Cybox | Take Away Information

Congratulations for finishing the cybersecurity escape room Cybox. Please see the information below regarding best practises in cybersecurity for phishing emails, public wifi, removable devices, and unknown software. If you need to replay the game, please click here.

Phishing Emails

Phishing is the technique of delivering fake messages that appear to come from a trusted source. It is typically done by email. The purpose is to steal sensitive information such as credit card and login information, or to install malware on the victim's computer system. Here is some importants tips to identify and prevent phishing email attacks.

1. Asking for personal details through email.
2. The email is poorly written.
3. Suspicious attachments.
4. The email is sent from a public email address.
5. Misspelt domain name.
6. Suspicious links.

Public WiFi

The number of free public WiFi networks is constantly increasing, but keep in mind that not every hot spot you access is safe and secure; your device's security firewall may not be strong enough to defeat any incoming cyber attacks; use these tips to prevent anything malicious from accessing your data.

1. Enable two-factor authentication on all accounts.
2. Use a VPN (virtual private network) when you use public WiFi.
3. Access only https websites.
4. Always keep up to date on security updates.
5. Signing into accounts that hold personal information, such as social networking and online banking, should be avoided.
6. Close shared files and turn off file sharing on your computer.

Removable Devices

The best protection against this type of assault is to only use trusted removable media or devices in your computer. Other preventive and diagnostic measures would be:

1. Install, run, and keep anti-malware/anti-virus software up to date on your computer.
2. Disable any auto-run features. These functions run any programmes that are installed on the media or device.
3. Use data blocker.

Untrusted Softwares

They can hide computer viruses and spyware or open a back door that allows others to access your computer without your knowledge. Some tips to help protect your computer and data.

1. Download files, programmes, and plugins only from credible sources.
2. Downloading plugins to view pictures, videos, music, and other internet content without first confirming their authenticity is not recommended. These are often infected with malware.
3. Downloading unfamiliar applications or files is not recommended. Free software given online or by email should be avoided at all costs.
4. Never disable your computer's antivirus or other security software. Set them to update on a regular and automatic basis.