Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

PREVENTATIVE SECURITY TOOLS

NOVEMBER 2020 **ITSAP.00.058**

Preventative security tools supply important layers of protection for your networks and devices. Security tools can help your organization reduce the risks associated with malicious intrusions (e.g. malware, spyware, and unauthorized users). Each of these security tools target specific areas to help prevent security breaches from happening to your organization's network and devices.

EXAMPLES OF PREVENTATIVE SECURITY TOOLS

Firewalls

A firewall is a security barrier placed between two networks that controls the amount and the kinds of traffic that may pass between the two. Firewalls prevent the unauthorized flow of data from one area of a network to another through the following actions:

- Monitors incoming and outgoing traffic, then filters out the known bad sources.
- Ensures downloaded data is part of a legitimate connection.
- Decrypts and analyzes downloaded data to ensure there is no trace of malicious content before forwarding the data on to your network.

Anti-Virus Software

Anti-virus software defends devices against malware through the following actions:

- Scans files for viruses before they are downloaded to your device.
- Blocks known malicious software from downloading.
- Scans your system's files against a list of known viruses to remove if detected.

Virtual Private Networks (VPNs)

A VPN is a private communications network (referred to as a tunnel) through an untrusted network. A VPN is used to establish a secure connection with authentication and protected data traffic.

It sends and receives data through an encrypted tunnel to prevent observations by threat actors. You can use it within your organization or between several different organizations to communicate over a wider network.

For more details on VPN, refer to *ITSAP.80.101 Virtual Private Networks*.

Application Allow List

Application allow list is a technique used to control which applications can run on a device.

- Approves specific applications and application components to run on organizational systems.
- Prevents users from installing unauthorized software.

Virtualization

Virtualization is a technique that creates an isolated environment for specific applications to run on your device. Virtualization can be used for the following purposes to improve security:

- Separate business and personal applications.
- Isolate different applications and processes for specific groups and business lines.
- Download malicious content for testing, using an isolated environment to prevent access to other applications.

AWARENESS SERIES

Ad Blockers

An ad blocker is a browser extension software that blocks advertisements (e.g. webpage displays and pop-ups) from your system while you browse the web.

Anti-Phishing Software

Anti-phishing software reports and blocks phishing emails to prevent attacks from occurring or spreading further (e.g. through other recipients). You can use this software to prevent identity theft, credit card fraud, and financial loss.

You should also follow Domain-based Message Authentication, Reporting, and Conformance (DMARC) policies to prevent phishers from using your organization's domain to send spoof emails. These policies also authenticate domains to filter legitimate email domains from hidden phishing domains.

For more information on phishing prevention, refer to *ITSAP.00.100 Spotting Malicious Email Messages* and *ITSAP.00.101 Don't Take the Bait: Recognize and Avoid Phishing Attacks*.

Cloud Security Subscriptions

Cloud security subscriptions can provide protection services over your cloud network, data, and accounts. These services may include the following examples of security features:

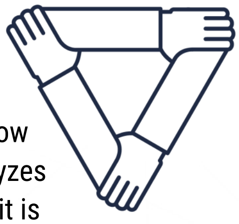
- Encryption and key management to protect your data.
- Traffic filtering based on rules you create (e.g. blocking HTTP addresses and common attack patterns).
- Detection of threatening network activity and account behaviour (e.g. unauthorized access) within your cloud environment.
- Anti-ransomware and anti-malware protection to prevent threat actors from stealing or damaging data.

Cloud Access Security Broker (CASB)

CASB software helps monitor your cloud service usage by offering the following security features:

- Validation that the network traffic between your organization's devices and the cloud provider complies with your organization's security policies.
- Detection of threats and monitoring of sensitive data in transit.

UNIFIED THREAT MANAGEMENT (UTM)



UTM is a solution (e.g. hardware appliance, software, or cloud service) with multiple functions to address different types of threats. UTM often includes preventative security tools such as firewalls, VPNs, anti-phishing, allow lists, and web content filtering. UTM analyzes content that enters the system to ensure it is clean before sending it to the user. UTM removes detected malicious content before the device accesses it and then sends a report to notify the user of the removal.

WHAT TO REMEMBER

Corporate security policies can help determine which of the preventative security tools described in this document are right for your organization. Although these security tools help reduce cyber security risks, there are still other ways for threat actors to gain access to your system. You should also implement the following security practices:

- Patch and update your security software frequently.
  - Out-of-date software can raise the risks of your devices being infected by malicious content.
  - Refer to *ITSAP.10.096 How Updates Secure your Device* for more information.
- Apply the principle of least privilege.
  - Grant individuals only the privileges necessary to complete their jobs, limiting potential damage caused by accidental, incorrect, or unauthorized use of data and systems.
- Offer tailored training to employees.
  - Promote awareness on current cyber security threats.
  - Ensure employees know their responsibilities in using preventative security tools.
  - Refer to *ITSAP.10.093 Offer Tailored Cyber Security Training to Your Employees* for more information.

Need help or have questions? Want to stay up to date and find out more on all things cyber security?
Come visit us at Canadian Centre for Cyber Security (Cyber Centre) at **cyber.gc.ca**