Guidebook on Staying Safe Online

Cyber Hygiene for Public Institutions and SMEs

By

Vladan Babić and Aleksandar Bratić

October 2022

DCAF Geneva Centre for Security Sector Governance

About DCAF

DCAF – Geneva Centre for Security Sector Governance is dedicated to improving the security of states and their people within a framework of democratic governance, the rule of law, respect for human rights, and gender equality. Since its founding in 2000, DCAF has contributed to making peace and development more sustainable by assisting partner states, and international actors supporting these states, to improve the governance of their security sector through inclusive and participatory reforms. It creates innovative knowledge products, promotes norms and good practices, provides legal and policy advice and supports capacity-building of both state and non-state security sector stakeholders. DCAF's Foundation Council members represent over 50 countries and the Canton of Geneva. Active in over 70 countries, DCAF is internationally recognized as one of the world's leading centres of excellence for security sector governance (SSG) and security sector reform (SSR). DCAF is guided by the principles of neutrality, impartiality, local ownership, inclusive participation, and gender equality. For more information visit www.dcaf.ch and follow us on Twitter @DCAF_Geneva.

DCAF – Geneva Centre for Security Sector Governance
Maison de la Paix
Chemin Eugène-Rigot 2E
CH-1202 Geneva, Switzerland
Tel: +41 22 730 94 00
info@dcaf.ch
www.dcaf.ch
Twitter @DCAF_Geneva
Photo credit: Shutterstock, image contributor: Illus_man
Design & layout: DTP studio

Contents

Introduction

This document is an overview of the minimum standards for establishing systems of cyber hygiene in public institutions and small and medium-sized enterprises (SMEs). It presents the measures that any organization should implement in order to ensure an adequate level of information security for its information systems.The focus here is on providing an introduction to the importance of cyber hygiene and recommending actionable steps that will improve cybersecurity within your organization.

In short, security hygiene is just like hand washing. When Hungarian doctor Ignaz Semmelweis uttered the three simple words “wash your hands” in 1850, he revolutionized medicine, even if no one took him seriously at first. He observed that good hygiene was inextricably linked to good health, and over time, data proved that preventive hand sanitization did reduce infections.

Cyber hygiene similarly refers to practices meant to prevent malware infections, as well as cyber intrusions and data loss or corruption, and maintain a healthy cyber environment. This ensures the health of systems and improves cybersecurity in the same way that routine handwashing helps prevent the spread of disease.

Given that all organizations use information systems to do business today, all are at risk of exposure to various cyberattacks that can prevent the functioning of information systems or block access to data. Thus, every organization must protect its information system(s) and must establish procedures and policies, and offer regular trainings, to establish adequate cyber hygiene practices.

Definitions

Many different definitions of cyber hygiene have been put forth, and all of them are accurate.

- Digital Guardian refers to cyber hygiene as “the practices and steps that users of computers and other devices take to maintain system health and improve online security.”
- Kaspersky Lab emphasizes that cyber hygiene “is about training yourself to form good habits around cybersecurity so that you can stay ahead of cyber threats and online security issues.”
- Security magazine describes cyber hygiene in terms of “making sure you have the fundamental security controls operating and that they are consistently applied across your environment.”
- CyberSecurity Forum notes that cyber hygiene “is a colloquial term that refers to best practices and other activities that computer system administrators and users can undertake to improve their cybersecurity while engaging in common online activities, such as web browsing, emailing, texting, etc.”
- Endpoint blog characterizes cyber hygiene as “a set of habitual practices for ensuring the safe handling of critical data and for securing networks. It is like personal hygiene, where you develop a routine of small, distinct activities to prevent or mitigate health problems.”

In other words, cyber hygiene is a set of basic security practices that can be taken by all personnel to protect themselves as well as the health of personal and organizational hardware, and software, in computer-based systems.

Common measures

Good cyber hygiene calls for the implementation certain common measures, from the establishment of standardized procedures and policies to regular trainings that help employees understand ever-evolving cyberthreats. The nature and character of some of these threats are outlined later in the text (see Common Cyberthreats). But first, the key elements of an effective cyber hygiene programme are detailed, as well as good practices.

Analyze systems and establish procedures and policies

Asset inventory

Maintain a hardware & software inventory

Managing IT hardware and software (IT assets) can be an overwhelming task, especially if equipment and personnel constantly move or change, but it is essential. Hardware, software, and all network and non-network devices count as assets for this purpose.

Maintaining a hardware and software inventory will support different processes in your organization, such as:

- Incident management
- Problem management
- Change management

And in these processes, similar questions are asked:

- What does this IT asset do?
- What kind of Operating System does it use?
- What applications are stored on/in the asset?
- What is the network topology?
- Who has access to the asset?
- Who is accountable for it?

To provide answers, a centralized information base is needed. Thus, a first step in establishing cyber hygiene practices is **standardizing the inventory of software and hardware** by:

1. Documenting the baseline security posture of the organization
2. Standardizing this across the organization based on policy and procedures
3. Monitoring and responding to deviations
4. Reducing any vulnerabilities introduced by rogue hardware and software

The benefits of maintaining a software and hardware inventory are quickly evident, and include:

- Control of the IT environment
- Control of software assets (version, patch, dependency, accountability, proof of concept (PoC))
- Control of hardware assets (version, criticality, PoC, dependency)
- Effective governance
- Better MTTRS (Mean time to restore service)

Information inventory

Maintain an inventory of sensitive or critical information

Protecting sensitive information – which entails properly labelling, discovering, and managing it – is extremely challenging. It can be hard to understand how users interact with and share this information. Thus, it is no wonder that more than half of corporate data is 'dark', meaning it is not classified, protected, or governed.

It is vital to **understand your data landscape and identify important data across your environment**. To this end, it is important to create a data classification policy as a first step. There are different classification schemes that may be used based on need, but the example below features three levels:

- **Restricted** – sensitive data that poses a great risk if compromised, accessed on a need-to-know basis.
- **Confidential** – moderately sensitive data, accessed only internally.
- **Public** – non-sensitive data that would cause a little or no risk at all if accessed.[1]

1 https://digitalguardian.com/blog/expert-guide-securing-sensitive-data-34-experts-reveal-biggest-mistakes-companies-make-data

As a second step, data should be encrypted, especially any data marked with a ‘restricted’ label.

Finally, a **data loss prevention system** should be implemented to detect potential data breaches/data exfiltration transmissions and prevent them by monitoring, detecting, and blocking sensitive data while in use, in motion, and at rest.

This should include some scanning and automation (for which Microsoft is a good tool), and should cover:

- On site repositories
- Office apps
- SharePoint sites
- Exchange
- Non-Microsoft cloud and SaaS apps

Risks assessment

Identify risks

Risk management requires an understanding of the threats your organization faces and the steps that can be taken to prevent, reduce, or prepare for situations that may or may not occur.

There are three areas of risk to information systems:

- **Human risk**, such as fraud, theft, or human error.
- **Natural risk**, like floods, fires, or earthquakes.
- **Technical risks**, such as software failures, hardware, or lack of knowledge.

As a starting point, assessing risk involves assigning value to critical assets, both financial and reputational. This will help you begin to evaluate how much concern specific threats pose. One effective way of doing this is by scoring each scenario – first, on the likelihood of occurrence, and second, on the harm its occurrence would cause.

This will give you a better understanding of where to focus efforts and will help you decide how to approach mapped risks, for example, by:

- **Avoiding**, when risks are not a direct concern to your business
- **Reducing**, when risks call for the implementation of a new security solution
- **Accepting**, when a risk is unlikely to occur or its prevention is beyond current capabilities
- **Transferring**, when a risk can be insured

Backup procedure

Establish a regular backup procedure

It is extremely important to have a backup procedure. The goal is to create a copy of data that can be recovered in the event of data failure – which can result from hardware or software failures, data corruption, or human caused events such as malicious attacks or accidental deletion. A well-conceived backup and restore policy, with clear procedures, is essential and represents the last line of defence for an organization.

Almost all organizations have some backup system in place. The question is, does it adequately meet the needs of your organization and the services you provide? It is important not to backup just for the sake of backing up, but to backup so that key data can be recovered when needed, and with as little impact as possible on operations.

For example, backups should cover day-to-day work, but should also allow for work when a system is down. Or, in a disaster context, data should be stored in a location where it can be recovered.

Organizations should be realistic in creating a backup policy, and should develop a written backup plan that details:

- What is being backed up?
- Where is it being backed up?
- How often will backups occur?

- Who is in charge of performing backups?[2]

Always give the highest priority to crucial data

Set a backup schedule based on how much work your organization is willing to risk losing. Keep in mind that database and accounting files are your most critical data assets, and should be backed up before and after any significant use. For most organizations, this means these files should be backed up daily. Yet, non-profits that do a lot of data entry should consider backing up their databases after each significant addition, even if this is more than once daily. Core files such as documents (in a 'Your Documents' folder, for instance) and email files should be backed up at least once a week, or even once a day.[3]

Always test your backups

By testing backups, you can see if they work the way you intended. This allows you to measure how fast your business operations can be restored after a failure, and to identify any issues that need to be addressed.

Use the 3-2-1 rule for backups

Professionals recommend a practice of backup redundancy known as the 3-2-1 rule. This translates to three copies of your data, on two local (but different) devices, and on one off-site device. This approach makes it highly unlikely that data will be lost.

Indeed, moving important files to a hard drive or flash drive does not constitute the creation of a sufficient backup. Hard drives fail. Further, flash drives and SD cards are small and easy to lose. A good backup system requires redundancy in the form of multiple copies, protected in the case of an unforeseen incident.

Use remote storage

Off-site or cloud storage solutions are a cost-effective and efficient way of ensuring your data is separate from your location, but still available to you.

Make frequent and regular backups

Today, there are tools that allow you to make backups automatically, and these are both easy to set up and affordable.

Incident response plan

Create an incident response team

An incident response team is a group of IT professionals within an organization who are charged with preparing for and reacting to any IT emergency that arises.

Typically, these professionals come from a variety of backgrounds and roles and have complementary technical skills, which ensures the team is able to respond to a wide range of security incidents, including a breach or cyberattack.

An incident response team is typically responsible for developing a response plan (see below) so that a methodical approach can be taken to addressing security incidents and managing the aftermath. The team also tests and resolves system vulnerabilities, maintains strong security practices, and provides support for incident-handling measures.

Create an incident response plan (IRP)

An IRP is a risk management tool that defines controls to reduce breaches or incidents and lays out what to do if a breach occurs. It will help mitigate the risk of a breach, assuming your organization has an incident response team.

It is important to keep in mind that incidents will occur regularly in any enterprise environment. Your

2 Your Organization's Backup Strategy, Articles and How-tos, techsoup.org

3 Ibid.

incident response team will need to prioritize which incidents must be addressed immediately and which can be addressed later. **The scope and goals of the incident response team are set by management in the IRP**.

Well-defined procedures that detail appropriate responses to incidents are imperative, especially as there may be cases in which incidents must be reported to local authorities, depending on the regulations that affect your industry. The structure of an IRP depends on the framework in use, such as ISO 28035 or NIST (preparation, detection & analysis, containment, eradication & recovery, post-incident activities).

When an incident occurs, it is critical that you follow your IRP, which will stipulate procedures for responding to different types of incidents.

Many incidents are caused by inside users, so it is important to train employees and other end-users in appropriate computer security and also monitor their use to ensure they are not engaging in malicious actions. To do that, organizations must:

- Communicate to end-users how to report an incident, with appropriate email addresses, portals, hotlines, and help desk information.
- Develop an internal page that lays out the details needed for proper reporting.
- Organize annual security trainings that include instruction on what to do in case of an incident (malware report, data leak report, spam & phish report, etc.).
- Train end-users to disconnect machines from the internet when an incident occurs, if your organization does not have technical measures in place to automatically contain an infected host.
- Teach end-users not to perform any action in the aftermath of an incident unless it is approved by the incident response team, in order to preserve necessary evidence for potential forensic investigation.
- Train end-users to offer as much information about an incident as possible, including:
    * What happened?
    * When did it happen?
    * Where did it happen?
    * Who was involved?
    * What additional information may speed up information gathering in the triage phase?

Continuity and disaster recovery

Establish a business continuity and disaster recovery plan

While business continuity refers to the recovery, restoration, and maintenance of an organization's entire operation in the face of a major unexpected disruptive event, disaster recovery refers here to specific activities that have to do with communications and technology infrastructure and data.

When an unplanned incident occurs, it is vital that an organization can resume work as quickly as possible. A business continuity plan is aimed at that goal in totality, and a disaster recovery plan sets out how an organization can efficiently and effectively recover access to its critical data and technology systems.

A disaster recovery plan therefore addresses two things fundamentally:

- restoring IT and communication systems and technology; and
- gaining full access to good quality, clean data on which the organization relies.

The type of unplanned disruptive events that could necessitate implementation of a disaster recovery plan include:

- Natural disasters
- War or terrorism
- Civil disruption
- Accidents or human error
- Cybercrime

Such events can cause varying degrees of disruption, affecting:

- A single data centre or building
- An entire organization
    * Local or city-wide systems
    * Regional or national systems
    * Global systems

An effective disaster recovery plan that minimizes disruption should consider potential commercial losses and the reputational impact on the organization, and should help an organization avoid regulatory or legislative breaches.

Six key elements should be spelled out in a disaster recovery plan:

1. A full inventory of assets (hardware, software, and data)
2. Minimum acceptable impacts (down time and service level)
3. Document disaster recovery processes and procedures (SLAs, restoration priorities, backup resources, data validation)
4. Disaster recovery responsibilities, both operational and authorizational; i.e., who performs disaster recovery actions and who approves them.
5. A communication and PR plan (to address key stakeholders and regulators, and protect an organization's reputation)
6. Training (a plan is of no use if no one knows how to use it)

Protect your information system

Patching and updating

Patch and update your operating system and application software

Keeping your system and applications up to date can feel like a nuisance at times, but it is very important to do, for several reasons:

1. **Safety**: updates help secure your computer against attacks. As new attacks are discovered, the gaps that cybercriminals use to compromise your operating system and applications are identified. Those gaps are addressed through updates.
2. **New features**: Microsoft, Apple, Android, and others offer additional features in updates, and other software from other companies sometimes cannot be used without first updating these systems.
3. **Fixes**: Not every problem is due to a virus. Sometimes, problems arise in systems and software and just need to be fixed. Many glitches that affect end-users are resolved in updates.

Thus, it is wise to **use automatic updates for systems and applications**. That way, essential security fixes that address system vulnerabilities are downloaded automatically.

Keep in mind: when that little update prompt appears, it might be a good thing; but it is still important not to click blindly.

Secure configurations

Use secure configurations for all devices and software

One way to protect people and organizations against malicious activity is to use secure configurations for devices and software. At the same time, this represents a significant challenge, by introducing an almost constant need for new operating system patches, upgrades to applications, and modifications to networks. Therefore, a primary goal is to document all updates and changes, to offer a view into the configurations for all systems.

When changes are made to an application, this requires modifying and updating the documentation created for that particular asset. Good documentation should enable the rebuilding of an entire instance

from the very beginning and should include:

- A log of changes to operating systems and applications (updates), network modifications, new application instances, etc. All of these must be documented and tracked accurately.
- A list of all assets in your organization. Any hardware and software should be identified and documented.
- A security baseline for assets. This is an agreed minimum security standard that applies for example to disabling unnecessary services, removing guest accounts, exposure to public internet, etc.
- A review and approval process that is easily tracked. It is good practice to review your configurations and settings from time to time, as incidents in your environment can offer hints as to what needs to be modified. Also, individuals should not change settings based on their own needs but should go through a standardized approval process.
- A log of configuration changes.

Documentation should also include:

- Diagrams of networks and devices, as well as the layout of physical data centres
- Application environment parameters:
    * Established baselines to follow
    * Firewall settings, patch levels, OS versions
- Naming conventions and standards, for:
    * Devices (asset tag name and number, computer name, location, serial number)
    * Networks (port labelling)
    * Domain configurations (account names, email address)
- IP schema
- For end-users, secure configuration requires:
- Removing and disabling unnecessary accounts
- Changing default or easily guessed (“weak”) passwords
- Removing or disabling unnecessary software
- Disabling any auto-run features that allow file execution without user authorization

Sensitive data

Encrypt all sensitive data

Encryption is the process of scrambling information so that it cannot be read without a key of some sort. For example, owners of encrypted data can unscramble it by using a password, biometric information, or other kind of key.

Encryption is a critical element of cybersecurity and can be used in several ways to keep data confidential and private, such as on secure (HTTPS) websites, in secure messaging applications and email services, and through virtual private networks (VPNs). Encryption protects information while it actively moves from one location to another (i.e., in transit), from sender to receiver, and also safeguards information while at rest. If someone gains access to a database in which encrypted information exists, encryption represents an additional layer of security.[4]

In other words, **encryption helps guard sensitive and private information by making it unreadable to cybercriminals**, even in the case they are able to exfiltrate that information.

Recognizing sensitive information in your unique environment that should be encrypted is vital, but typically this includes, among other things:

- Personally identifiable information
- Financial data
- Healthcare data
- Credit card numbers

4 Should I Encrypt Sensitive Files on My Computer?, Experian

Countering malware

Implement anti-malware software

Malware or malicious software is any programme designed to perform unwanted or harmful functions affecting computers, servers, and networks. Anti-malware software is thus a necessary part of a security toolkit.

Years ago, cybersecurity companies tried to create universal anti-virus solution that could address all our needs in one product. Yet, that's no longer effective, because cybercriminals have evolved. The threats they pose are becoming ever more sophisticated, leading companies to develop specific anti-malware programmes.

It is important to understand that all viruses are malware, but not all malware are viruses. A computer virus spreads from user to user by self-replicating, and anti-virus programmes identify known threats by detecting unique signatures. But modern malware scanners use heuristic detection, which can proactively search for malicious code.

Anti-malware solutions will block most malicious and potentially unwanted programs and will scan incoming data to prevent malicious software from executing on a device, changing settings, or loading additional compromised software. They also block users from visiting websites known to distribute malicious code (in phishing and ransomware attacks).

Beyond that, anti-malware software offers:

- Real-time protection
- Boot scans
- Scans of external devices
- Protection of sensitive information
- Protection from spam and identity theft

Firewalls

Implement firewalls

Firewalls provide protection against cyberattacks by helping guard computers and networks. Firewalls can be both software or hardware, on devices or a network, but all work in the same way by inspecting traffic and blocking unwanted packets.

A firewall will significantly reduce risk for individuals and organizations. Organizations that do not use firewalls are simply making the job of cybercriminals easier, allowing them potential access to systems and files as well as the ability to spread malicious content. A properly configured, maintained, and monitored firewall is therefore key to protecting your data, your network, and your devices.

Among other things, a firewall helps secure you from:

- Remote logins
- The hijacking of email sessions
- Application and OS vulnerabilities
- DoS
- Email bombs
- Malicious macros

WI-FI networks

Protect your WI-FI networks

WI-FI networks should be secure, encrypted, and hidden:

- **Wireless network encryption must be turned on**. Encryption is essential to security. Hence, your router must support WPA2 encryption, and it should be replaced if it does not.
- **Keep software up to date with security updates and patches**.
- Consider the location of routers as a matter of security. Often, people are unaware that a router

positioned near a door or window increases the chance that a WI-FI signal will be intercepted by someone with malicious intent. To improve WI-FI security, **it is best to place your router as close to the centre of your office as possible**, as this will reduce the chance that hackers can connect to your network.
- **Enable MAC address filtering** to control the devices that have access to your network.
- **Disable remote administration**.
- **Create a separate WI-FI network for clients**, to avoid them accessing your internal network.

Web browser settings

Configure web browser security settings

Web browsers exist on almost all devices. Since they are relied on heavily in everyday life, it is vital to configure them securely, especially since they are usually used on default settings.

Web browsers represent a significant target of attack for cybercriminals to exploit, and an insecure browser can leave users or organizations open to the installation of malicious content without the user's knowledge. In some cases, this can lead to a loss of control over a device, the use of a user's information, or even the use of a device to attack others.

Any web browser (Firefox, Chrome, DuckDuckGo, Brave, etc.) should be secured. In doing so, be sure to:
- **Enable automatic updates**. This **crucial step** will defend your organization against the many vulnerabilities discovered daily. This is an essential part of the proper cyber hygiene of your web browser, and it will help you stay safe and secure.
- **Block pop-ups**, **plugins**, **and phishing sites**. Most pop-ups are ads, which can be infected with malicious content; and plugins are known for their security risk implications.
- **Do not store passwords**. This habit of convenience is not recommended because, if a browser is compromised, so are any stored credentials.
- **Disable third-party cookies**.
- **Uninstall any unused browser extensions**.
- **Regularly update any extensions that are used**.
- Personal choice also plays a role in browser security, such as by users accessing **https sites instead of http sites**.

Mobile devices

Secure mobile devices

Mobile devices can create significant security and management challenges, especially if they hold confidential information or can access a corporate network.

To manage the use of mobile devices, organizations should require users to:
- password-protect devices;
- encrypt all data; and
- install security apps that prevent the theft of information when a phone uses public networks.

Organizations should also:
- Set reporting procedures for lost or stolen equipment.
- Configure devices to lock automatically after a set period of time.

IoT devices

Secure IoT devices

The growing importance of technology in our lives has fostered the "Internet of things", or IoT. This means that a large number of devices are connected to the internet through IoT sensors that allow them to collect real-time data and share it. By collecting data from physical and virtual systems, the IoT represents a sizeable "attacking surface" for cyberattackers, if not properly secured.

Securing an IoT network means securing devices before they join the network. To do so:

- Change default passwords
- Use strong passwords
- Update the software on devices (always verify available updates from manufacturer websites before applying them to devices)
- Encrypt and authenticate devices
- Change default privacy settings
- Change default settings
- Ensure the security of your network and WI-FI
- Create a guest network

Physical security

Take care of the physical security of devices, especially mobile devices

Physical security is just as important as cybersecurity. If a thief steals a laptop or mobile device, the most immediate loss is the device itself, but if the thief is able to access information on a device, all of that information could be at risk. There is also the potential that additional information could be accessed by using the data stored on these devices, including sensitive corporate or customer account details – such as passwords or credit card information – that should not be accessed by unauthorized individuals.[5]

To protect yourself and others in your organization:

- Secure your device with a password and implement two-factor authentication (2FA)
- Keep valuables with you at all times and never leave devices unattended, especially when traveling

Remote access

If your organization uses remote access, it should be secure, encrypted, and hidden. This calls for:

- Ensuring all remote access software is patched and up-to-date.
- Restricting remote access from suspicious geographical locations or IP addresses.
- Restricting the remote access of employees to only the systems and computers they need to do their work.
- Requiring strong passwords to gain remote access.
- Enabling multi-factor authentication, if possible.
- Ensuring that monitoring and alerting is enabled to warn of suspected attacks or suspicious activity.

Apply good practices

Passwords

Every organization should have a password policy to ensure that complex and separate passwords are used and are changed regularly. Passwords represent the first line of defence against unauthorized access.

A password policy is necessary to avoid some of the most common vulnerabilities, such as:

- The habit of users to store passwords in notes, text files, or other unprotected documents that can be easily accessed by cybercriminals.
- The tendency of users to save passwords in browsers, which represents another target for cybercriminals.
- Passwords that include personal information easily obtained online.
- The use of only one password for multiple accounts.
- The sharing of passwords with colleagues, or through email, instant messages, or other platforms (this is especially a vulnerability if passwords are not changed regularly).

5 https://www.cisa.gov/uscert/ncas/tips/ST04-017

The easiest way to change or mitigate the behaviour of users related to passwords is to **use a password manager**. This allows for the creation of complex passwords for different accounts, all of which are encrypted and stored, so that users only need to memorize a single master password to access their password vault. A password manager helps users generate passwords and indicates how strong a password is, and can also notify users about security breaches involving their email, and more.

If your organization does not use a password manager, here are some **tips for creating a password policy**:

- **Longer passwords are better** because they take longer to hack. Passwords should thus contain a minimum of 12 characters.
- **Complexity is key**! Passwords should include symbols, a combination of lower and uppercase letters, and numbers. And then they should be scrambled.
- **Use gibberish** and avoid predictability. Ideally, passwords should not include words that can be found in dictionaries (in any language).
- **Keep passwords unique**. The rule in any organization should be: one account, one password.

It is also important to **change default passwords** before giving devices to employees, to avoid risks related to the possibility of exposure to hackers or some other major breach.

Multi-factor authentication

Use multi-factor authentication whenever possible

There are three ways that a computer, or any system, can identify a user. It can ask for something a user knows, is, or has. These are the **three factors of authentication**. The gold standard for verifying identity is a multi-factor authentication that uses at least two of these factors.

The idea is that two different passwords are not much better than one, but two factors are. This is why a cash withdrawal from an ATM requires two-factor authentication: something a person has (an ATM card), and something a person knows (their PIN).

Passwords alone are no longer considered secure, as hackers have developed countless methods over the years to steal the necessary credentials to get unauthorized access to private accounts. The sad truth is that almost 90% of such incidents could be blocked with the use of multi-factor authentication.

Organizations should implement two-factor authentication (2FA) for users wherever possible, to:

- secure users from identity theft via a stolen password.
- protect organizations from weak employee passwords.
- mitigate the use of unmanaged devices, especially with increased rates of work from home during the COVID pandemic.
- increase the effectiveness of other security measures.
- help organizations remain compliant.

Accounts

Use limited accounts for regular and everyday purposes

Accounts must be treated with care, as account misuse can lead to the loss of information, organizational reputation, and money.

There are two types of accounts: Standard User and Administrator.

The characteristics of a Standard User account are that it is:

- more suitable for everyday tasks (using apps, browsing the web);
- configured to protect your system from obvious attacks; and
- does not allow users to make changes that affect everyone who uses a computer.

Standard User accounts have less flexibility than Administrator accounts. But, on the other hand, malware installed under a Standard User account can do little damage to system files. This is because attackers who gain access to a Standard User account can access only that user's files. In this sense, restrictions

on Standard User accounts work in an organization's favour should an adversary or malicious program gain access.[6]

Employee access

Employee access should be limited so that no employee can access all data systems

It is recommended that no single employee be given access to all data systems. Employees should only be given access to the specific data systems they need to do their jobs.

Do not allow employees to install software without permission

Employees should never be able to install software without permission.

Logging

Maintain logging

From a security perspective, a log acts as a red flag when something bad is taking place. Regularly reviewing logs can help identify malicious attacks on your system.

Indeed, a log that is easy to access and includes crucial information can save an information or computer system. Logging will help with:

- Debugging
- Error tracking
- Performance troubleshooting
- Accounting
- Auditing
- Security

Notably, log files can also be used to maintain regulatory compliance. Many organizations must comply with various regulations that require an auditing of activities, including the provisioning of user accounts or access to financial systems.

The biggest issue related to logging is a lack of monitoring. It is important to understand what must be logged, based on best practices, and to review logs on a daily basis in search of errors, anomalies, or suspicious activity. Still, excessive logging is not helpful, as it creates a lot of "noise" and requires more storage capacity. Hence, some activities may need to be prioritized for logging over others.

Cybersecurity awareness

Common cyberthreats

A cyberattack is a malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization. Usually, the attacker seeks some type of benefit from disrupting the target's network. Organizations face myriad cyberthreats, and attackers use a variety of strategies to attempt or carry out attacks.

Social Engineering Attacks

Social engineering attacks mislead and manipulate targets, to obtain information or gain access to their computers. This kind of attack relies on human interaction and usually involves the manipulation of a user so that they violate security procedures and best practices to gain unauthorized access to systems or share sensitive information.

6 Why You Shouldn't Use an Admin Account as Your Main Account, Make Tech Easier

In social engineering attacks, cybercriminals hide their true identities and motives, presenting themselves as trusted individuals. The attack is then executed by tricking users into clicking malicious links or by physically gaining access to a computer.

Phishing

A majority of cyberattacks begin with a phishing email. Phishing is a type of social engineering attack in which cybercriminals trick victims into handing over sensitive information or installing malware.

Even while technical security measures continue to improve, phishing remains one of the cheapest and easiest ways for cybercriminals to gain access to sensitive and personal information. Users merely have to click on a link and their security can be jeopardized to the extent that they may become victims of identity theft. Users can also compromise their personal information, login credentials (usernames and passwords), and financial information (credit card numbers) if they click the link.

Often, attackers achieve this through malicious emails that appear to be from trusted sources. But sometimes, they use other methods, too.

How does phishing work?

Most phishing campaigns employ one of two basic methods:

1. **Malicious attachments** in emails, which usually have alarming subject lines like 'INVOICE'. When opened, these attachments install malware on a user's machine.
2. **Links to malicious websites** that are often clones of legitimate sites. Navigating to the site can trigger the download of malware, or the site's login page may contain credential-harvesting scripts.[7]

Types of phishing attacks

Spear Phishing

Spear phishing is a malicious email spoofing attack that targets a specific organization or individual, pursuing unauthorized access to sensitive information. Spear phishing attempts are not likely to be executed by random attackers, but by cybercriminals seeking financial gain or other valuable information.[8]

In a spear phishing attack, an email is sent from a reliable source but leads to a fake website mined with malware. These emails tend to use creative means to get the attention of users.

Spear phishing is much more effective than other phishing attacks, but requires that cybercriminals spend time and resources undertaking pre-attack research, as they will be more successful if they learn about their target before launching an attack.

Whale Phishing/Whaling

Whale phishing is similar to spear phishing, with a few notable differences. Whereas spear phishing is usually directed at members of a group, whale phishing is focused on a specific individual – usually the 'biggest fish' at a target organization or an individual with noteworthy wealth or power.

Vishing

Vishing, or "voice phishing", involves the manipulation of people over the phone. Attackers seduce a target into revealing sensitive information in an attempt to use this data for their own benefit, typically to gain financially.

Smishing

The term smishing refers to SMS phishing, and involves a text message rather than an email. Targets generally receive a misleading text message that compels them to provide personal or financial information to a cybercriminal pretending to be a government agency, bank, or other legitimate company.

7 What is phishing? Everything you need to know, IT Governance UK

8 Types of Cyber Threat in 2019, IT Governance USA

Smishing attackers often seek personal or bank account information, such as account credentials, credit card numbers, and identification numbers. Then, they use that information to carry out various attacks, including financial, gift, or customer support fraud.

How to prevent phishing attacks

In Email: learn to look carefully at emails, especially if they contain attachments and web links

Educate employees on how to recognize phishing attempts and report suspected encounters. Here are some tell-tale signs that an email might be malicious:

- **Poor spelling and grammar**. Professional companies or organizations usually have an editorial staff to ensure customers receive high-quality, professional email content. If an email message is fraught with errors, it is much more likely to be a scam.
- **Suspicious links.** Users should never click any links in an email message they suspect may be malicious. One way of testing the legitimacy of a link is to rest the mouse – without clicking –over the link, to see if the address matches information in the message.
- **Suspicious attachments**. If a user receives an email with an attachment, either from someone they don't know or from someone they were not expecting to send an attachment, they must consider whether it may be a phishing attempt. It is recommended that attachments are never opened until their authenticity is verified. Because there are multiple ways attackers can trick recipients into trusting that an attached file is legitimate, it is important that users know:
    * The icon associated with an attachment cannot be trusted without other verification.
    * They should be wary of combined file extensions, such as 'pdf.exe', 'rar.exe', or 'txt.hta'.
    * The best course of action, if in doubt, is to contact the person who ostensibly sent the email message in question, to ask them to confirm that the email and attachment are legitimate.
- **Coercive messaging**. These emails are meant to cause a sense of panic or pressure, to generate a quick and unconsidered response from the recipient. For example, they may include a statement like, 'You must respond by end of day!' Or, they may imply that the recipient faces potential financial penalties for failing to respond.
- **Spoofing**. Spoofing emails use **suspicious links** that appear to connect to legitimate websites or companies and may display legitimate-looking pop-up windows, but which take users to phony scam sites. One form of spoofing uses **altered web addresses** that very closely resemble the names of well-known company websites, such as 'www.micorsoft.com' or 'www.mircosoft.com'.
- **Mismatches**. Recipient should be suspicious if the text of a link and URL do not match, or if the sender's name, signature, and URL do not match.[9]

Public WI-FI: Take care when using public WI-FI networks

We are surrounded by public WI-FI networks in hotels, malls, coffee shops, airports, etc. Many of us have gotten in the bad habit of connecting to these networks without a second thought about security. Yet, they pose real security risks and should be used with caution.

The biggest security problem with public WI-FI is that users do not know who runs the network or who else is sharing the network.

Hence, organizations should:

- **Train employees on the risks of using public WI-FI**.
- **Forbid employees from accessing sensitive data while using public WI-FI**.
- **Instruct employees to connect only to trusted networks**.
- **Forbid employees from connecting to password-protected sites when using public WI-FI**.

Instead of using public WI-FI, other options should be considered. A phone can serve as a mobile hotspot, for example, allowing the device owner to control the network and who uses it. If public WI-FI must be used, a VPN can be engaged to encode any data being sent over WI-FI, which hides this data from anyone who is "listening" on the same network.

9 Protecting against coronavirus themed phishing attacks, microsoft.com

Business email compromise

Business Email Compromise (BEC) is a type of scam that targets companies which conduct wire transfers and have suppliers abroad. Corporate or publicly available email accounts of executives, or of high-level employees who handle finance or are involved with wire transfer payments, are either spoofed or compromised through key loggers or phishing attacks to carry out fraudulent transfers. This can result in hundreds of thousands of dollars in losses.[10]

Drive-by downloads

In a drive-by download attack, downloads of malicious script end up on a computer or other device without the user's knowledge, exposing the user to various cyberthreats. This can happen on any device running any operating system and usually occurs when a user navigates to and browses a compromised website.

Man in the middle (MITM) attacks

An MITM attack takes place when a cybercriminal secretly inserts themselves between devices, or between a device and an insecure WI-FI network, to intercept communications that may then be read and/or modified. In such a case, a user can unintentionally pass credentials or other information to the cybercriminal.

USB drop attacks

In a USB drop attack, a USB device containing malicious code is plugged into a computer.

Typically, the cyberthreat posed by this kind of attack is malware or virus infection. Infection through a USB drive can be both intentional and unintentional, depending on the malware in question.

Organizations would be wise to stop trusting obsolete USB technology, and embrace the power of secured digital networks by using cloud storage.

Malware

Malware is a general term used to define any file or program intended to harm or disrupt a computer. This includes:

- **Botnet software** designed to infect large numbers of devices connected to the internet. Some bot-nets comprise many devices, each using a relatively small amount of processing power. This can make it difficult to detect this type of malware, even when the botnet is running.
- **Ransomware attacks**, which encrypt user information and require payment in return for the de-cryption key, to retrieve the information. Paying a ransom does not necessarily guarantee recovery of the encrypted data, though.
- **Spyware** used to illicitly monitor a user's computer activity and harvest personal data.
- **Trojans** that appear as legitimate software but perform malicious activity when executed.
- **Viruses and worms**, which are malicious code installed without the user's knowledge. Viruses can replicate and spread to other computers by attaching themselves to other computer files. Worms are also self-replicating, but do not need to attach themselves to another program to do this.[11]

DoS/DDoS Attack

A Distributed Denial-of-Service (DDoS) attack is a cyberattack in which the attacker floods a server with internet traffic to prevent users from accessing connected online services and sites.

A DDoS attack is a subcategory of the more general Denial-of-Service (DoS) attack. In a DoS attack, the

10 https://www.trendmicro.com/vinfo/hk/security/definition/business-email-compromise-(bec)

11 Types of Cyber Threat in 2019, IT Governance USA

attacker uses a single internet connection to barrage a target with fake requests or to try and exploit a cybersecurity vulnerability. DDoS is thus larger in scale, utilizing thousands (even millions) of connected devices to fulfil its goal. This sheer volume of devices makes DDoS much harder to fight.[12]

There are three general types of DDoS attacks:

- **Volumetric attacks**: In this classic type of DDoS attack, methods to generate mass volumes of traffic are employed to completely saturate website bandwidth, creating a traffic jam that makes it impossible for legitimate traffic to flow into or out of the targeted site.
- **Protocol attacks**: These attacks are designed to eat up the processing capacity of network infrastructure resources like servers, firewalls, and load balancers by targeting Layer 3 and Layer 4 protocol communications with malicious connection requests.
- **Application attacks**: Among the more sophisticated DDoS attacks, these attacks exploit weaknesses in the application layer – Layer 7 – by opening connections and initiating process and transaction requests that consume finite resources like disk space and available memory.[13]

Regular trainings

To **raise awareness about cyberthreats and information security**, security awareness training is one of the most important cyber hygiene elements that can be implemented by any organization, to teach employees how to avoid, identify, and report potential threats.

Enrolling staff in a robust security awareness training course is one of the proactive measures organizations can take to ward off cyberattacks. Without accounting for this human element, the door of your organization is left open to cyberthreats.

Security awareness training helps increase user knowledge about potential threats, which:

- decreases risk;
- prevents downtime;
- improves employee confidence; and
- fosters client trust.

Security awareness training is thus vital to effective cybersecurity and cyber hygiene. And over time, annual security awareness trainings can change the cybersecurity culture in your organization. At minimum, these trainings should include information about:

- Sensitive information: what it is and how to handle it
- How to recognize phishing emails
- How to properly use company devices
- How to report incidents
- What to do in case of an emergency that impacts computer and information systems
- How to handle personally identifiable information (PII)
- Basic cyber hygiene: what it is and how to implement it

Expanded trainings should focus on content, support materials, phish testing, metrics, reporting, and surveys.

Successful security awareness training programmes:

- Educate and support employees without discouraging or shaming them.
- Do not focus only on phishing campaigns (the goal is that employees learn to recognize and report real-time threats, which take on myriad and ever-changing forms).
- Avoid reiterating the same content and seek to enrich employees new information in every training.
- Include material that relates beyond the professional world to the private lives of employees, as this personalizes the content and may make employees more willing to listen.

It is recommended that outcomes of trainings – positive or negative – remain internal and are not shared with stakeholders.

12 https://www.fortinet.com/resources/cyberglossary/ddos-attack

13 https://cybersecurity.att.com/blogs/security-essentials/types-of-ddos-attacks-explained

Summary

Almost all cyberattacks take advantage of conditions that fall under the umbrella of poor cyber hygiene. This includes missing patches, bad configurations, and poor user awareness. A lack of consistent cyber hygiene is therefore one of the most pernicious threats that can emanate from inside an organization. To foster good cyber hygiene across your organization:

- Provide employees ample training to identify and report suspicious cyber activity.
- Ensure that all servers, workstations, smartphones, and other devices used by employees receive frequent security updates.
- Implement a strong system access management policy requiring multi-factor authentication whenever possible and strict password standards.
- Invest in systems and solutions that enable clear visibility and granular control access to the organization's entire network infrastructure.

While it may seem that complexity would be the enemy of cybercriminals, it is in fact the enemy of your own cybersecurity. In a complicated and dynamic digital world, your best defence is actually getting back to the basics.

To improve cyber hygiene and scale it up, it is not enough for an organization to simply offer examples to employees and declare the importance of cybersecurity. In any organization, cyber hygiene must be specifically defined and then supported through metrics and education.

A security framework is a great starting point, but it should be:

- Right-sized to your organizational needs
- Aligned with your unique regulatory requirements
- Complemented by training that is available & affordable for your organization
- Maintainable/repeatable with your organizational resources
- In support of your business and operational goals

Conclusion

Ultimately, bad cyber habits – or poor cyber hygiene – are the cause of most successful cyberattacks. This is why it is so important for organizations to develop a culture of good cyber hygiene. But the measures recommended in this Guidebook, though presented mostly through the lens of organizational security, are applicable to both organizations and individuals. Organizations should thus emphasize to employees that they consider implementing cyber hygiene habits at home as well. After all, good cyber hygiene habits practiced at home are even more likely to be practiced at work. Moreover, we are all safer in the cyberworld when a culture of cyber hygiene extends across both personal and professional spaces.

References

ENISA: Review of Cyber Hygiene practices https://www.enisa.europa.eu/publications/cyber-hygiene

Centre for Cyber Security Belgium: Cyber security guide for SME https://ccb.belgium.be/sites/default/files/CCB-EN%20-C.pdf

ANSSI: Guideline for a healthy information system https://www.ssi.gouv.fr/uploads/2013/01/guideline-for-a-healthy-information-system-in-42-measures_v2.pdf

CPME-ANSSI: Guide Des Bonnes Pratiques De L'informatique https://www.ssi.gouv.fr/uploads/2017/01/guide_cpme_bonnes_pratiques.pdf

NIST: Small business information security: the fundamentals https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf

CISA: Cyber Essentials Starter Kit https://www.cisa.gov/sites/default/files/publications/Cyber%20Essentials%20Starter%20Kit_03.12.2021_508_0.pdf

CMU SEI: Cyber Hygiene: 11 Essential Practices https://insights.sei.cmu.edu/blog/cyber-hygiene-11-essential-practices/

Canadian Centre for Cyber Security: Cyber Hygiene https://cyber.gc.ca/en/guidance/cyber-hygiene

Kaspersky: Good cyber hygiene habits to help you stay safe online https://www.kaspersky.com/resource-center/preemptive-safety/cyber-hygiene-habits

ANSSI: 40 Essential measures for a healthy network https://www.ssi.gouv.fr/uploads/2013/01/guide_hygiene_v1-2-1_en.pdf

US House of Representatives: Promoting Good Cyber Hygiene Act of 2017 https://www.congress.gov/115/bills/hr3010/BILLS-115hr3010ih.pdf

NCSC NL: Cyber Hygiene in the Netherlands https://english.ncsc.nl/research/research-results/cyber-hygiene-in-the-netherlands

NIST NCCoE: Critical Cybersecurity Hygiene: Patching the Enterprise https://www.nccoe.nist.gov/projects/critical-cybersecurity-hygiene-patching-enterprise

CISA: Cyber Hygiene Services https://www.cisa.gov/cyber-hygiene-services

CYBER4Dev: Cyber Security Hygiene/Awareness https://cyber4dev.eu/cyber-security-hygiene-awareness/

eGA: What is Cyber Hygiene? https://ega.ee/blog_post/podcast-what-is-cyber-hygiene/

Annex: Good practices checklist

ANALYZE SYSTEM AND ESTABLISH PROCEDURES AND POLICIES		
Category	**Good practices**	**Relevant stakeholders**
Hardware & software Inventory	- Maintain a hardware & software inventory - Standardize your software and hardware inventory	Public institutions & SMEs
Sensitive or critical information inventory	- Maintain an inventory of sensitive or critical information - Understand your data landscape and identify important data across your environment - Create a data classification policy - Encrypt data, especially data classified as “restricted” - Implement a data loss prevention system	Public institutions & SMEs
Risk analysis	- Identify risks • human risk (fraud, theft, human error) • natural risks (floods, fires, earthquakes, etc.) • technical risks (software failures, hardware, lack of knowledge) - Avoid risk – if not a direct concern to your business - Reduce risk – by implementing new security solutions - Accept risk – if it is unlikely to occur or beyond your organization’s current capabilities - Transfer risk – through insurance	Public institutions & SMEs
Backup procedures	- Establish a regular backup procedure - Be realistic in creating a backup policy, and develop a written backup plan that stipulates: • What is being backed up? • Where is it being backed up? • How often will backups occur? • Who is in charge of performing backups? - Always give the highest priority to crucial data - Always test backups - Apply the 3-2-1 rule - Use remote/cloud storage - Update frequently and regularly	Public institutions & SMEs
Incident response	- Create an incident response plan or IRP - When an incident occurs, it is critical the IRP is followed	Public institutions
Business continuity and disaster recovery	- Establish business continuity and disaster recovery plans	Public institutions

PROTECT YOUR INFORMATION SYSTEM		
Operating system and application software	- Patch and update your operating system and application software, for: • Safety • New features • Fixes - Turn on automatic updates for both systems and applications	Public institutions & SMEs
Secure configurations	- Use secure configurations for all devices and software - Document all updates and changes • Log constant changes • Establish a security baseline • Implement a review and approval process • Log configuration changes	Public institutions & SMEs
Sensitive data	- Encrypt all sensitive data - Encryption helps guard sensitive and private information by making it unreadable to cybercriminals, as it can only be accessed with a key	Public institutions & SMEs
Anti-malware software	- Use anti-malware software - Anti-malware solutions will block most malicious and potentially unwanted programs	Public institutions & SMEs
Firewalls	- Use firewalls, in order to: • block most malicious and potentially unwanted programs • prevent malicious software from executing on a device • prevent malicious software from changing settings • prevent malicious software from loading additional compromised software	Public institutions & SMEs
WI-FI networks	- Protect WI-FI networks - Use wireless network encryption - Keep software up-to-date with security updates and patches - Place WI-FI routers as close to the centre of your organization as possible - Enable MAC address filtering - Disable remote administration - Set up a separate WI-FI network for guests	Public institutions & SMEs
Web browser settings	- Configure web browser security settings universally - Block pop-ups, plugins, and phishing sites - Do not allow passwords to be stored - Disable 3rd party cookies - Uninstall unused extensions - Regularly update extensions that are used - Encourage users to access https sites instead of http sites	Public institutions & SMEs
Mobile devices	- Require users to: • Password-protect devices • Encrypt data • Install security apps to prevent cybercriminals from stealing information while the device is connected to public networks • Configure device to lock automatically - Set reporting procedures for lost or stolen equipment	Public institutions & SMEs
IoT devices	- Secure IoT devices by: • changing default passwords • using strong passwords • updating device software regularly • encrypting and authenticating devices • changing default privacy settings • changing default settings • ensuring the organization's network and WI-FI are secured • creating a guest network • always verifying available updates on the manufacturer website before applying to devices	Public institutions & SMEs
Physical security of devices	- Take care of the physical security of devices, especially mobile devices, by: • Protecting devices with strong passwords • Keeping valuables with users/owners at all times	Public institutions & SMEs

Remote access	- Ensure all remote access software is patched and updated - Restrict remote access from suspicious geographical locations or certain IP addresses - Restrict remote access of employees to only to the systems and computers they need to do their work - Enforce strong passwords for remote access - Enable multi-factor authentication if possible - Ensure monitoring and alerting is enabled to warn of suspected attacks or suspicious activity	Public institutions & SMEs
APPLY GOOD PRACTICES		
Passwords	- Longer passwords are better - Complexity is key! Require symbols, lowercase and uppercase letters, and numbers - Use gibberish and avoid predictability - Keep all passwords unique - Change all default passwords	Public institutions & SMEs
Multi-factor authentication	- Use multi-factor authentication whenever possible - Use two of the three factors of authentication – something a user knows, is, or has	Public institutions & SMEs
Accounts	- Use limited (Standard User) accounts for regular and everyday purposes - Establish Standard User and Administrative accounts for different purposes	Public institutions & SMEs
Employee access	- Do not provide any single employee access to all data systems - Provide employee access only to the systems they need to do their work - Do not give employees the freedom to install software without permission	Public institutions & SMEs
Logging	- Maintain consistent logging - Be sure to understand what logs are necessary based on best practices, and review them daily in search of errors, anomalies, or suspicious activity	Public institutions
CYBERSECURITY AWARENESS		
Common cybers threats	TYPE OF CYBERTHREAT	RECOMMENDATIONS

	- Social Engineering
	- Phishing Attacks
	  • Spear Phishing
	  • Whale Phishing/Whaling
	  • Vishing
	  • Smishing
	- Business Email Compromise
	- Drive-By Downloads
	- MITM Attacks
	- USB Drop Attack
	- Malware
	  • Botnet software
	  • Ransomware attack
	  • Spyware
	  • Trojan
	  • Viruses and worms
	- DoS/DDoS attacks
	  • Volumetric
	  • Protocol
	  • Application
		- EMAILS: Take care with emails, especially if they contain attachments and web links. Look for:
		  • Spelling and bad grammar
		  • Suspicious links
		  • Suspicious attachments
		  • Threatening language
		  • Spoofing
		  • Altered web addresses
		  • Mismatches
		- PUBLIC WI-FI NETWORKS: Always exercise caution when connecting to public WI-FI networks, by:
		  • Not accessing sensitive data
		  • Only connecting to trusted networks
		  • Opting not to connect automatically

		Public institutions & SMEs

Regular trainings	- Raise awareness about cyberthreats and information security through annual or more frequent trainings
	- A robust security awareness training course should cover:
	  • Sensitive information: what it is and how to handle it
	  • How to recognize phish email
	  • How to properly use company devices
	  • How to report incidents
	  • What to do in case of emergency that impacts computer and information systems
	  • How to handle personally identifiable information (PII)
	  • Basic cyber hygiene: what it is and how to implement it
		Public institutions & SMEs

DCAF Geneva Centre for Security Sector Governance

DCAF Geneva Headquarters

P.O.Box 1360
CH-1211 Geneva 1
Switzerland

info@dcaf.ch
+41 (0) 22 730 9400

www.dcaf.ch

@DCAF_Geneva