A Digital Security Guide for Everyone

A publication by

cameco+

About This Publication

Our professional and personal lives are becoming more and more digitalized, forcing each one of us to face a reality that is as full of risks as it is full of new opportunities and possibilities.

The challenge is to increase our understanding of this phenomenon so that we can remain alert without becoming panic-stricken. The need of the hour is to identify the resources we already possess to deal with the risks and any potential crises. The question, therefore, is: How can we obtain a level of digital literacy that is adequate without each one of us having to become an expert in the field?

This guide is meant for anyone, whether an employee or not, who is willing to understand some of the key concepts around digital security. The aim is to make readers aware of what the experts are saying, and help them implement the best practices to protect their data, information, and assets.

The guide begins with an introduction to a main concept or category (for example, virtual private networks and password security) followed by relevant recommendations regarding use (how to have stronger passwords, whether should one opt for a personal VPN, etc.).

The last part of the guide consists of final recommendations, a glossary, references, and additional resources for further in-depth exploration of the topics discussed here.

We recommend devoting at least two hours to this document. Please refer to the table of contents if you are looking for a specific subject.

Finally, we gratefully acknowledge the experts who (as well as the organizations that) work in the fields around digital security and share our interest in and commitment to promoting security in this realm, and whose ideas and expertise have informed and shaped the content of this guide. Their tireless work continues to impact and improve lives in the digital world.

The guide is designed and drafted by Emy Osorio Matorel, Advisor for Digital Analysis and Strategy at CAMECO.

We wish you the best of luck in your efforts to be digitally safe!

About CAMECO

The Catholic Media Council (CAMECO) is a non-profit consultancy specializing in media and communications in Africa, Asia, Latin America, Central and Eastern Europe, the Middle East, and the Pacific. CAMECO offers its services to local partners, organizations active in delivering media assistance, and donors, among them many faith-based agencies.

Through our work, we aim to:

- support donors in assessing and evaluating media and communication projects and proposals, identify any relevant risks and challenges, as well as the opportunities and potential they offer;
- advise partner organizations on methods and approaches to develop, plan, implement, and monitor media and communication projects, and the ways and means in which to establish a sustainable financial and organizational footing;
- and help raise awareness regarding methods of audience research, participation, and interaction to build and strengthen a relationship between media and communication initiatives and their target groups.

About the Author

Emy P. Osorio Matorel is an experienced Social Communication professional from Universidad de Cartagena, Colombia. Specialized in journalism and culture, she currently works as the Digital Analysis and Strategy Advisor at CAMECO, and is a member of the Association for Media and Communication Research (IAMCR).

During her studies, Emy spent a year abroad with an Erasmus Mundus PUEDES Action 2 scholarship at Aristotle University in Thessaloniki, Greece.

Throughout her career, she has collaborated with well-known organizations such as the Global Forum for Media Development, Internews, La Silla Vacia, the Kettering Foundation, Fundacion Gabo, and Women's Link Worldwide. This experience of collaboration has resulted in her formidable expertise in journalism, strategic communication, and humanitarian efforts, endowing her with a profound understanding of various media-related fields.

With over seven years of work experience, Emy has developed her skills in media development, advocacy, and impactful social research. She is deeply committed to promoting digital inclusion, nurturing the ethics of digitalization, and contributing to the growth of media in the Global South, especially in Latin America and the Caribbean.

Page of Contents

Page of Contents

Digital Security

About Digital Security

1. What is digital security?

Digital security refers to a range of tools and methods aimed at safeguarding your online identity, data, and assets.

This includes resources like web services, antivirus software, smartphone SIM cards, biometrics, and secure personal devices. Put simply, it is all about the steps and precautions you need to take to keep your online identity safe.

2. Are digital security and cybersecurity the same?

As explained by the OECD, digital security refers to the economic and social aspects of cybersecurity, compared to those that are purely technical, and are related to criminal law enforcement or national and international security.

In other words, digital security focuses on the means through which you, as an individual, can protect your online identity, data, and assets, while cybersecurity is meant to ensure protection from cyber threats posed by internet-connected systems involving hardware, software, and data.

3. Why should you care about digital security?

Our lives are becoming increasingly digitalized. While this is helping us become more efficient in many ways, it is also increasing the risks that are inherent in the digital reality, and we may not even be aware of them.

If you do not keep close track of your digital identity, data, and assets, you may become compromised in both the digital and real worlds.

4. What are the examples of digital security risks?

Not all of your personal information is valuable to cybercriminals, but it may be of interest to some ordinary people with bad intentions. Therefore, the data you should try to secure the most are:

- Personal identification information (including names, phone numbers, addresses, emails, IP addresses, and Social Security numbers, which are often used in identity theft);
- Personal payment information (for example, credit or debit card numbers, online banking information, and PINs, which are frequent targets of phishing scams);
- Personal health information (involving medical history, prescriptions, and health insurance, which are the targets of insurance fraud and drug scams).

How Can You Be Digitally Safe?

- **Stay updated on the subject.** As this is a fast-changing field, it is critically important to remain informed and up-to-date regarding the latest trends.

  Most magazines and newspapers have a good tech section. We recommend checking wired.com, technologyreview.com, computerworld.com, technowize.com, analyticsinsight.net and sciencefocus.com/future-technology, to mention a few.

- **Consider attending online and on-site trainings.** These can help you acquire the relevant knowledge and skills needed to recognize and mitigate digital threats effectively.

  Many organizations offer paid and certified training. A free online option is the Digital Security course for journalists and human rights defenders, developed by Meta and ICFJ.

- **Be aware of your online presence.** We will delve into specific topics in the following pages, but keep in mind that you should check which apps are on your phone, which applications you use, and what information about you is available online. Awareness is a key component of your ability to evaluate the risks you might face.

- **Make sure your software is always updated.** Software updates often contain patches for known vulnerabilities.

  Cybercriminals exploit these weaknesses, so keeping your software current helps protect against potential security breaches.

Keep in mind, safeguarding your data requires constant vigilance to ensure their security.

Digital Footprints

About Digital Footprints

1. What is a digital footprint?

A digital footprint is a track record of everything we do online. It is what we leave behind whenever we use the Internet, and it is a kind of reflection of who we are, even when we are not online.

All that you do online (namely, posting, searching, or sharing) creates a data trail. People can use this trail to piece together an idea of who you are. That is why it is important to be mindful of what you are doing online and take steps to keep your information safe.

2. How do digital footprints work and why should you be mindful of their risks?

When we use the Internet, we unintentionally leave a data trail, similar to how we walk. Search engines, social media platforms, advertising, and other businesses collect and store this information. While certain information becomes available to the public, other aspects stay private.

Data from our digital footprints can be used to track our online behaviour. In some worst-case scenarios, this information can be used to create fraudulent profiles.

3. What are the benefits and disadvantages of having an online footprint?

Following are some negative aspects you should be aware of:

- Privacy concerns from information accessed and used without your consent;
- Reputational damage;
- Employment concerns from a negative footprint.

That being said, there are also positive aspects, such as:

- Increased trust from having an online presence;
- Increased professional opportunities from having a positive digital footprint.

About Digital Footprints

3. How many types of digital footprints exist?

Experts have identified six (6) types of digital footprints:

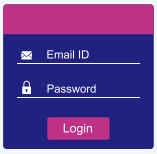
- **Personally Identifiable Footprints:** They include your name, postal address, email address, and phone number, which can be used to identify exactly who you are. As they comprise the most sensitive types of data, they should be protected at all costs.

- **Anonymous Footprints:** These include the online sites we visit and the searches we make, which cannot be used to identify anyone individually. Therefore, digital footprints of this kind are not as sensitive as the personally identifiable ones. But it is advisable, nonetheless, to protect them through the use of a reliable VPN or other cybersecurity tools such as antivirus or antimalware apps.

- **Active Digital Footprints:** These are footprints we create on purpose. They include things like the comments we leave on social media, the posts we share, and the searches we make. Keeping track of them is easy as we are usually aware of where they are.

- **Passive Digital Footprints:** Typically, created without our knowledge or consent, these footprints include the websites we visit, the videos we watch, and the ads we see while we are online. Because we are mostly unaware of such passively created digital traces, it is more difficult to maintain a positive digital footprint of this kind.

- **User Input Footprints:** These are created when we insert information such as our username, password, and credit card number into a website or application. Such footprints should always be protected because they can be used to steal our resources and identities.



- **Sensor Data Footprints:** The devices we use create such footprints, which include information involving our location, age, and gender. Sensor data footprints can be used to track our behaviour and personal preferences.

How Do You Protect or Erase Your Digital Footprint?

If you want to protect your digital footprint:

- Consider using a VPN to hide and protect your personally identifiable footprints.
- Use strong and complex passwords, as they make it harder for hackers to access your information.
- Be careful with the social media you use and with the personal information you share and save online.
- Adhere to good cybersecurity practices (e.g., using antivirus software, updating your software regularly, and being careful about the websites you visit).

If you want to erase your digital footprint:

- Deactivate and delete your social media accounts to remove from the Internet a large portion of the information associated with you.
- Unsubscribe from mailing lists to stop them from saving your information.
- Delete cookies because they track your online activities and collect information about you.
- Submit a Google Listing Removal Request if you want to remove your name and contact information from the search results.

If you want to erase your personal information, you can do so by contacting the website or organization that has your information and asking them to remove it.

Services such as Ghostery can be a good option because they scan the Internet for information about you and remove it.

Virtual Private Networks (VPNs)

About VPNs

1. What is a VPN?

A VPN, short for "virtual private network," safeguards your internet connection and online privacy. It establishes an encrypted data tunnel, shields your IP address, and ensures secure use of public Wi-Fi and open networks.

2. How many types of VPNs are there?

There are three types of virtual private networks or VPNs:

- Remote-access VPNs enable users to connect to a distant network, often through specialized software. If you ever needed to access your office network remotely, you probably used a remote access VPN. It enhances the safety and convenience of working outside the office, enabling employees to access data and resources from any location.

- Site-to-site VPNs are primarily utilized by businesses, especially large corporations, to facilitate secure network access between chosen locations. They serve as an excellent means to interconnect all company offices, enabling different branches to securely share resources and information.

- Personal VPNs operate much like remote-access VPNs, but instead of linking to a private, restricted network (like your workplace), you connect to your VPN provider's servers for Internet security and privacy.

3. Do you need a personal VPN?

You must be careful when you access, download, or upload content on the Internet. To ensure safety while browsing the web, using a personal VPN is particularly important when you:

- connect to public and open wireless networks;
- access content that is normally restricted in specific areas, no matter whether you are at home or abroad;
- want to keep your personal data private (usernames, passwords, email addresses, credit card information, etc.);
- and want to hide your IP address.

How Can You Choose the Right Personal VPN?

- **Opt for a paid VPN instead of a free VPN.** Keep in mind that all companies need to make money to cover their costs, so free VPNs tend to profit by using ads and selling their users' data. Free VPNs also tend to provide slower connection speeds and fewer features.

- **Where your VPN provider is located matters a lot.** Depending on their home country's laws, they may have to collect and share data with authorities, which can impact your privacy. On the other hand, VPNs in places with fewer data rules can be risky, too. So, knowing where your VPN comes from is important.

- **Review your VPN's privacy policy. Many VPNs say they do not log any data, but that is not always the case.** Most VPNs need to keep some logs, such as connection data, to work properly. However, certain information, such as your Internet activities, should remain private. Make sure to double-check your VPN provider's statements and carefully read their privacy policy.

- **Research the providers that are already on the market and compare the reviews published about them.** Some of the most reputable personal VPN providers are ExpressVPN, NordVPN, Surfshark, ProtonVPN, CyberGhost, TunnelBear, Norton Secure VPN, and Private Internet Access VPN.

Before acquiring and using a personal VPN, know your needs: privacy, geo-restricted content, or secure public Wi-Fi? Choose a provider based on your needs.

About Passwords

About Passwords

1. What is a password?

It is a unique set of characters used as a security measure to authenticate your user identity and protect personal data and system access from unauthorized access.

2. Why are strong passwords necessary?

A strong and complex password will be more difficult to break. For creating a secure password, the website, platform, or app will require you to use unusual words, phrases, and dates, or combinations of letters, numbers, and symbols.

For example, the worst passwords you could create would be those containing your name, the name of a common object or a place you hold dear, or your date of birth.

3. How do hackers crack passwords?

They use a variety of methods, such as:

- **Dictionary method.** Hackers use software that tests words from a dictionary as passwords, making common words risky.
- **Brute force.** Sophisticated hacking software attempts various word and character combinations, powered by machine learning and AI.
- **Rainbow table attacks and network analysis.** Cybercriminals use these methods to match passwords to decryption keys or intercept network data for information extraction.
- **Phishing and social engineering.** Phishing downloads malware via links, while social engineering tricks users into revealing login credentials.
- **Spidering.** Criminals pose as contractors or clients, engaging in conversation to glean information about company networks or vital systems.

About Passwords

4. Are there many types of passwords?

Generally speaking, there are just two types of passwords: weak and strong. However, some experts subcategorize them in the following manner:

Weak passwords

- **Simple.** It could be an ordinary word from the dictionary. It is important to understand here that adding a digit to a commonplace word would not enhance password security. Hence, “commun1cation” will be as weak as “communication”.
- **Easy to guess.** These passwords would typically include a name or term that could be linked to you with a bit of research. If your current password is, for example, your street address, the name of your child or pet, or your favourite singer, you could be hacked quite easily.
- **Dates.** Your birthday, your favourite number, or your wedding anniversary, to mention a few, are not materials for safe passwords. They could be guessed by hackers in a matter of minutes.
- **Universal passwords.** This would be a single password that you use on multiple websites. The password itself may be very strong and secure, but you cannot be sure of the security of the sites or platforms where you use it. If one site gets hacked, the attackers will have access to this universal password of yours and use it to access your other accounts.

Strong passwords

- **Alphanumeric.** A strong password would contain letters and numbers. It could also include special characters, which would only boost its effectiveness. Using random words increases password strength even further. (For example, r3M3mB3R tH!$?)

- **Random.** It might be even better to create passwords using random characters, which do not form any word, phrase, or sentence. This would make it extremely hard, if not impossible, to crack such passwords.

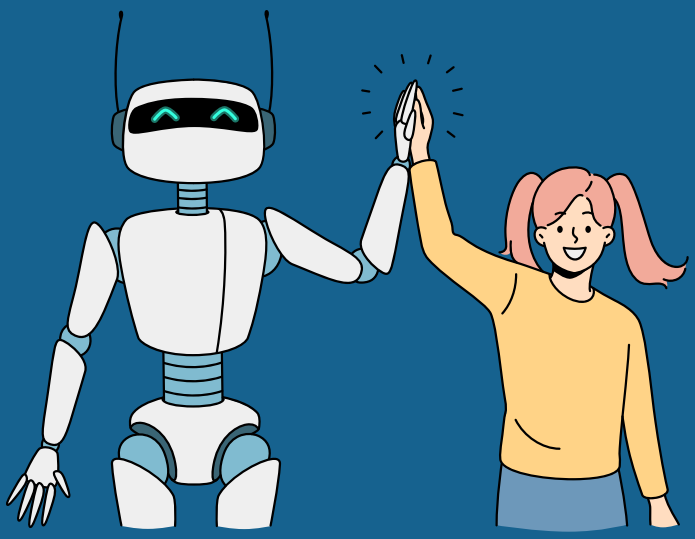
- **Pattern-Based.** You can devise a unique password by using keyboard patterns. This password type won’t require you to remember a combination of symbols. Instead, you’ll use memorable keyboard paths to create a random password that you can actually remember.

How Do You Reinforce Your Passwords?

- **Avoid common and ordinary passwords.** Using easily guessable passwords like "123456" or "password" puts your accounts at risk. Instead, create unique and complex passwords.
- **Never use the same password for multiple sites.** Reusing passwords means that if one account is compromised, all linked accounts become vulnerable.
- **Keep your passwords private and do not share them with anyone.** Sharing passwords, even with trusted individuals, can lead to security breaches. Keep your passwords confidential.
- **Consider using password generators.** They can create strong, random passwords that are difficult for hackers to guess.
- **Consider using a trustworthy password manager.** They help store and organize passwords securely. You need to remember only one master password to access all the others.
- **Get used to changing passwords.** Regularly changing passwords adds an extra layer of security. It prevents unauthorized access, even if someone has discovered an old password.
- **Consider using password managers.** Storing passwords in insecure places like sticky notes or Word documents is risky. Password managers provide a safer and more organized alternative.
- **Employ additional security methods.** Two-factor authentication (2FA), multi-factor authentication (MFA), and one-time passwords (OTP) add extra layers of protection to your accounts by requiring more than just a password for access.

Practise better password hygiene by using a unique and complex password for each account you have. A password manager can help generate and store them. Finally, enable an extra identification method whenever available.

About Generative AI



Generative artificial intelligence (AI)

1. What is generative artificial intelligence?

Generative AI refers to deep-learning models with the ability to create high-quality text, images, and diverse content using the knowledge gained from their training. Well-known examples include ChatGPT, Bard, DALL-E, Midjourney, and DeepMind.

2. In simple terms, how does generative AI work?

Generative AI, like all deep-learning models, can process raw data and extensive datasets like Wikipedia. Through such processing, it can "learn" how to produce statistically likely outputs in response to specific prompts.

These generative models essentially encode a simplified version of the data they were trained on and use them to craft new content that resembles, though isn't identical to, the original dataset.

3. Are generative AI models new?

Not at all. They have been used for years in statistics to analyze numerical data. The rise of deep learning, however, has made it possible to extend the use of such models to images, speech, and other complex data types.

4. What are the new risks that generative AI could bring to digital security?

- **Tricking victims.** Generative AI creates convincing imitations of text, videos, voice recordings, and images, enabling scams and deepfakes to spread false information and deceive victims.

- **Building better, more sophisticated malware.** AI-driven tools automate tasks, mimic human behaviour, and learn from past attacks, making malware detection and defense tougher.

- **Exploiting application vulnerabilities.** The potential backdoors of AI-generated codes are uncertain. If AI can track known exploits, it can create adaptive attacks that are difficult to contain.

- **Data security.** Most generative AI lacks data privacy guarantees, leading to criticism and regulatory scrutiny, as seen in the temporary ban of ChatGPT over privacy issues.

How Can You Strengthen Your Digital Security Amidst the Rise of Generative AI?

- **Stay informed on the developments in generative AI and its potential risks.** Understanding the technology is the first step to protecting your organization and yourself.

- **Beware of deepfakes** because generative AI can create convincing deepfake videos and audio.

- **Verify information by cross-checking information from multiple reliable sources**, especially in cases where there's a potential for AI-generated disinformation and misinformation.

- **Secure personal data** by using strong, unique passwords, enabling two-factor authentication, and monitoring your online accounts for any unusual activity.

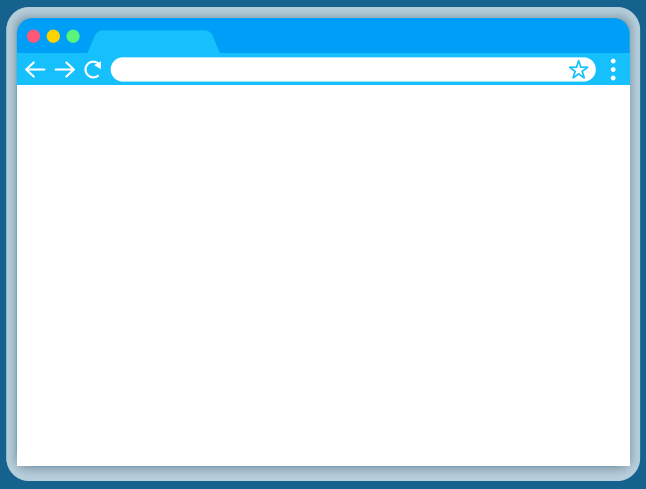
- **Use trusted social media and communication platforms** that invest in AI detection tools to combat fake content.

- **Report suspicious AI-generated content** used for harmful purposes to the relevant platforms and authorities.

- **Update your privacy settings** by regularly reviewing and adjusting the privacy settings on your online accounts to control the information you share.

By staying vigilant and adapting your digital security practices to the evolving landscape of generative AI, you can better protect yourself from potential threats.

Browsers



About Browsers

1. What are browsers?

Web browsers, or browsers, are software applications that enable users to search for and access information on the Internet. They present content from web pages on various devices like computers, tablets, or mobile devices by connecting to webpages through hyperlinks identified with uniform resource identifiers (URIs).

Most browsers exhibit text, images, and graphics from the Internet. Yet, certain browsers may necessitate additional "plug-ins," small software programmes that integrate supplementary functionalities into a standalone computer application to handle multimedia content like audio and video.

2. How safe web broswers are?

Web browsers are frequently set up for user convenience, sometimes compromising user safety. Therefore, it is crucial to utilize a secure web browser, as using an insecure one may expose users to risks such as hacking, data theft, tracking, malware, and other potential threats.

However, it is important to note that even a secure browser does not provide absolute security. Adopting good web hygiene practices is a valuable initial step, and enhancing protection through additional layers of security is advisable.

3. What are the main challenges you can face through the browser you use?

- Man-in-the-middle attacks: cybercriminals may intercept communication between the user and a website, leading to the theft of sensitive data or the injection of malicious content.

- Credential theft: malicious actors may attempt to steal login credentials through various means, such as phishing sites or keyloggers, compromising user accounts and sensitive information.

- Browser hijacking: users may unknowingly install browser hijackers that alter browser settings, redirect traffic, or inject unwanted advertisements, affecting the overall browsing experience and potentially compromising security.

- Social engineering attacks: cybercriminals may employ social engineering techniques to trick users into taking actions that compromise their digital safety, such as downloading malicious files or revealing sensitive information.

- Data tracking and profiling: some websites and third-party trackers collect user data for advertising and profiling purposes, compromising privacy.

- Drive-by downloads: visiting compromised or malicious websites may lead to unintentional downloads of malware, posing a risk to the user's device and data.

How to Secure Your Browser?

No matter which browser you choose for your devices, make sure you follow these security recommendations:

- **Keep your web browser updated.** Most well-known browsers receive updates on a regular basis to fix bugs, add new functionality, and patch security vulnerabilities.
- **Use as few extensions as possible.** The greater the number of extensions you use, the greater the likelihood of your information being compromised.
- **Install a reliable Adblocker.** They block malicious ads, various annoyances, privacy threats, trackers, and more. Some of the available options are: uBlock Origin, Adblock Plus, and AdBlock.
- **Block pop-up windows.** They are bothersome and dangerous because they often lead to malicious websites. Fortunately, most popular browsers popular can block pop-ups without a third-party extension.
- **Delete unwanted cookies.** Do this to prevent cookies from tracking you and compromising your privacy.
- **Disable the autofill feature.** It makes it simple to enter sensitive information into a form created by a cybercriminal. Furthermore, anyone with access to your computer can retrieve the saved information.
- **Use a Virtual Private Network (VPN).** As mentioned in previous chapters, a VPN allows data to be safely transported over the public Internet, preventing all third parties from seeing what you do online.

Take advantage of private browsing or the incognito mode.

The purpose is not to hide your online activity, as many people believe, but it is to delete all information about your browsing session, including your history, downloads, and cookies, when you close the private window.

About Social Media

About Social Media

1. What are social media?

Simply put, these are forms of media that allow people to communicate with other users, businesses, communities, and content. They also allow users to share information using the Internet or devices such as computers, laptops, and tablets, among others.

2. What are the most prominent examples of social media platforms?

Currently, some of the most popular platforms are Facebook, YouTube, WhatsApp, Instagram, TikTok, Snapchat, Pinterest, Reddit, LinkedIn, and Twitter (now known as X).

These platforms serve various purposes, from personal communication and content sharing to professional networking and entertainment. Each has its own unique features and user communities.

3. What are the benefits and disadvantages of having social media accounts?

Some of the benefits are:

- Getting to know about and being involved in important causes;
- Being able to promote and advertise products/contents;
- Connecting with people and forming communities;
- Staying updated through good sources of information;
- Having increased opportunities for learning and diversifying education;
- Being able to direct traffic to a website or to other platforms;
- Reaching larger and more diverse audiences;
- Being able to have direct communication with individuals and institutions;
- Finding more entertainment options.

Some of the risks are:

- Being vulnerable to cyberbullying;
- A greater risk of being hacked;
- Reduced face-to-face spaces and skills;
- Receiving and spreading misinformation and disinformation;
- The risk of addiction;
- Physical and mental harm to one's health;
- Wastage of time;
- The shortening of attention span.

How Can You Use Social Media Safely?

- **Manage your privacy settings.** They help you control who sees what you post and manage your online experience in a positive way.

- **Protect your reputation on social networks.** Whatever you post online stays online. Even if you delete a post, it can still exist in backups or be archived by others.

- **Keep in mind the context.** If you are in a risky environment, be careful not to share too much information about yourself or about the people you work with.

- **Keep personal information private.** The more information you post, the easier it may be for someone to use that information to steal your identity, access your data, or commit other crimes such as stalking.

- **Know what action to take in specific situations.** For example, if someone is harassing or threatening you, remove them from your friends list, block them, and report them to the site administrator. Also, consider involving the authorities in cases that make you feel you are at risk.

- **Be cautious on social networking sites.** Even messages or links that look like they come from friends can sometimes contain harmful software or be part of a phishing attack. If you are at all suspicious, don't click the button or link. Contact your friends and acquaintances to verify their validity.

- **Do not share sensitive information (text, video, or pictures) over messaging systems.** They are susceptible to hacking, data breaches, and interception, jeopardizing the confidentiality and privacy of your data.

Remember: what you share, no matter how innocent it seems, may be a piece of the puzzle that criminals and malicious people use for bad purposes.

Sociocultural Aspects of Digital Safety

About the Sociocultural Aspects of Digital Safety

1. Why the context matters when it comes to digital safety?

A given context can influence the perception and practice of digital security, whether at the individual, community, or organizational level. How you perceive privacy, or what you share online, may have been determined by, among other factors, the social norms of the place where you were born, your age, and your political and ideological views.

2. What are the threats you can face based on sociocultural aspects?

Although everyone is exposed to risks and threats online, some people are more vulnerable due to their race, ethnicity, gender, nationality, creed, or other identity-related factors. For example, women can be harassed online just because of their gender. And the harassments can be in the forms of defamation, impersonation, extortion, stalking, sexual surveillance and harassment, emotional harm, and even threats of rape and death.

Threats that some communities face in the real world can migrate to the digital domain, which in itself can be a spawning ground for new forms of threat.

3. Are there other risks that everyone is vulnerable to?

Well-being challenges, cancel culture, and self-censorship can collectively contribute to an online environment that is less safe and inclusive. Mental health issues resulting from negative online experiences may compromise an individual's ability to navigate the digital world confidently. Cancel culture and self-censorship can restrict the open exchange of ideas, hindering the development of a robust and diverse digital discourse.

- Well-being challenges: The digital landscape can have significant impacts on individuals' mental and emotional well-being. Social media, for example, can contribute to issues such as cyberbullying, social comparison, and the pressure to maintain a curated online persona.
- Cancel culture: This refers to the practice of withdrawing support for individuals or entities whose actions or statements are perceived as offensive or objectionable, often leading to public shaming and social exclusion. Individuals may become hesitant to express diverse opinions or engage in open dialogue for fear of public backlash, impacting free expression and the exchange of ideas.
- Self-censorship: The fear of being criticized, harassed, or "cancelled" can lead to self-censorship, stifling creativity, diverse perspectives, and constructive discourse. It may create an environment where individuals feel pressured to conform to prevailing opinions rather than expressing their authentic views.

How Can You Stay Safe Online While Keeping in Mind Your Sociocultural Environment?

The answer to this question will depend on your circumstance. Nonetheless, here are some general and useful recommendations:

Cultivate digital literacy and cultural awareness:

- Develop a strong understanding of digital literacy to navigate online spaces effectively.
- Be aware of and respect cultural differences in online behaviour and communication.
- Stay informed about sociocultural nuances to avoid unintentional misunderstandings.

Promote positive online behaviour:

- Foster a positive online environment by engaging in respectful and constructive communication.
- Encourage open dialogue and diverse perspectives in online communities.
- Avoid participating in or promoting cancel culture; instead, engage in respectful debates.

Use privacy settings effectively:

- Adjust privacy settings on social media platforms to control who can access your information.
- Regularly review and update these settings in accordance with your comfort level and cultural norms.

Be mindful of your well-being:

- Set boundaries for your online activities to avoid burnout and stress.
- Prioritize mental health and take breaks from social media if needed.
- Be aware of the potential impact of online interactions on your emotional and psychological well-being.

Use social media responsibly:

- Be mindful of the content you share on social media, considering the potential sociocultural implications.
- Think before posting to avoid inadvertently causing offence or contributing to negative online dynamics.

Encourage digital empathy:

- Foster empathy in online interactions, considering the feelings and perspectives of others.
- Report and address online harassment to create a safer and more empathetic online space.

Seek support and report incidents:

- Reach out for support if you experience online harassment or feel unsafe.
- Report incidents to the relevant platforms or authorities, emphasizing the importance of a supportive digital community.

Glossary: Key Notions

About cookies

What is a cookie?

In the digital sphere, a cookie (also known as an HTTP cookie, a browser cookie, or an internet cookie) refers to a system that tracks your website activity. The objective of the cookies is to remember information about you, including a record of your website visits and activity.

Cookies aren't always bad. And through careful management, you can make sure websites are only collecting information that is useful for your user experience. With our cookie tips, you can navigate the web confidently.

How many types of cookies are there?

There are four types:

- **Persistent cookies.** These are designed to store data for an extended period of time. Each persistent cookie comes with an expiration date, ranging from a few days to several years following your site visit.

  For example, when you log in to a site and ask it to remember you, a persistent cookie stores your username and password, making it quicker for you to log in in the future.

- **Session cookies.** These are temporary cookies and will be deleted when you close your browser.

  When you are shopping online at a specific site, a session cookie keeps the items you've selected in your shopping cart, even if you click on different pages around the site.

- **Third-party cookies or tracking cookies.** These collect data about your online behaviour, and pass them to the website that created the cookies, usually for advertising insight.

  For example, when you look at an item but don't purchase it, third-party cookies store the information about your online viewing and pass it on to advertisers. The next day, you find an ad on your social media account for the exact item you viewed online the day before.

- **Supercookies.** A type of tracking cookies, supercookies are not stored at the browser level but at the network level. They can travel across browsers and are permanent. The biggest risk involving these cookies is that they can access information such as your browsing habits, login credentials, and image caches even after you've deleted your cookies.

If you want to protect from the bad cookies, accept only the necessary cookies when you are navigating. Also, use an encrypted connection or a virtual private network (VPN).

About Software

What is a software?

A software is a set of programmes that allows users to perform a defined function or a specific task. It is responsible for directing all computer-related devices and tells them how to perform.

How many types of software are there?

Overall, there are two types of software, each subdivided into several modules:

System software

System software involves computer programmes that help the user to run computer hardware or software and manage the interaction between them.

a) Operating systems: a group of software that handles the execution of programmes and offers general services for the application that runs over the computer. Examples: Microsoft Windows, Apple's MacOS, Android, Ubuntu, Linux.

b) Device drivers: a type of software that operates or controls specific hardware devices linked to your system. Examples: Display drivers, printer drivers, etc.

c) Firmware: a type of software embedded in a hardware device, and not in a computer. Example: printer software.

d) Utility: its job is to offer support to the system infrastructure. Examples: Norton and McAfee Antivirus, WinRAR, WinZip, Windows File Explorer.

Application programmes

Also known as software applications, these are end-user computer programmes developed primarily to provide specific functionalities, such as assisting the user.

a) Word processor: these are applications used for documentation, making notes, and typing data. Examples: MS Word (Microsoft), iWork-Pages (Apple), and Google Docs.

b) Database software: it is used to create, manage, modify and organize a massive amount of data quickly retrieved. Examples: Oracle, MS Access, SQLite, FileMaker, dBase.

c) Multimedia software: this type enables the users to play, create or record images, music, and video files. Examples: Adobe Photoshop, Windows Movie Maker, iMovie, etc.

d) Web browsers: they are used to browse or navigate the Internet. Examples: Chrome, Mozilla Firefox, Opera, Microsoft Edge, Safari.

About Sofware

Are there more types of software?

Based on availability and shareability, there is a further classification of software:

a) Freeware: As the name suggests, this type of software is available free of cost for an unlimited time. Any user can easily download such software from the Internet and start using it instantly without paying any charges or fees.
Examples: Adobe Reader, Zoom, Skype, Audacity, Anydesk.

b) Shareware: This type of software is readily available on the Internet to download on a fixed trial basis. It is distributed freely with a set time limit, and at the end of the trial period, the user is asked either to pay the fee or uninstall the software.
Examples: Grammarly, Adobe Suite, WinZip.

c) Open-source: Unlike freeware, this kind of software is available online along with its source code. This means, the user can change, transform, and even add additional features to an open-source software. Based on the service, it can be either chargeable or free.
Examples: Mozilla Firefox, OpenOffice, MySQL, Thunderbird.

Why is it so important to update software?

Software updates are important for reasons such as:

- Repairing securityholes to fix computer bugs. Updates can also add new featuresto your devicesand remove the outdated ones.
- Including software patches, which cover securityholes to keep the hackers at bay.
- Protecting your information from ransomware attacks, which can target your emails, home address and even information related to your bank account.
- Protecting your devicesfrom being infected by viruses and transferring them to those of your family or colleagues.
- Improving the systems, and keeping them from crashing. Regular updates also ensure more stability, boosting programme performance and speed, among other things.

Some updates require your device to be connected to Wi-Fi or power, have sufficient storage, or be rebooted. In such cases, follow the instructions your device gives you.

About Hardware

What is a hardware

While software encompasses the intangible part of a device, hardware involves its physical components, responsible for storing and executing the instructions provided by the software.

What is the difference between internal and external hardware?

Computer hardware can be categorized in internal and external components.

Internal hardware components are those necessary for the proper functioning of the computer, while external hardware components are attached to the computer to add or enhance functionality.

a) Internal hardware

The internal components collectively process or store the instructions delivered by the programme or operating system (OS).

These include the motherboard, CPU, RAM, hard drive, and heat sink, among others.

b) External hardware

External hardware components are items that are often externally connected to the computer to control either input or output functions. These hardware devices are designed to either provide instructions to the software (input) or render results from its execution (output).

Some examples of input hardware components are the mouse, keyboard, scanner, camera, and memory card.

Monitors, printers, speakers, and headphones are the output hardware components.

Hardware and software are complementary. A device can function efficiently and produce useful output only when both hardware and software work together appropriately.

Final Recommendations and Further Resources

Final Recommendations

1 Use two-factor authentication on as many devices and accounts as you can

This security method provides extra protection during the login process. It makesit much more difficult for attackers to break into someone's devicesor online accounts.Even if a hacker gets hold of a password, it won't be sufficient to pass the security check.

2 Consider having a phone or laptop just for work

Having devices exclusively dedicated to work enhances security by reducing the risk of accidentally compromising sensitive work data on personal apps or websites. This helps protect data (especially if you manage sensitive information and face a data leak or breach), ensuring compliance with data protection and privacy laws.

3 Be mindful of country-specific regulations; context matters

It is possible that using a personal VPN is allowed in your country, but it is illegal in others. Do your research every time you travel to make sure you are following the local laws.

4 You may not be famous but still be a target

Even if you are not a celebrity, digital security matters because it safeguards your personal information, financial assets, and privacy from digital threats that can disrupt your life and lead to financial losses or identity theft.

5 Small actions can make a difference

You do not have to buy the most expensive gadgets or be skilled in every single piece of software. Just doing regular software updates on every device you use, or changing your passwords to stronger ones, can make a significant difference in your digital security.

6 There is no 100% digital safety

Given the rapidly-evolving threats, human factors, and the interconnected nature of the digital world, total digital security is impossible.

But you can still aim to be as safe as possible by adopting best practicesand staying updated on the latest trends and reports.

Further Resources

For further knowledge in **digital security**, consider the following training courses:

- Introduction to personal digitalsecurity, taughtby Codeacademy Digital security and Human Rights, offered by Amnesty International.
- Digital safety and security, taught by the ArizonaState University Watch the recording of the trainingDigital SecurityWebinars for Journalists and Human Rights Advocates, offered by The International Center for Journalists (ICFJ), in partnership with the Border Center for Journalists and Bloggers (BCJB), and Meta

For further knowledge and training in **cyber security**:

- Introduction to cyber security, taught by The Open University Cybersecurity essentials, offeredby The Linux Foundation

For additional knowledge and training in **digital well-being**:

- Intro to **digital well-being**, offeredby Google
- Digital tools and well-being, taught by the ArizonaState University
- Digital well-being taught by the University of York

For additional knowledge and training in **various digital and tech topics**:

- Watch the educational videos and materials posted by IBMon their YouTubechannel
- Listen to the GoogleTalks posted on their YouTube channel
- Learn a new digital needed skill with Google Garage

References

These sources were helpful and valuable in the development of this guideline. We recommend reviewing them if you want more information about the mentioned subjects:

Britannica: *www.britannica.com/technology/browser*

Capterra: *www.capterra.com/glossary/browser/*

Data Prot: *www.dataprot.net/articles*

Digital Scholar: *www.digitalscholar.in/pros-and-cons-of-social-media/*

Free Code Camp: *www.freecodecamp.org*

F-Secure: *www.f-secure.com/en*

Java Point: *www.javatpoint.com*

National Cyber Security Centre - UK: *www.ncsc.gov.uk*

NordVPN: *www.nordvpn.com*

Norton Blog: *www.us.norton.com/blog*

OECD Digital: *www.oecd.org/digital/digital-security*

OSIbeyond: *www.osibeyond.com/blog/tips-for-making-web-browsing-more-secure*

Security Boulevard: *www.securityboulevard.com*

Simplilearn: *www.simplilearn.com*

Software Lab: *www.softwarelab.org*

Standford: *https://share.stanford.edu/education-and-outreach/learn-topics/digital-safety*

Tech Target: *www.techtarget.com*

University of Pittsburgh - Information Technology: *www.technology.pitt.edu/security*

From Theory to Practice

This guide contains concepts and notions, but also recommendations to help you understand and improve your digital hygiene. After reading it, we suggest using the complementary checklist as often as possible (meaning, each month, trimester, semester, or year).

Bear in mind that you need to personally assess the recommendations to ensure their relevance to your specific context and need.

Contact

Cameco is open to peer learning and exchange. If you have comments, questions, and suggestions, contact Emy Osorio Matorel, Advisor on Digital Analysis and Strategy, at emy.osorio@cameco.org

A Digital Security Guide for Everyone

Published by
CAMECO
2024

Postbox 10 21 04
52021 Aachen
Germany

For inquiries, please contact

Emy Osorio Matorel (emy.osorio@cameco.org)
Cameco General Office (cameco@cameco.org)

cameco+