interfuture

BUSINESS **IT** SECURITY

Interfuture Security News

Usually in the summer months, with many away on summer holidays, businesses tend to slow down: in cyber security though the fun never stops: find out more about in the latest edition of the **Interfuture Security Newsletter!**

We have a couple of Top 5 lists for you to take a look at this week: one warns of who might be most at risk from cyber crime and the other explains some of the methods (and protective measures you can take).

As always, any feedback or queries please contact us via our social media channels or through our website.

Key Point

Even if you are not in one of these industries that is frequently targeted, you may still be at risk - bad actors will take any opportunity to exploit you.

Cyber attacks can happen to anyone, from high-level CEOs in big companies, to your grandma clicking on the wrong thing online.

Remember to always be vigilant and help those who are less cyber-aware when you can!

Top Types of Targets

Here are the industries that cyber criminals target most:

5. Government & Public Sector: Government organisations hold a lot of important data, making them enticing targets for bad actors. Attacks are frequently enacted by a foreign government or a cyber threat group with a political agenda.

4. Healthcare: Healthcare organisations hold a lot of personal data that they need to keep private – if released, it could lead to significant patient safety risks: it isn't just biological viruses, but digital ones that you need to be aware of!

3. Professional, business & consumer services: When one party interacts with another, it creates a chain that can lead to weaknesses in security. Even if your security is robust, if the business you are dealing with is compromised, you could be too.

2. Finance & insurance: Money: that is the biggest motivator behind cyber-attacks. Ransomware is designed to extort companies out of payment, and these companies have the funds to pay it (and they want to protect their reputations).

1. Manufacturing: Often manufacturing companies rely on outdated or poorly secured systems, making them easy prey. Attacks can lead to production downtime, which results in a loss of income, as well as client and investor trust.

Social Engineering Methods

5. Quid Pro Quo

In this type of social engineering, the attack offers something to the victim in exchange for valuable data or access. Verify the identities of anyone requesting access: for example, if they are claiming to be IT support for your company, find out if they exist and if they're credentials are as they should be, and limit how much information you give out to unknown individuals.

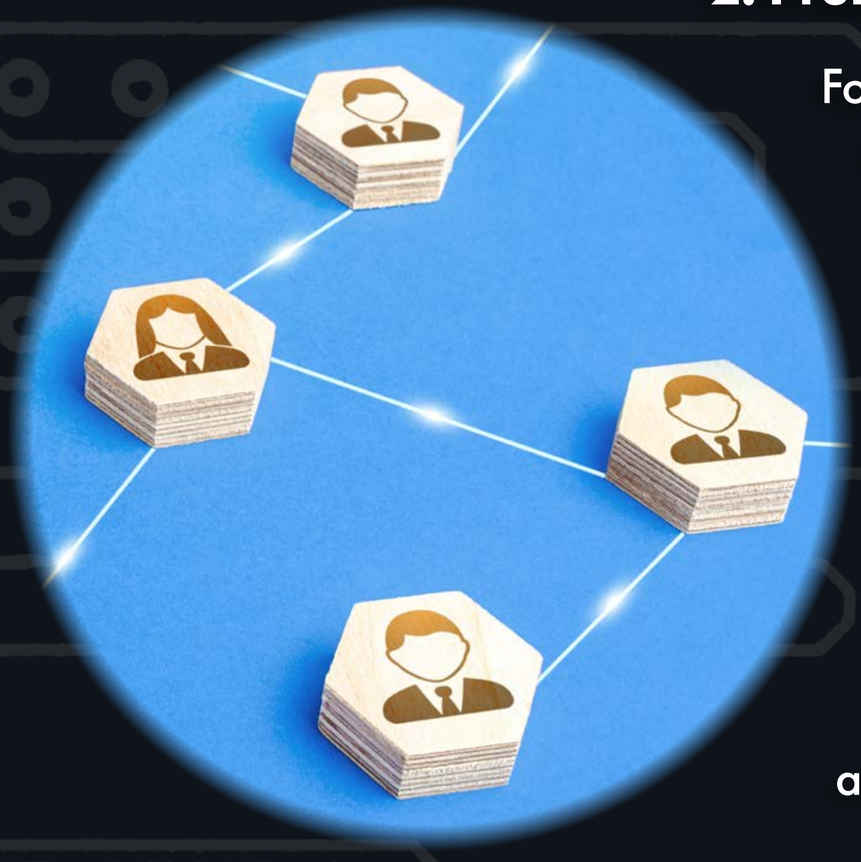
4. Tailgating (or Piggybacking)

This is a physical method of attack, so more relevant if you work in an office. Bad actors can gain access to restricted places by pretending to be someone who belongs, like a delivery driver. Once there, they can get into important systems. Ensure your critical systems have strong access controls, with badges and biometrics. Additionally, provide staff with security training and keep your computer locked when you step away from your desk.

3. Baiting

Users are enticed with the offer of free software, or free USB drives, which when installed are found to be malicious, infecting your systems with malware. Preventing this is simple: if it seems too good to be true, it probably is. Don't accept freebies, only download from trusted sources and block unauthorised USBs.

2. Pretexting



For this method, the attacker creates a scenario to manipulate you into revealing information or performing actions. This may be pretending to work for a bank and asking for financial details. Use zero-trust as a starting point: if you never assume an access request is legitimate, then bad actors can never get through.

1. Phishing

Phishing emails and texts appear to be from trusted sources, but are designed to trick victims in to clicking on corrupted links or divulging private information. While training and awareness are the best protective methods, using email filtering and anti-phishing tools can also be good deterrents.

Help Us Help You

With your feedback, we can take steps to improve our service, making it better for you. Additionally, it encourages new clients, which helps us expand, allowing us to increase in scope to offer you greater protection: talk about a win-win!

If you could leave a review via the link below, it would be greatly appreciated.

Review Interfuture Security via the link in the footer of this email

★★★★★