Cybersecurity Terms & Metaphors

AVAST CYBERHOOD WATCH **TOOLKIT**

What is a VPN?

Imagine your computer or mobile device as a car, and the internet as a road. Along this road are petrol stations, coffee shops and high street retailers. These are the equivalent of websites. Unbeknown to you, every time you step into your car to visit one of these “websites”, a helicopter with advertisers and government officials on board is deployed to track you. Now they know where you go, what you like and what you buy.

Luckily, virtual private networks (VPNs) act as tunnels connecting two locations. With a VPN switched on, every time you set foot in your car to visit your favourite retailer, you immediately enter this tunnel. You become invisible to the helicopter and its occupants.

The purpose of a VPN is to cloak you in anonymity by encrypting your internet connection between two networks. It allows you to surf the web in privacy, offering sufficient and essential protection from hackers and prying eyes as you cruise through today’s deregulated and dangerous cyber highways.

VPN TOP TIP

Use a VPN on open Wi-Fi networks to avoid online tracking and data collection by third parties, and to keep your banking details safe from cybercriminals.

What is Phishing?

Phishing is one of the internet's oldest and most well-known scams. We can define phishing as a cybercrime technique that uses fraud, trickery or deception to manipulate you into disclosing sensitive personal information, such as your bank details.

Phishing usually starts with an email or phone call from an attacker pretending to be an individual or organisation you trust. The attacker sends a targeted pitch aimed at persuading you to click a link, download an attachment, send requested information, or even complete an actual payment. Usually, a link or attachment in an email or text will contain malware, or the link will direct you to a malicious, fake version of a legitimate website, such as your bank's.

If you enter your username and password, it can be stolen by the owner of the fraudulent web page and used to access other accounts or steal money.

PHISHING TOP TIP

Always hover over the link in any suspicious email or text message before you click it. Look for obvious contextual errors, spelling mistakes and an unusual sense of urgency in the message. Question anything that seems too good to be true. If in doubt, copy the link into the search bar of your browser.

What is Ransomware?

Ransomware on a device such as your computer or smart TV is the digital equivalent of an individual accessing your home and locking all your personal belongings in a safe with a highly-complex password combination. The individual tells you that the only way he'll give up the password to the safe is if you pay him a certain amount of money before a certain deadline. If you refuse to pay, the safe and its contents will be destroyed. If you decide to pay, there's still no guarantee that the individual will comply by providing the code.

A typical ransomware attack process operates in a similar way. In many cases, an attacker will infect a device through malicious links or attachments in seemingly legitimate emails, or from fake online adverts placed on websites.

Once a device is infected, the malware will lock files such as work documents, photos or videos - or sometimes the entire device itself - with a request for payment in exchange for returning access.

RANSOMWARE TOP TIP

Make sure your device and your applications are always up-to-date. Install a strong antivirus with an anti-ransomware feature. Back up your most important files to an external device such as a hard drive, and never click a link in an email or text that looks suspicious. Finally, never pay the ransom if you fall victim of ransomware.

What is a Smart Home Hack?

Let's start by explaining what a smart home is. A smart home is a home that's been equipped with lighting, heating and electronic devices that can be controlled remotely by a phone or computer. So what's a smart home hack?

Consider an airborne disease like the flu. Flu is still one of the most dangerous threats to global health because it's transmitted through the air at high speeds and does not require contact to infect another person.

Smart home hacks are similar. Once a virus has infected a connected device, such as a smart thermostat, it can spread to other connected devices in the home, such as your smart TV, your smart speaker and webcam, until all of your smart devices are infected.

This 'army' of zombie devices (as they're known) are now under the control of a cybercriminal who can use their collective power to take down websites, attack critical infrastructure and steal money. Like the flu, attacks on smart homes will be one of the most dangerous cyberthreats over the next decade because of the rapid rise of internet-connected gadgets entering households around the world.

SMART HOME HACK TOP TIP

Always change the default password that's shipped with a smart device or router, and make sure its software is always up to date. Always check the credibility of the manufacturer by looking at independent reviews before you make a purchase. And always think twice; you are bringing a smart device into your own home, and it could be the weakest link.