPORT EFFORTS TO STRENGTHEN AN ADVANCED CYBER HYGIENE FOR ALL ACTORS

ABOUT CYBER HYGIENE

Why cyber hygiene

Never have we been reminded of the importance of good hygiene routines as much as in 2020. Simple actions, such as washing our hands, have become key factors in protecting ourselves and the people around us from new threats to our health. The same is true of cyber hygiene, serving the same purpose in the online ecosystem.

Cyber hygiene refers to the practice of implementing protocols and precautions that maintain system health and improve cybersecurity, reducing the risk of falling victim to an attack. The term cyber hygiene was coined by Vinton Cerf, an Internet pioneer, who used that the expression in his statement to the **United States Congress Joint Economic Committee on 23 February 2000:**

> *It is my judgment that the Internet itself is for the most part secure, though there are steps we know can be taken to improve security and resilience. Most of the vulnerabilities arise from those who use the Internet--companies, governments, academic institutions, and individuals alike--but who do not practice what I refer to as good cyber hygiene. They are not sufficiently sensitive to the need to protect the security of the Internet community of which they are a part. The openness of the Internet is both its blessing and its curse when it comes to security.*

Mr. Cerf's statement remains true to this day. In fact, with technology playing a much more prominent role in our lives, cyber hygiene is more essential now than it was twenty years ago. Greater attention is needed to protect ourselves and the online ecosystem that we all rely on. While some cyber hygiene practices can be resource intensive, most practices such as creating strong passwords, limiting the use of public WiFi, using multi-factor authentication (MFA) and backing up personal data, are simple enough to implement.

While it is impossible to eliminate every cybersecurity risk, research suggests a proactive approach to cyber hygiene could resolve over 90% of online attacks. Practicing cyber hygiene makes it harder for cybercriminals to execute their cyberattack and cause substantial damage. It will help to reduce your risk and protect the health of your organizations' network and assets.

Cyber hygiene best practices

There is no shortage of guidance on cyber hygiene. Several governments around the world have developed and shared guidance and best practices that both individuals and organizations can implement to protect themselves and their assets online. Here are some examples:

For Businesses

- **Australia:** **Strategies to Mitigate Cyber Security Incidents**. The Australian government recommends that businesses implement eight essential mitigation strategies as a baseline to prevent cybersecurity incidents (the Essential Eight). These include enabling multi-factor authentication and performing daily backups so that information can be accessed following a cyber security incident. Organizations can start implementing the Essential Eight at a basic level and then gradually increase their maturity.
- **Canada:** **Security Actions to Protect Internet-Connected Networks and Information.** Developed by the Canadian Centre for Cyber Security, this guidance aims at helping businesses build a strong IT infrastructure and at protecting their networks. The guidance includes actions such as patching operating systems and applications, minimizing the number of users with administrative privileges as well as providing tailored awareness and training to staff. When implemented as a set, the 10 actions help minimize intrusions or the impacts to a network if a successful cyber intrusion occurs.

- **France:** 40 Essential Measures for a Healthy Network. This guide developed by France's national cybersecurity and cyber defense agency (ANSSI) sets out 40 essential IT measures that organizations should follow to safeguard the security of their information systems. The guide includes a wide range of security measures, amongst others on upgrading software, ways to make authentication more secure and organizing a response in the event of an incident.
- **United Kingdom:** Cyber Essentials. Cyber Essentials is the UK government-backed cybersecurity assurance certification allowing businesses to show consumers that they have measures in place to help defend against the most common cyber threats. Businesses can either assess themselves against five basic security controls (firewalls, secure configuration, user access control, malware protection and patch management) with a qualified assessor verifying the information provided. Or, a qualified assessor examines the same five controls, testing that they work through a technical audit.
- **United States:** Critical Cybersecurity Hygiene: Patching the Enterprise. This project by the National Cybersecurity Center of Excellence (NCCoE) aims to increase awareness of the importance of cyber hygiene issues and recommends specific prioritized actions that organizations can take to overcome common security obstacles. In particular, it provides actionable guidance on establishing policies and processes for the entire patching lifecycle. Further, it establishes a playbook with rapid mitigation actions for destructive malware outbreaks that organizations can execute tactically in the first 30 days, and recommendations that can be implemented strategically beyond 30 days.

For Individuals

- **Australia:** Protecting Individuals and Families Online. This comprehensive guide was developed by the Australian Cyber Security Centre (ACSC) and asserts that taking care of your online safety is no more complicated than steps taken to safeguard your physical belongings. The organization suggests that individuals and families can use anti-virus software and should backup their data to avoid falling victim to a cyberattack. Other guidance includes making good choices on the web, taking precautions when sharing files, using MFA, and protecting your passwords which safeguard private information.
- **Canada:** Cybersecurity at Home and in the Office, Security Your Devices, Computers, and Networks. The Canadian Centre for Cyber Security has a number of comprehensive guidelines for individuals looking to bolster their cybersecurity practices online. Tips include securing your mobile, computer and smart devices by deploying security updates, using strong passwords, proactively spotting malicious email messages, and backing up your information. Additional resources include "Have you Been Hacked?," which explores the warning signs and potential mitigations if you've already fallen victim to a malicious actor.
- **France:** Digital Security Best Practices for Business Travelers. The National Cybersecurity Agency of France (ANSSI) shared digital guidelines for business travelers which included not transporting relevant data, exercising discretion while on the road and changing any passwords used during your trip upon your return. ANSSI also suggested doing research beforehand to find out about the cybersecurity legislation of the country you're going to, not leaving your documents or devices unattended, and if in doubt to ensure your devices are checked by your security officer.
- **United Kingdom:** Cyber Security advice for Individuals and Families. The National Cyber Security Centre shares practical tips for dealing with common cyber problems, including what to do when you've been hacked, how to deal with a ransomware attack or malware on your device, and next steps if your username and passwords have been stolen.
- **United States:** Alerts and Tips. The Cybersecurity and Infrastructure Security Agency developed tips for dealing with online threats, including guidance for safe browsing online, and further shared information on how to avoid ransomware and malware attacks. The agency also encouraged users to stay safe when engaging in online communications, by enhancing their mobile safety.

CYBER HYGIENE FOR ALL

10 steps to securing our online environment

Good cyber hygiene involves many different practices, policies, and training that organizations, governments and individuals can implement to make our internet ecosystem more secure. At the heart of all these practices and protocols there are a few basic steps that all users of technology products should follow to protect from cyber threats.

Such measures do not require specific cybersecurity skills and they can be easily implemented as a part of our routine, both at home and at work. On top of this, there are more specific cyber hygiene practices that companies from all sectors, including the tech sector, should put in place to protect our internet ecosystem. We will return to these later. In this first section, we will focus on cyber hygiene for all.

In 2018, as we celebrated Cybersecurity Awareness Month we looked at some of these recommendations and identified 10 key steps that all users of technology products should take to stay safe online:

1.
Always change your default passwords, create strong, unique passwords for each of your accounts, and consider using a password manager to help keep personal information safe;

2.
Use multi-factor authentication (for example, using both a password and a fingerprint or email verification) whenever possible in addition to strong passwords to confirm your identity when logging into your accounts;

3.
Use a firewall to block unauthorized access to computers and devices;

4.
Ensure that you update your operating system, browser, and other software up to date with security patches to minimize threats from viruses and malware;

5.
Limit what you do over public Wi-Fi and use software that creates a secure connection over the internet such as a Virtual Private Network (VPN) to safely connect from anywhere;

6.
Practice safe surfing and shopping, checking that the site's address starts with "https", instead of just "http";

7.
Enable privacy settings and increase the default security settings of the software you use;

8.
Be selective when sharing personal information as this could be used by hackers to guess passwords and logins;

9.
Do not download pirated software as it is not only illegal, but it often includes some type of malware;

10.
Back up your data, either to an external hard drive or the cloud, as this is the easiest way to recover from ransomware, as well as other attack methods.

The benefits of using a Virtual Private Network

The problem

Many of us use public WiFi to work, shop online, connect to our social media accounts, view or transmit personal information and data when we are not at home and do not have access to our home network. Today, free internet access points are available almost everywhere: at restaurants, hotels, airports, bookstores. This freedom comes at a price, however, and there can be risks associated with these connections. Free Wi-Fi hotspots which require no authentication to establish a network connection can create easy opportunies for hackers to get access to unsecured devices on the same network. The biggest threat to free Wi-Fi security is the ability for hackers to position themselves between users and the connection point – so-called "Man-in-the-Middle Attacks". This allows hackers to access any information that passes between users and the websites they visit.

Another risk of using free public Wi-Fi is that you may be connecting via a rogue hotspot. This is an open hotspot, usually with a name similar to that of a legitimate hotspot as a disguise, which cybercriminals set up deliberately to lure people into connecting to their network. Once a victim connects to the rogue Wi-Fi hotspot, the host hacker can then intercept data and even use tools to inject malware into the connected devices.

Protecting against unsecured Wi-Fi

A virtual private network (VPN) offers online privacy and anonymity by creating a private network from a public internet connection. VPNs rely on servers, protocols, and encryption to hide your data and location from bad actors. Once connected, a VPN can direct your internet traffic to one of its servers, where it is encrypted, and sent to the site you intend to visit. The data encryption makes it difficult for anyone to track your online activity or execute a cyberattack. Moreover, using a VPN disguises your location by replacing your IP address with their server's, which is why they are probably best known for accessing video streaming services in different countries. Finally, some VPNs come with additional built-in protections, which automatically block malicious sites and pop-ups. In short, using a VPN – on both your phone and computer – increases your privacy and security online.

How do you choose a VPN?

When choosing a VPN, your first question should be whether you want to run your server or go with an external provider. There is no simple answer for that, as it will depend on your needs and whether you are looking for your personal use or for your organization.

External providers tend to be more cost effective, as offers tend to be inexpensive, or even free. When it comes to organizations, you should also consider whether the service is compatible with your preferred operating system, does it work on both mobile and desktop, and does it have multi-user support?

Price aside, using an external provider can expose you to more risk. It is important to remember that the VPN provider might be able to see your online traffic, will likely retain your credit card data, and potentially your IP address. Using a VPN does not mean you are anonymous online.

If you decide to go with an external provider, how do you decide which one to use amongst the hundreds available? We recommend asking the following questions to ensure you select a provider that prioritizes cybersecurity:

- Does the VPN collect user data, or does it have a no logs policy?
- Does it accept anonymous forms of payment?
- Does it have DNS leak protection in place, which ensures that your activity is not unintentionally routed back to the internet service provider?
- How safe is the VPN's encryption? What is the strength of its encryption ciphers, and does it use end-to-end encryption?
- Does it support IPv6?
- Does it protect from WebRTC exploitation, i.e. the technology that browsers use to communicate with each other?
- Where is the VPN based, and which privacy laws does it follow?
- What do their product reviews look like? Have they been in the news recently? Do they highlight examples of any reputable clients? Do they publish transparency reports?

What are the best VPN options out there?

While the recommendations highlighted above will help you navigate this space, we understand it isn't easy to make an informed choice with so many factors to consider. If you're feeling stumped, we recommend taking a look at this **VPN comparison chart**, which analyzed almost 200 providers based on their jurisdictions and policies, as well as this **set of recommendations** focused on privacy. **PC World** recently made a comparison listicle which focuses on usability, privacy and security.

Overall, pick the solution that works best for you and remember to keep the VPN on whenever possible.

Our work to raise awareness about the benefits of using a VPN

In 2020, as a part of our commitment to the Paris Call, we launched a blog series to raise awareness about the importance of cyber hygiene practices including the benefits of using a VPN. You can read more about our work **here**.

The importance of "patching"

The Problem

Software vulnerabilities are weaknesses or flaws present in software code. They are considered the root of most cybersecurity incidents, as they can allow malicious actors to gain access to our devices and personal data. Issuing a "patch" is considered the most effective way to remedy the problem, but the process of patching can be time-consuming and costly.

Patches are most commonly encountered in the form of updates that your devices (including a smartphone, computer, smart TV, etc.) will ask you to deploy from time to time. Companies create patches for numerous different reasons, from solving a system issue to improving software efficiency or adding a feature update. However, the most significant is undoubtedly the security patch, which seeks to mitigate a security vulnerability.

Although applying patches is a fairly basic an straightforward security principle, 57% of data breaches are still attributed to poor patch management. More needs to be done to improve the practice, in particular to improve the speed with which patches are applied. It takes, on average, 102 days to patch a flaw.

On an individual level, there remains limited awareness about the importance of patching, and some hold unfounded fears that updates allow vendors to access your data and personal information. At an organizational level, patching can sound more straightforward than it is and generally requires organizations to consider several factors. First, deploying security updates entails an accurate inventory of the technology in use, which many businesses and other large organizations don't have. Similarly, many organizations continue to use old technology that is no longer compatible with the latest software updates. Additionally, patching can be resource-intensive and require personnel with a deep understanding of the patch management process, including testing, as certain updates can impact other functions in unexpected ways. Many organizations fall short on one or several of the above points and leave their systems vulnerable to bad actors.

Protecting against cyber threats by mastering patching

For consumers that understand the importance of keeping your devices secure, it is as simple as allowing the software to update as soon as there are updates available. Often these updates are done in the background, but sometimes it requires the end user's approval.

On the other hand, to minimize a company's exposure to software vulnerabilities, some legwork is required. Here are a few steps to take:

1. **Do an inventory of all your technical assets to ensure you know your risks.**
2. **Conduct a risk analysis of all your technical assets to help you with prioritization.**
3. **Monitor to ensure that you are aware of all available patches for your systems.**
4. **Determine the importance of each patch and deal with the most critical updates first.**
5. **Implement additional security controls to ensure that you are protected if you cannot deploy the patch immediately.**
6. **Test the patch to prevent any unexpected consequences.**
7. **Back up your production environment, just to be safe.**
8. **Deploy the patch, ideally staggering the scheduling of patches to reduce downtime.**
9. **Rinse and repeat!**

Our work to raise awareness about the importance of patching

Earlier this year as, part of our commitment to the Paris Call, the Cybersecurity Tech Accord launched a blog series to raise awareness about the importance of cyber hygiene practices including patching. You can read more about our work here.

On a more practical level, the Cybersecurity Tech Accord signatories Cisco, Microsoft and Tenable are currently working with the National Cybersecurity Center of Excellence (NCCoE), a part of the U.S. National Institute of Standards and Technology (NIST) to build common enterprise patch management reference architectures and processes. The results will be publicly available in the NIST Special Publication 1800 practice guide.

Securing our IoT devices

The Internet of Things (or IoT) is a term used to describe how more and more devices and processes are coming online. This trend includes consumer products, where everything from smart toasters to children's toys to vacuum cleaners, to boilers are increasingly connected to the Internet, enabling our homes and products to do more. While IoT products bring tangible benefits, and demand for them increases every year, the security threats that surround them are frequently underestimated or simply overlooked. However, the staggering 2.8 billion cyber-attacks on IoT devices registered in the second half of 2019 alone highlight just how real these threats are, and how important it is to pay close attention to IoT security.

What are IoT security risks?

The cybersecurity threats that surround IoT products range in scope and impact, and can include data theft, physical device threats, and large-scale attacks.

Private and corporate data threats

Whether it is personal or corporate, data theft represents a very lucrative temptation for cybercriminals. It is estimated that 57% of IoT devices are vulnerable to medium or high severity attacks (Palo Alto Networks, 2020). Their vulnerabilities can be used to steal credit card information, addresses, social security numbers, insurance policies, or health information, which can then in turn be sold for high sums on the dark web.

Illicit Surveillance

Hackers might also be looking to illicitly survey our homes and businesses by exploiting the security loopholes of our connected devices. A break-in could for example be orchestrated by using IoT security cameras and checking whether the owners of a business or residents of a home are present.

Physical Threats

Cyber-attackers could also hack into devices to slow them down in exchange for a ransom. While these kinds of physical attacks on consumer IoT devices in our homes are less dangerous and rarer, they have been carried out to shut down entire large scale IT systems, electrical power grids and industrial production lines. Attackers can also "brick" a device, effectively shutting it down permanently.

Threats to Others

Attackers can also leverage the power of many different IoT devices combined for nefarious purposes. One such example is the use of botnets, which provide attackers with access to and control of several thousand computers at a time and allow them to carry out malicious activities. These can include large scale data leaks, denial of service attacks, credentials leaks, etc.

While it can take some time before the owners of an IoT device to realize that they have fallen victim to a cyber-attack, attackers can be quick and ruthless. It can take mere minutes for a skilled hacker to exploit devices with poor security.

Our work to help protect against IoT security risks

The security threats surrounding of IoT products have made cyber hygiene even more important. While the previously mentioned basic practices apply here as well, additional steps need to be taken to keep IoT devices secure. With the objective of raising awareness around the risks that IoT devices can pose and ways to protect against them, in May 2020 we launched, in a conversation with Consumers International, the "Stay Smart. Stay Safely Connected" campaign, which included a repository of information to ensure consumers have more information about how to keep their IoT devices secure.

Smart Speakers

Beginner

- Don't put speakers near a window which could enable someone to connect to them.
- Turn off the device when not using to stop it listening.
- Turn on email notifications to watch for any unauthorized access or purchases.

Intermediate

- Delete voice history and past commands.
- Train speakers to recognize different voices.
- Monitor the accounts you link to for any unusual activity such as purchases you did not initiate.
- If possible, turn off 'personalized results'.

Advanced

- If possible, opt-out of sharing recordings used to improve the service with the manufacturers.
- Remove sensitive data stored on accounts associated with the speakers (e.g., turning payment functionality off).

Smart Doorbells

Beginner

- Attach the device securely so it can't be stolen.
- Delete old footage.

Intermediate

- Hide your network name or ID to prevent your network from being visible and easily accessible. This can be done by using a Virtual Private Network (VPN).

Smart TVs

Beginner

- Disable or cover cameras and microphones when you are not using the device.
- Stick with your smart TV's dedicated remote and avoid smartphone remote apps, since they can make it easier for hackers to grab login information if your device is otherwise compromised.
- Download applications with caution and always directly from the Google Play store, the App Store or your manufacturers' official application store avoiding allowing app installation on your devices from unknown sources.

Intermediate

- Applications installed on the TV usually have their own privacy and security setup which is independent from the TV. Ensure that you enable privacy and security options on each of the installed applications.

Smart Toys

Beginner

- Talk to your kids about never giving out personal information or posting sensitive information online.
- Check reviews and consumer advisory to see if there have been negative reports on the toy.
- Always make sure the toy is switched off or unplugged when not in use.

Intermediate

- Check what in-place security measures come with the toy (e.g. whether data is encrypted or if you need to protect your data with a password) as well as what kind of data is captured, such as voice recordings or facial recognition.

Smart Home Locks

Beginner

- Use a PIN for voice unlocking.
- Create unique codes for individuals.
- Increase the length of your codes and passwords – longer passwords are better because they lower the chance of brute force attacks.

Intermediate

- Create expiring codes with scheduling.
- Enable extra features like decoy numbers available on some devices.

Smart Printers

Intermediate

- Require owners to authenticate themselves before allowing them to print.

Advanced

- Turn off unused protocols and disable unused ports.

Smart Baby Monitors

Intermediate

- Disable remote access to your baby camera.
- Periodically check the logs for unauthorized access.
- Change the port used to access your camera. Like for any other default settings, default ports could make it easier for hackers to access your device.

Intermediate

- Disable Dynamic DNS (Domain Name Server) on your camera, which could allow remote access to your device.
- Disable port forwarding and UPnP (Universal Plug and Play), which could allow an attacker to bypass your firewall and gain control over your device through malware.

Smart Indoor & Outdoor Security Cameras

Beginner

- If you don't need the internet streaming feature, it's best to disable it.

Intermediate

- Make sure the smart camera is able to download the latest updates of its software and firmware.

CYBER HYGIENE FOR BUSINESSES

Coordinated vulnerability disclosure policies to keep customers secure

The Problem

Software enables the many digital technology products and services we use every day, and it also it underpins the operations of our critical infrastructure and services, including everything from public transportation to hospitals, banks, governments, and electricity/water supplies. However, even well-designed software will likely have some unknown security vulnerabilities. Once such a software vulnerability becomes known, nefarious actors are in a race against the clock to exploit it.

Having a coordinated vulnerability disclosure (CVD) policy in place ensures that any risk or potential harm to users stemming from a vulnerability can be deliberately minimized in a timely fashion once it has been identified. While the process of disclosing vulnerabilities can be straightforward, a vast number of different stakeholders are also often involved (e.g., manufacturers, vendors, reporters, government agencies, IT security providers), which can add significant operational and legal complexities. Moreover, different stakeholders may have very different motivations to disclose (or not disclose) vulnerabilities: technology companies want to preserve the integrity and security of their products and services and, ultimately, their reputations; while security firms may profit from sharing such information; researchers may want to use vulnerabilities for academic purposes; and of course criminals could seek to exploit them.

Protecting customers by adopting CVD policies

CVD policies can significantly contribute to addressing these complexities. They give ethical hackers clear guidelines for submitting security vulnerabilities directly to the affected company instead of publicly posting the information or selling it to nefarious actors. As a rule, it is important that an issue is shared directly with the impacted vendor as soon as possible, as they are best positioned to lead subsequent coordination efforts to validate the vulnerability and to develop remediations for their own products or services.

By keeping the entities involved to a minimum, the risk of the flaw being exploited before a patch is deployed is minimized. Proper communication among those included is perhaps the most important element of any CVD policy. Responsive acknowledgment and, as needed, ongoing dialogue between the finder and vendors working to investigate and fix the issue can increase trust and decrease uncertainty, making collaboration more straightforward. CVD policies are generally based on a belief that anyone reporting an issue is likely benevolent in doing so. On that basis, companies should consider adopting a vulnerability disclosure "safe harbor" policy as part of this effort, committing not to pursue criminal or civil actions for good-faith or accidental violations of their disclosure processes.

Successful CVD policies

The Cybersecurity Tech Accord signatories strongly believe in CVD policies and support the idea that all developers of technology should endorse this approach – not just technology companies. While there are different approaches to CVD based on the context of any given company, the Global Forum on Cyber Expertise (GFCE) has developed a helpful overarching guide on the matter: **Global Good Practices on Coordinated Vulnerability Disclosure (CVD).**

From an industry perspective, it proposes that manufacturers, vendors, and user organizations should:

- Use existing standards and guidelines (e.g., ISO/IEC standards, FIRST's guidelines, ENISA good practice);
- Implement the required processes to deal with incoming reports, investigate the reported vulnerabilities, and communicate with reporters, being as transparent as practicable about risk-based remediation timelines. This also includes publishing CVD policies on organizations' websites;
- Allocate adequate resources to implement CVD policies to ensure that organizations have the necessary expertise. This could include running a pilot and starting with a narrow set of in-scope products/services, using a third-party bug bounty platform, and/or consulting with similarly situated organizations that have CVD policies and processes in place;
- Ensure continuous communication with all stakeholders, explicitly stating expectations towards reporters and third-party organizations;
- Agree on timelines on a case-by-case basis, avoiding a 'one-size-fits-all' policy and maintaining flexibility in handling various vulnerability discovery cases;
- Provide a clear explanation of pros and cons to the legal counsel, ensuring they have a good understanding of the national legal framework on CVD and the importance and advantages of CVD for an organization.

Our work on vulnerability disclosure

As a part of our efforts on cyber hygiene, **all of our signatories have committed to adopt and publish their CVD policies**, in keeping with one of the GFCE's best practices inviting organizations to be as transparent as possible. In addition, we call on more technology companies to adopt CVD policies and hope to announce further actions to encourage this initiative in the coming months.

Finally, **we made available a series of webinars, including on vulnerability disclosure**, to help companies understand the process of developing, adopting and making public their vulnerability disclosure policies and the importance of taking these steps.

CVD policies of the Cybersecurity Tech Accord signatories:

Click to open policy

ABB | ACCESS SMART | AIMS360 | ALITER | ANOMALI | ARM

ATLASSIAN | AVAST | AVEPOINT | BIG CLOUD CONSULTANTS

BINARY HOUSE | BITDEFENDER | CAPGEMENI | CARBON BLACK | CISCO

CLOUDFLARE | CLOUDREACH | COM LAUDE | CORNERSTONE IT |

CONTRAST SECURITY | CSC GLOBAL | DATASTAX | DELL | DOCUSIGN | EATON

ESET | EXELTEK | FACEBOOK | FASTLY | FIREEYE | F-SECURE | GIGAMON

GITHUB | GITLAB | GUARDTIME | GREENLIGHT | GREYCORTEX | GTD GROUP

HITACHI | HMATIX | HP INC | INTEGRITY PARTNERS | HPE | INTUIT

JUNIPER NETWORKS | KPN | LASALLE CONSULTING PARTNERS | LINKEDIN

MEDIAPRO | MERCADO LIBRE | MICROSOFT | NETAPP | NOKIA | NORTHWAVE

NTT | ORACLE | ORANGE | PANASONIC | PANDA SECURITY | PANGO | PAX8

PREDICA | PROFESSIONAL OPTIONS | ROCKWELL AUTOMATION | RSA

SAFE PC CLOUD | SAFETICA | SALESFORCE | SAP | SCHNEIDER ELECTRIC

SCITUM | SILENT BREACH | SONDA | SSRD | STACKPATH | STRIPE

SWISSCOM | SYNACK | TAD GROUP | TANIUM | TELECOM ITALIA

TELEFONICA | TENABLE | TRENDMICRO | US LICENSING GROUP | VALIDY NET

INC | VMWARE | VU SECURITY | WIPFLI | WISEKEY

Securing Email Communications: DMARC

The Problem

With over 4 million users, email remains one of the primary communications channels for private individuals, organizations and government institutions, and its widespread use makes it the preferred attack method for impersonation and fraud. Attackers often seek to exploit e-mail to gain control over an organization, access confidential information, or disrupt IT access. Common threats to e-mail systems include malware, as well as spam and phishing and social engineering attacks. Research by F-Secure found that over one-third of all security incidents start with phishing emails or malicious attachments sent to company employees. The cost of these email security threats to an organization can be enormous. Aside from the fines and legal actions that result when sensitive customer information or financial data is breached, email security threats can have a huge cost in reduced customer confidence, damage to reputation and, ultimately, loss of business.

Protecting against email threats

Domain-based Message Authentication, Reporting & Conformance (DMARC) is an email authentication policy and reporting protocol and a leading way to prevent impersonation attacks via email.

Designed on the basis of real-world experience by some of the world's largest email senders and receivers, DMARC builds on a system where senders and receivers collaborate to improve the email authentication practices of senders and to enable receivers to reject email that cannot be authenticated. **DMARC allows:**

Domain owners (email senders) to

- Signal that they are using email authentication (SPF, DKIM).
- Provide an email address to gather feedback about messages using their domain – legitimate or not.
- Establish a policy to apply to messages that fail authentication (report, quarantine, reject).

Email receivers to

- Be certain a given sending domain is using email authentication.
- Consistently evaluate SPF and DKIM along with what the end user sees in their inbox.
- Determine the domain owner's preference (report, quarantine or reject) for messages that do not pass authentication checks.
- Provide the domain owner with feedback about messages using their domain.

Our work to promote the uptake of DMARC

In 2018, as a part of our commitment to the Paris Call, **the Cybersecurity Tech Accord partnered with the Global Cyber Alliance (GCA) to endorse and encourage the use of DMARC**. In 2020, in keeping with GCA's guidance to improve email security and promote a wider adoption of the DMARC protocol on a broad scale, we also published a blog to educate users by dispelling the myths about DMARC:

Myth #1:

It's used on email domains only

ANY domain can be impersonated and used in phishing attacks, so we need to do more than just secure the domains used to send mail. Every domain owned by your organization should be secured with its own DMARC policy.

Myth #2:

It's a Silver Bullet

DMARC is not an inoculation against every cyber risk. It protects only one type of spoofing. All organizations need a layered defense when it comes to securing email, and DMARC is an important layer but still only one. Your organization may also use other secure email mechanisms, such as DNS-Based Authentication of Named Entities (DANE) or Message Transfer Agent Strict Transport Security (MTA-STS) (as well as others).

Myth #3:

It's not good for privacy

With DMARC, you can view who is sending emails on your domain's behalf, thus preventing hackers from using your domain to send suspicious messages within your organization or to your customers. In this way, DMARC reporting actually prioritizes privacy above other secure email practices.

Myth #4:

It's easy

Starting the implementation of DMARC may be relatively simple, but the real work comes with analyzing reports and adjusting your policy levels for enforcement, which can be more labor-intensive.

Myth #5:

It's going to negatively impact my email

DMARC actually improves the delivery rate of the email you send to customers and others.

Myth #6:

It's only for large entities

Every organization with a public-facing domain can be vulnerable to spoofing and phishing, regardless of size. DMARC needs to be implemented by ALL organizations, from small startups to Fortune 500 corporations.

Finally, we published a video series on cyber hygiene including an introduction to DMARC

Tackling Threats to the Internet's Routing System: MANRS

The Problem

The speed and volume of our digital communications require a stable and secure online environment. The reality is that accessing an online website, paying with a credit card, or even just looking for and exchanging information online can be delayed at any time by incidents affecting our routing infrastructure. In 2017 alone, more than 14,000 routing outages or attacks, such as hijacking, leaks, and spoofing, led to stolen data, lost revenue and reputational damage. One such example is a hijacking event from April 2018 that impacted the Ethereum cryptocurrency. When connecting to the service (MyEtherWallet), users were faced with an insecure SSL certificate, a broken link in the site's verification. Clicking through that, they were redirected to a server based in Russia which proceeded to empty their wallet. These kinds of examples make it clear that more needs to be done to address some of the common challenges related to routing security, which is the basis for the Mutual Agreed Norms for Routing Security (MANRS).

Protecting against threats to the Internet routing system

The MANRS initiative, supported by the Internet Society (ISOC), focuses on four actionable measures that can deliver immediate results to improve routing security. **They include:**

- **Filtering,** to help combat the propagation of incorrect routing information. This measure aims to ensure the correctness of operator and customer routing announcements to adjacent networks with prefix and AS-path granularity;
- **Anti-spoofing,** a measure by which network operators implement a system that enables source address validation for at least single-homed stub customer networks, their own-end users and infrastructure. The goal is to prevent packets with an incorrect source IP address from entering and leaving the network;
- **Coordination,** to ensure that network operators maintain globally accessible up-to-date contact information in common routing databases and coordination with their peers; and
- **Global validation,** to enable network operators to publish routing data, so others can validate routing information on a global scale.

Our work to promote the uptake of MANRS

The Cybersecurity Tech Accord signatories strongly believe that a more robust and secure global routing infrastructure demands shared responsibility and coordinated actions from the community of security-minded organizations. We originally endorsed MANRS in 2018 and published a series of webinars on the topic, including on **Improving Routing Security Through Concerted Action**.

Our initial endorsement of MANRS led to the creation of a dedicated working group, tasked with investigating how companies beyond network operators and IXPs could contribute to routing security. Initially established as an exploration between the Cybersecurity Tech Accord and ISOC, it has grown in scope and brought in other technology players as well. In 2020, the working group developed a set of six actions for cloud service providers and content delivery networks to support routing security:

- **Prevent propagation of incorrect routing information.** Cloud providers and content delivery networks often have their own internal networks, as well as peering relationships, where good filtering practice should still apply to help prevent propagation of incorrect routing information.
- **Prevent traffic from illegitimate source IP addresses** by implementing anti-spoofing controls to prevent packets with illegitimate source IP addresses from leaving the network.
- **Facilitate global operational communication and coordination** by maintaining up-to-date contact information in PeeringDB and relevant WHOIS RIR databases.
- **Facilitate validation of routing information on a global scale** by documenting ASNs and prefixes that are intended to be advertised to external parties in either IRRs or an RPKI repository.
- **Encourage MANRS adoption by the technology industry.** The adoption of these norms has a multiplying effect, whereby the greater the number of adopters, the more secure the entire routing system becomes.
- **Provide monitoring and debugging tools** to peering partners to facilitate easy resolution of any challenges that may arise and ensure there is a clear feedback mechanism available.

Domain Name System (DNS) Security

The Problem

Domain Name System (DNS) attacks are not a new phenomenon. They first emerged as a preferred tool of political hacktivists; however, over the past four years DNS attacks have escalated and become a major source of cybersecurity risk for all types of organizations. Attacks against the DNS seek to hijack or undermine an organization by tampering with its domain presence. Risks associated with these types of attacks include possible reputation damage, loss of intellectual property or funds, threats stemming from data breaches, and potential loss of control of business-critical Internet assets like websites, email, apps, VPNs, and VoIP.

Vulnerabilities within domain name management systems can allow cybercriminals to change the authoritative DNS and redirect users to malicious sites, apps or intercepted email. In addition, such attacks can incorporate the issuance of rogue digital certificates to make the activity appear legitimate to end users. Attackers can also try to obtain the username and password to a registrar's portal that is not protected by multi-factor authentication, IP validation, or registry lock, giving them access to change the nameservers for domains accessible within the account.

Protecting against DNS hijacking

There are some good practices when it comes to protecting organizations from DNS hijacking that are worth sharing. The Cybersecurity Tech Accord signatories want to encourage organizations to apply security controls that will help them defend their digital assets outside the firewall, **such as:**

- **Incorporate secure domain, DNS, and digital certificate practices into your overall cybersecurity posture.**
  - Organizations should validate that their domain name registrar is Internet Corporation for Assigned Name and Numbers (ICANN) and registry accredited and can demonstrate their investment into systems and security. This should include both staff training on cybersecurity, as well as a variety of controls, processes, and security measures that ensure a defense-in-depth approach. The provider should offer two-factor authentication, IP validation, and federated identity for a single sign-on environment. It should also have security controls in place for the registry lock process.
  - It is business-critical that organizations leverage a multi-provider strategy for redundancy in DNS services to avoid a single point of failure.

- **Control user permissions**
  - User permissions for staff with access to domains and their DNS portal should be continuously reviewed and only trusted individuals should have access to elevated permissions.

- **Introduce proactive, continuous monitoring and alerting:**
  - Organizations should ensure that their domain name registrar or DNS hosting provider offers proactive and continuous monitoring, including of routing security, so that any potential disruption of business continuity can be quickly mitigated.

- **Utilize Resource Public Key Infrastructure**
  - The routed prefixes associated with authoritative DNS nameserver ranges should leverage Resource Public Key Infrastructure. The route origin authority represents a cryptographic confirmation of relevant authorization.

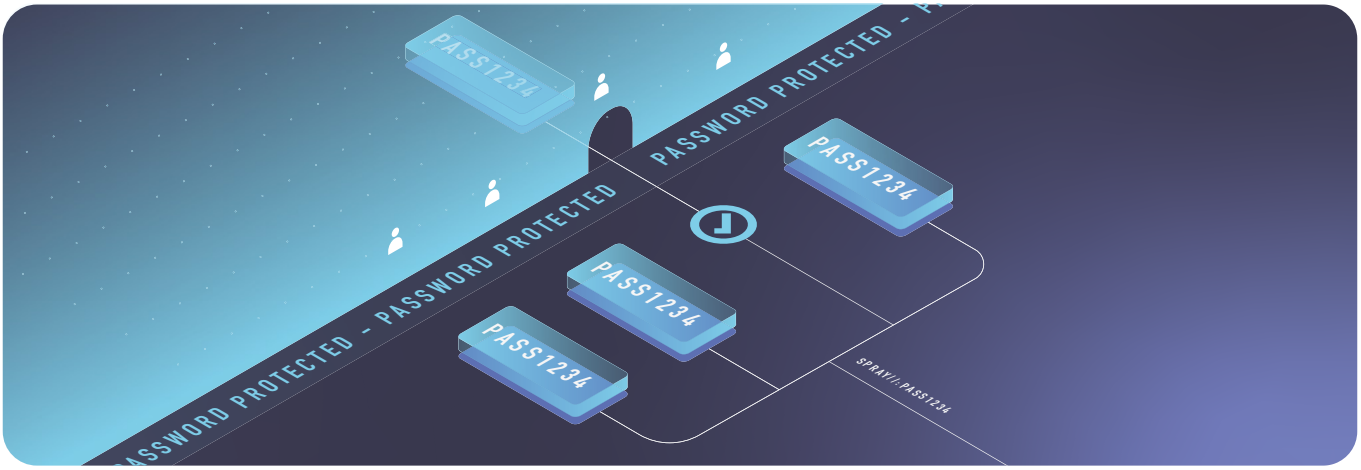
- **Proactively leverage the appropriate advanced security measures:**
  - Utilize domain name system security extensions (DNSSEC), for both signing zones and validating responses.
  - Prevent the execution of unauthorized requests with registry locks to stop automated changes of DNS records.
  - Initiate a Digital Certificate Policy with certification authority authorization (CAA) records allows only authorized certification authorities to issue a certificate on your domains.
  - Ensure (/DMARC/MTA domain-based message authentication, reporting, and conformance (DMARC/ DKIM/ SPF/MTA), which gives organizations protection against unauthorized use of their domains, commonly known as email spoofing.

Our work to raise awareness about DNS hijacking

Since 2018, the Cybersecurity Tech Accord has focused on driving greater awareness around the types of attacks that threaten DNS and how to best protect against them. In line with our commitment to the Paris Call, we collaborated with signatories to host a webinar on how to secure your digital assets from cyberattacks, published a blog that explores DNS as a missing link in cybersecurity risk postures, as well as provide information that encourages organizations to apply security controls.

More information can be found here.

In addition, as part of our video series on cyber hygiene there is an introduction to DNS security:



Protect against "password spray"

The Problem

"Password spray" refers to a type of cyberattack in which a malicious actor attempts to break into online accounts by simply testing a small number of commonly used passwords, such as Password123, 123456, or 00000, against different accounts on a domain. Advanced attackers can use this method against a large number of different accounts in a single attack, repeating the login attempts multiple times with different passwords while remaining undetected.

Typically, these attacks involve hackers gaining access to an organization's usernames through information readily available online or on individuals' personal accounts. Compromised or commonly used passwords are then used to attempt a login against different accounts on the network. Once they infiltrate the system, they can often obtain additional email addresses, change passwords, and even expand laterally within the network to achieve their goals – whether that is data exfiltration or something even more nefarious.

This stealthy attack, used by some of the most advanced adversaries, is not easy to detect, and victims often don't even realize they've been targeted. Last November, Microsoft reported that a state actor known as "Holmium," or APT33, used password spraying to target industrial control system suppliers for electric utilities, as well as oil and gas facilities, among other industrial environments. The report warned that such attacks could be a first step toward sabotage attempts and highlighted how it took less than a week from initial access to obtaining "unhampered access and full domain compromise."

Password spraying has become more common in recent years, not only because passwords are easy to guess, but also because compromising credentials have become widely available and methods for automating or executing large-volume tasks are easier to utilize. Think about how often you have read about large breaches in which hackers procured personal information and passwords. Users are leveraging an increasing number of services and applications nad reusing passwords is a common way to manage the inconvenience of having to remember multiple, complex passwords. As a result, compromised credentials for one service often give hackers an easy way to access others.

Protecting against password spray

A question you may ask yourself is how to make sure you and your organization do not become victims to this kind of attack. As with most things in cybersecurity, you can never be 100 percent sure you are protected. However, the following cyber hygiene practices can definitively reduce your cyber risk and exposure to a password spray attack:

- **Enable multi-factor authentication (MFA)** by default across your organization. Having a secondary layer of authentication eliminates the ability to compromise an account by guessing a password. This action requires that users sign in with at least two authentication factors that include a password or PIN, biometrics and/or a trusted device.

- As a stronger layer of protection and second link of trust, integrate an **IT centralized password manager** with Password Authentication Infrastructure (PAI) to alleviate employee-managed passwords.

- Implement a **"Managed Detection and Response" (MDR)** solution to help detect signals for password spraying. A mature cybersecurity program may collect all the data into centralized systems called Security Incident and Event Managers (SIEMs.

- Put a **virtual private network (VPN)** in place. This is a helpful tool to protect from man-in-the-middle attacks. Organizations must carefully monitor activity on their VPN and maintain security patching to avoid this layer of network access also becoming a threat vector.

- Implement an **effective password policy** for your organization, balancing usability and security, and blacklisting the most common and compromised passwords, as well as rejecting password reuse over time. Enforce periodic password resets. Moreover, make sure that new account passwords are not generic . As an individual, use a password generator service to ensure your passwords are secure and unique to each account.

- Set **account lockout policies** to prevent passwords from being guessed after a certain number of failed login attempts. However, make sure you don't give away critical information by ensuring applications return a generic error message no matter the incorrect log in entered.

- Finally, spread the word. As an organization, **implement security training** that ensures users are aware of bad password habits and act responsibly, not just when it comes to their work, but for their personal accounts as well. As an individual – tell your friends and ensure we all take steps to be more secure online.

Our work to raise awareness about password spraying

In 2020, as a part of our commitment to the Paris Call, the Cybersecurity Tech Accord launched a blog series to raise awareness about the importance of cyber hygiene practices including protecting against password spray. You can read more about our work **here**.

Multi-factor authentication (MFA): A foundational cyber defense for organizations

The Problem

Weak user credentials are one of the leading contributors to successful attacks. Stolen credentials are used by nefarious actors to compromise email accounts and web servers to steal money and sensitive data. They are also used to launch large-scale phishing campaigns or send targeted emails with similar purposes but more far-reaching effects, compromising companies' data and financial assets. Despite this being a well-known problem and despite many organizations' efforts to invest in password management, it is clear that there are many companies struggling to properly manage passwords and prevent password-related attacks.

Protecting against credentials breaches

Experts consider multi-factor authentication (MFA) to be foundational to establishing a strong cybersecurity posture in today's threat environment. The security team at Google asserted that MFA can prevent over 95% of bulk phishing attempts and over 75% of targeted attacks. Similarly, researchers at Microsoft found that this method can prevent 99.9% of all automated cyberattacks. While there are many important practices for improving cybersecurity, utilizing MFA is perhaps the single most effective step organizations and individuals can take to protect themselves online.

MFA is not a complicated concept. It is an authentication method that requires the user to present more than one (multiple) verification type, such as a password along with an additional element, to gain access to a system. A common example of MFA is using a bank card, where in most cases you need both a card and PIN-number to clear an ATM transaction.

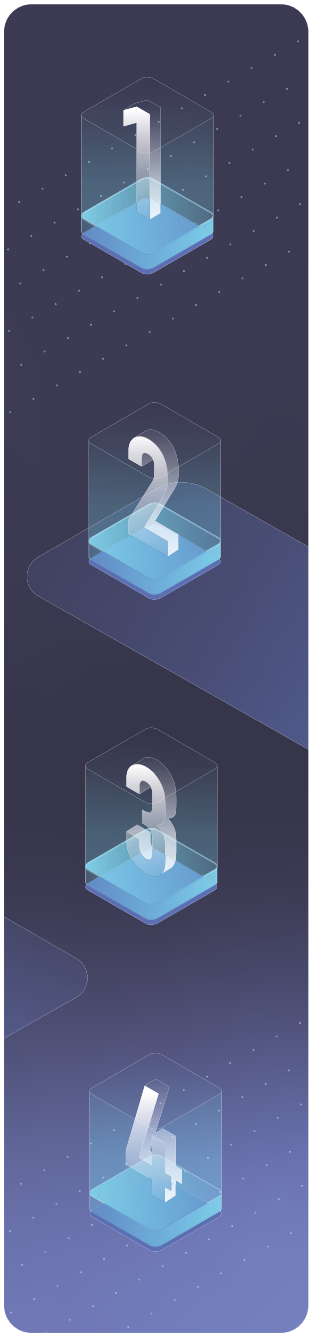
These "elements" of verification are typically categorized into three different classifications:

- **Knowledge-based:**
  Things only the user knows, such as a password or a PIN;
- **Biometric:**
  Things that are a part of a user, like fingerprints, retinas, or voice recognition; and
- **Possessions:**
  Things that only the users have, such as a badge or a phone.

When gaining access requires more than one of these elements, users are protected even when one is compromised. Digital services are increasingly incorporating additional protections to prevent cyberattacks, often providing users a window of opportunity to authenticate or confirm things like the location of an attempted login from an unrecognized IP address, which may get flagged as suspicious activity.

MFA best practices

While MFA is not perfect, the majority of attackers who encounter MFA protections will move on to their next target rather than invest the time needed to bypass it. To further discourage would-be hackers, here are some useful best practices to help organizations and users stay vigilant online:



1. **Implement MFA across an entire organization.**
   Rolling out MFA at scale may not always be straightforward, however the goal should be to enable it for all users on all your systems, all the time. This includes all company devices, data, applications and the network.

2. **Make MFA easier on employees.**
   Activating MFA will always be an extra step for users. Therefore, providing alternative MFA options that best suit their needs will help eliminate some of that friction and create a more positive experience. It's worth investing in solutions that allow the option for different methods of authentication such as tokens, text messages, phone calls, and/or biometrics.

3. **Set up cloud Identity and Access Management (IAM).**
   IAM systems are an effective way for cloud-based enterprises to manage the roles and access privileges of individual network users through a single, centralized resource. This enables admins to proactively monitor activity and identify suspicious behavior.

4. **Layer your security controls.**
   As explained above, MFA can still be defeated by a determined attacker with the right resources. While MFA is an important foundational step toward securing systems, it should be considered one of several measures an organization implements rather than the only security measure. Layering additional security controls may include methods such as disabling legacy email protocols and enabling conditional access policies.

Our work to raise awareness about MFA

In 2020, as a part of our commitment to the Paris Call, we launched a blog series to raise awareness about the importance of cyber hygiene practices including MFA.

You can read more about our work here.

CYBERSECURITY TECH ACCORD RESOURCES

Our commitment to the Paris Call for Trust and Security in Cyberspace

- Blog: The Cybersecurity Tech Accord endorses the Paris Call; strengthening our commitment to ensuring trust and stability in cyberspace, 12 November 2018
- Blog: The Paris Call for Trust and Security in Cyberspace – In celebration of its first anniversary, 12 November 2019

Cyber hygiene for all

- Video: Introducing cyber hygiene, 22 June 2020
- Blog: 10 steps to securing your online environment: The Cybersecurity Tech Accord celebrates Cybersecurity Awareness month, 9 October 2018
- Blog: Basic cyber hygiene: The benefits of using a virtual private network (VPN), 7 August 2020
- Blog: Basic cyber hygiene: The importance of patching, 31 2020
- Campaign and information repository on IoT security: Stay Smart. Stay Safely Connected., 13 May 2020

Cyber hygiene for businesses

Vulnerability disclosure

- Blog: The Cybersecurity Tech Accord supports the GFCE's call for industry-wide adoption of transparent policies for coordinated vulnerability disclosure (CVD), 10 September 2018
- Blog: Leading by example. Cybersecurity Tech Accord welcomes new signatories and agrees to implement vulnerability disclosure policies across the group, 25 July 2019
- Blog: The Importance of vulnerability disclosure policies, 9 August 2019
- Blog: Operationalizing international cybersecurity norms: Vulnerability disclosure policies, 6 February 2020
- Webinar: Introduction to vulnerability disclosure, 22 June 2020

DMARC

- Blog: Cybersecurity Tech Accord joins cross-sector efforts to improve security of email communication; defend against most common and dangerous cyberattacks, 17 October 2018
- Blog: Dispelling the myths about DMARC, 25 March 2020
- Video: Introduction to DMARC, 22 June 2020

MANRS

- Blog: Cybersecurity Tech Accord endorses the MANRS initiative, joining efforts to eliminate the most common threats to the Internet's routing system, 9 August 2018
- Webinar: Introduction to Mutually Agreed Norms for Routing Security, 27 March 2020
- Blog: The MANRS initiative: Ensuring good practices are readily accessible to an even broader set of industry players, 31 March 2020

Domain Name System (DNS) Security

- Blog: Webinar: Securing Your Digital Assets From Cyberattacks Starts With Mapping Them To Your Risk Program, 12 November 2019
- Blog: Domain Name Security: Why businesses across the globe need to act now, 17 March 2020
- Video: Domain Name Security, 22 June 2020

Protecting against "password spray"

- Blog: Basic cyber hygiene: Protect against "password spray", 13 August 2020

Multi-factor authentication

- Blog: Multi-factor authentication (MFA): A foundational cyber defense for organizations, 6 October 2020