DIGITAL SECURITY CHECKLIST

This checklist should be filled out only after reading the Digital Security 101 guide.

Digital Security

○ I can understand the distinction between digital security and cybersecurity, and recognize the significance of both for my overall online protection.

○ I acknowledge the increasing digitalization of our lives and the associated risks.

○ I ensure my software is regularly updated to patch known vulnerabilities, reducing the risk of exploitation by cybercriminals.

○ I stay informed and updated on digital security trends through reputable sources.

○ I pay attention to my online presence by regularly checking the apps, programs, and personal information I have online.

Software

○ I recognize that a digital footprint is a record of my online activities, shaping my online identity even when not actively using the internet.

○ I understand that actions like posting, searching, or sharing online contribute to a data trail that can reveal aspects of who I am.

○ I am aware that using the internet leaves a data trail collected by search engines, social media, and businesses, posing risks such as potential fraud and privacy invasion.

○ I adhere to good cybersecurity practices, including using antivirus software and updating software regularly.

○ If needed, I know steps to erase my digital footprint, including deactivating social media accounts and submitting removal requests for personal information.

Passwords

○ I understand the criteria for creating a secure password, including the use of unusual words, phrases, and combinations of letters, numbers, and symbols.

○ I am aware of the existence of various methods used by hackers to crack passwords.

○ I never use the same password for multiple sites to prevent vulnerability across linked accounts.

○ I make it a habit to change passwords regularly to add an extra layer of security.

○ I use additional security methods such as two-factor authentication (2FA), multi-factor authentication (MFA), and one-time passwords (OTP) to enhance account protection.

DOCUMENT DEVELOPED BY
cameco+
Communication Consultancy for the Common Good

DIGITAL SECURITY CHECKLIST

This checklist should be filled out only after reading the Digital Security 101 guide.

Generative AI

○ I understand that generative AI creates text, images, and diverse content using knowledge gained from training.

○ I stay informed about generative AI developments and potential risks.

○ I am aware of risks in terms of digital security, such as convincing imitations for scams, sophisticated malware, and data security concerns.

○ I verify information from multiple reliable sources to counter AI-generated disinformation.

○ I report suspicious AI-generated content to relevant platforms and authorities.

○ I regularly update privacy settings on my online accounts.

Sociocultural Aspects of Digital Safety

○ I understand that the context, whether individual, community, or organizational, can shape perceptions and practices of digital security.

○ I am aware that certain individuals, based on race, ethnicity, gender, nationality, or creed, may face heightened online vulnerabilities.

○ I understand the diverse forms of online harassment, including defamation, impersonation, extortion, stalking, sexual surveillance, harassment, emotional harm, and threats of violence.

○ I acknowledge well-being challenges, cancel culture, and self-censorship as threats affecting everyone's online safety.

○ I encourage digital empathy, fostering understanding and reporting online harassment to create a safer online space.

Other aspects

○ I ensure a separate phone or laptop exclusively for work to enhance security.

I am mindful of country-specific regulations for digital practices, such as the forbidden use of personal VPNs in some places.

○

I recognize that, despite not being famous, I can still be a target for digital threats.

○ I understand that simple actions, like regular software updates and stronger passwords, can significantly improve digital security.

○ I acknowledge that achieving 100% digital safety is impossible due to evolving threats and human factors.

DOCUMENT DEVELOPED BY
cameco+
Communication Consultancy for the Common Good

DIGITAL SECURITY CHECKLIST

This checklist should be filled out only after reading the Digital Security 101 guide.

Browsers

○ I understand that using an insecure web browser may expose me to risks such as hacking, data theft, tracking, malware, and other threats.

○ I acknowledge that even secure browsers do not provide absolute security, and adopting good web hygiene practices is essential.

○ I keep my web browser regularly updated and use a minimal number of extensions to reduce the risk of compromising information.

○ I install a reliable adblocker to block malicious ads, annoyances, privacy threats, and trackers.

○ I block pop-up windows to prevent exposure to bothersome and dangerous content on malicious websites.

○ I regularly delete unwanted cookies to prevent tracking and protect privacy.

○ I disable the autofill feature to prevent entering sensitive information into potentially malicious forms.

Social Media

○ I recognize the dual nature of social media, embracing its benefits in learning and communication, while also acknowledging potential risks like cyberbullying and addiction.

○ I actively regulate my privacy settings to control the audience for my posts on social media.

○ I am mindful of the permanence of online posts, safeguarding my reputation by thoughtfully curating shared content.

○ I tailor my online presence, refraining from oversharing in environments that may pose risks.

○ I prioritize keeping personal information private to prevent identity theft.

○ I am aware of appropriate actions in specific situations, including removing and blocking harassers, reporting to site administrators, and involving authorities when necessary.

○ I exercise caution on social networking sites, steering clear of suspicious messages, links, or phishing attempts.

○ I avoid sharing sensitive information over messaging systems to mitigate risks of hacking, data breaches, and interception.

Virtual Private Networks (VPNs)

○ I recognize that a VPN, or "virtual private network," safeguards my internet connection, ensuring online privacy through an encrypted data tunnel.

○ I recognize the importance of using a personal VPN, especially when connecting to public Wi-Fi, accessing restricted content, protecting my personal data, and hiding my IP address.

○ I regularly evaluate my online activities to determine if a VPN is necessary for enhanced safety and privacy.

DOCUMENT DEVELOPED BY

cameco+

Communication Consultancy for the Common Good