Cyber Security 101

Hackers are creative, cunning and always looking for new ways to access your information. It's hard enough to keep your information safe — let alone keep up with all the jargon. That's why we've created this handy cheasheet breaking down some of most common types of attacks you need to be aware of.

WI-FI EAVESDROPPING

A cyber criminal installs a seemingly legitimate Wi-Fi network in a public location. Once users connect to this 'malicious hotspot' or 'rogue access point' they become vulnerable to a MAN IN THE MIDDLE attack.

MAN IN THE MIDDLE (MITM)

A cyber criminal inserts themselfes between the victim and a legitimate network server (e.g. website) in order to spy on activity and access private or sensitive information.

PHISHING

A cyber criminal attempts to pass off a malicious email as legitimate in order to influence a desired action from a (e.g. click a link, open an attachment, etc.)

Common schemes include downloading MALWARE via links or attachments and using phoney forms or login screens to access passwords or personal information.

PHARMING

A cyber criminal redirects the victim's web browser to a malicious website by exploiting vulnerabilities in their domain name system (DNS) software.

This false website will often be a passable facsimile of the intended destination and be used to harvest personal or sensitive information.

TYPO SQUATTING

A cyber criminal uses common spelling errors in web addresses to re-direct unsuspecting victims to malicious websites which are often a passable facsimile of the intended destination. They will use this fake website to harvest the victim's personal or sensitive information.

DENIAL OF SERVICE (DoS)

A cyber criminal overwhelms a server or device with traffic to disrupt its normal functioning. The mass influx of requests makes it impossible for legitimate users to access the website, network or internet connected device.

Top Three Tips to Avoid Becoming a Victim:

1. **Update your software frequently** — New versions will include security patches to protect you from contemporary vulnerabilities.
2. **Ensure you're visiting a secure web site** — Never provide sensitive information on a site that does not include HTTPS:// or a lock icon in the URL bar.
3. **Be hyper-vigilant about suspicious communications** — Read subject lines and web addresses carefully and be cautious of any links, offers or demands requiring you to input passwords, fill out forms or disclose sensitive information.

MALWARE

Any malicious software installed on a network or device without the victim's consent — e.g. viruses, trojans, adware, spyware, ransomware, etc. Functions can include crashing a computer, harvesting information, disruptive advertising, spreading malware to other devices, etc.

SPYWARE

Malware that enables cyber criminals to track user activity without their knowledge.

Common capabilities include keystroke logging, unauthorized webcam / microphone use, screen recording, data harvesting, etc.

RANSOMWARE

Malware that enables cyber criminals to access private or sensitive information and subsequently restrict the authorized user's (i.e. victim's) ability to use the infected computer / network.

Criminals will typically request payment (often in cryptocurrency) to either restore the user's access or refrain from publicly publishing the sensitive information.

DRIVE BY ATTACK

Cyber criminals embed malicious code onto an insecure website or server, which can trigger malware to automatically download when the victim visits the compromised destination.

This type of attack requires no action (e.g. link click) on the part of the victim to occur.

WIPER

Malware that completely erases the hard drive and any storage media connected to that computer or network.

Are you prepared for a cyber attack? Contact MNP todayto learn how you can prevent an attack and protect your most important information assets.

Danny Timmins, CISSP
National Leader, Cyber Security
T: 905.607.9777
E: danny.timmins@mnp.ca