SECURITY AWARENESS EDUCATION

Security awareness education is the most effective control against cyber threats. It provides employees with the knowledge and skills they need to stay safe online and can help reduce the risk of data breaches, malware infections, phishing, and other malicious activities.

PC1

REGULAR PATCHING AND UPDATES

Systems and applications are often vulnerable over time. Software providers regularly offer updates to protect against these flaws, so installing all vendor-recommended updates is a good idea.

PC2

USE SECURE AUTHENTICATION METHODS.

Use strong passwords with at least eight characters, including an uppercase letter, a lowercase letter, a number and a symbol in each password. Also, enable multifactor authentication, such as PIN or Security Question, in addition to a password.

PC3

ZERO TRUST SECURITY POLICY

Zero trust security is where businesses treat anyone accessing their systems, irrespective of their role, as a potential threat until they prove otherwise.

PC4

USE ANTIVIRUS PROGRAMS.

An antivirus such as Microsoft Defender can detect and block many malware attacks. They are designed to scan files, remove malware, block unsecure links, and ensure end-users are safe online.

PC5

TAKE REGULAR BACKUPS

Regularly backing up essential data for safer keeping is very important. Backups can be used for immediate and comprehensive service recovery if compromised by malware such as ransomware or other threats.

PC6

USE OFFICIAL SOFTWARE.

Pirated software from untrusted vendors may have malicious code that, once run, can change device settings so threat actors can exploit it. They also do not offer regular updates, which leaves users vulnerable.

PC7

HAVE A RESPONSE PLANS .

An incident response plan detailing what to do during a cyber-attack, with actionable steps for different attack scenarios, can get you back to running normally and safely in no time.

PC8

USE A SIEM TOOL.

Security information and event management tools monitor security incidents across all connected users and devices, including automated monitoring and malware mitigation.

PC9

POLICIES AND PROCEDURES.

Policies like those barring unauthorised software, those against malicious websites and unencrypted removable media are critical controls against malware distribution.

PC10

CHANGE REVIEWS AND APPROVALS.

Changes are essential in systems life-cycle management, as updating servers, systems, and software is often necessary. If done uncontrolled, they can introduce risks such as malware.

PC11

LOG ANALYTICS AND AUDITING.

Security logging and monitoring systems for known and expected threats and anomalies are essential for detecting, investigating, and remediating malware-related threats.

PC12

USE A MALWARE PROTECTION SERVICE

Malware protection services often provide customer support to help users with any issues they encounter while using the software. This may include assistance with installation, configuration, and troubleshooting.

PC13

IMPLEMENT SCHEDULED SCANNING

Most antivirus programs include the option to run full system scans at scheduled intervals. This helps ensure that any malware that may have slipped past the real-time scanner is detected and removed.

PC14

SETUP NETWORK FIREWALLS

A firewall forms a barrier between the internal network and the internet, controlling incoming and outgoing traffic based on predefined rules. This helps prevent unauthorized access to the system and stops malware from spreading.

PC15

SETUP BROWSER AND WEB PROTECTION

Most antivirus protection services also provide browser extensions or plugins that block access to known malicious websites, helping the user avoid accessing and accidentally downloading and installing malware.

PC16

BONUS POINT CARD

BONUS POINT CARD

BONUS POINT CARD

BONUS POINT CARD