Cyber Security Hygiene Best Practices for Your Organization

CANADIAN CENTRE FOR CYBER SECURITY
AUGUST 2022 | ITSAP.10.102

Your cyber hygiene is paramount in your ability to defend your networks, system, and data from threat actors. Laying a solid foundation of cyber security measures will better enable your organization to protect, defend, and recover from cyber incidents.

Cyber Hygiene Check List

Ensuring your organization is implementing, promoting, and monitoring good cyber hygiene practices is a critical component of your cyber security posture. The following table provides a list of actions your organization can take to strengthen your cyber security foundation with enhanced protective measures for your networks, systems, and data. Although your organization may not be able to implement all the actions provided below, you should implement the actions that are obtainable and sustainable to better enhance you cyber security posture.

Network and Endpoint Protection

- ☐ Protect your perimeter with anti-virus and anti-malware software, mobile threat management software, firewalls, and intrusion detection and prevention systems.
- ☐ Segment your networks to stop traffic from flowing to sensitive or restricted zones .
- ☐ Continuously monitor your Internet and mobile device gateways, network traffic, wireless access points, and audit logs to identify anomalies.
- ☐ Rotate cryptographic keys used to protect your systems, authenticate remote users and your websites.
- ☐ Monitor your Domain Name System (DNS) server to ensure your site remains reliable and trusted by users.
- ☐ Implement protective DNS to protect users from inadvertently visiting potentially malicious domains on the internet.
- ☐ Implement a security information management and security event management (SIEM) system to enable real-time continuous monitoring if resources are available.

System Protection

- ☐ Implement automatic updates and patches, especially for internet-exposed services and systems, to your firmware, hardware, software , and operating systems (OS).
- ☐ Use passphrases or strong passwords and keep them secure and confidential.
- ☐ Enforce multi-factor authentication (MFA) for accounts and systems—especially those with administrative privileges.
- ☐ Use dedicated workstations for administrator accounts that do not have web browsing or email enabled.
- ☐ Apply the principle of least privilege which ensures users are granted only the set of privileges that are essential to performing authorized tasks.
- ☐ Review user privileges within systems and their access rights to data—especially for users with administrative privileges—and remove or edit those that are unnecessary.
- ☐ Manage mobile devices with Mobile Device Management (MDM) or Unified Endpoint Management (UEM) solutions.
- ☐ Implement application allow listing to control who or what is able to access your networks and systems.
- ☐ Implement an incident response plan, and test it with table top exercises, to ensure you can restore critical functions and recover in a timely manner.
- ☐ Backup critical data and systems offline on a regular basis and ensure backups are isolated from network connections.
- ☐ Test your backups periodically to ensure data and systems can be recovered quickly and successfully.
- ☐ Assess third party applications for components or functions that are not needed and disable them or require human intervention before they are enabled (i.e. macros).
- ☐ Conduct and maintain an inventory of your organization's hardware and software assets.
- ☐ Categorize your assets to identify those that are most critical to the operational functions of your organization.

User Education and Additional Protective Measures

- ☐ Provide tailored cyber security training to your employees to ensure they know how to respond to suspicious links or emails.
- ☐ Provide privacy awareness training to your employees to reduce the risk of privacy breaches.
- ☐ Locate sources of information pertinent to your organization or subscribe to an alert service to ensure you are knowledgeable and up-to-date on the threats that could impact your organization.
- ☐ Develop an internal and external contact list of key stakeholders to alert during surge events.

Communications Security Establishment | Centre de la sécurité des télécommunications

Canada