NEWSLETTER

OCTOBER 2021

Less than a week into October - Cyber Security month - we had already seen Facebook whistleblower Frances Haughen revealing her belief that Facebook is a national security risk; Face-book, Instagram and WhatsApp had a prolonged nap on Monday essentially forcing social media addicts to turn to less secure platforms; and IT World Canada announced that there's a new text messaging cam going round which tricks people into installing malware on their phones. Of course, it's only natural that, as new technologies develop, so too do new threats.

The more you know, the better equipped you will be to defend your company's cyber battlements. So, we decided to dedicate this month's newsletter to that all-important aspect of any organisation – cyber-security.

Cyber Security Need-to-Know according to Forbes:

Ransomware attacks increased by **62% in 2020**

Ransomware attacks currently every **11 seconds**

Employees have a lack of confidence in their company's cyber policy.

Very concerning malware variants which saw a **74% increase**

KNOWLEDGE IS POWER

PHISHING

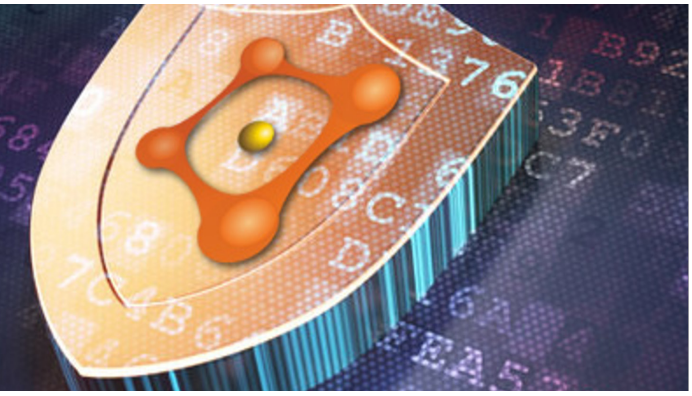
Phishing is the fishing of the cyber world. It's a strategy that lures the unsuspecting victim in and then ambushes them. The attacker (fisherman) dangles an attractive fake message (the fly/bait) in front of their victim (the innocent fish) causing the victim to open up and share information or allowing the attacker to send out malicious software (the hook). When the victim bites, it's game over!

Having made this last point, I must highlight that there is a more targeted approach called 'spear phishing' which, like its real-life counterpart, hones in more specifically on its target. Spear phishers will use personalised greetings and even private information to hoodwink their victims. And these aren't the only forms of phishing. There's also clone phishing, whaling and pop-up phishing!

HOW TO SPOT IT?

It's probably a phishing mail/message if it:

- Seems too good to be true
- Asks for personal information e.g. PINs
- Has spelling or grammatical mistakes
- Calls for urgent action
- Asks you to click on hyperlinks
- Asks you to open an attachment
- Comes from a source you don't recognise
- Uses a generic greeting



CLICKJACKING

Clickjacking tricks the user into doing something they didn't want to do. It does this by putting a false frame over the real content. So, for example, you might see and click a button labelled 'Play now', but what you're actually clicking is a 'Pay' button. You might inadvertently download malware, 'like' a post, turn on your webcam, delete all of your emails, send personal information, allow others to take control of your computer or pay money into an account.

It's advisable to avoid clicking buttons if you don't know exactly what they'll do and if you don't know and trust the source. If you receive a message on email or social media saying that someone has posted photos of you, is badmouthing you, is spreading rumours about you, or if you are offered a freebie which seems too good to be true, discounts on medication or if 'you're famous!', alarm bells should go off. **Do not click!**

BYOD

No, this isn't a Sunday braai and Bring-Your-Own-Dop. It's means Bring-Your-Own-Device and it refers to an IT policy that allows employees to use their own personal devices to access company information and data. BYOD is a vital component for future work and according to Forbes "… the BYOD market is expected to hit almost $367 billion by 2022, up from $30 billion in 2014."

Although convenient, if unmonitored, BYOD can present serious security risks. It is important for organisations to implement a structured security policy that takes into account which types of devices will be approved, security and data ownership policies and what, if any, IT support will be given to personal devices. These are just a few of the many cyber security terms that might come in handy.

PEN TESTING

You know that frustrating process where you need to take down an important number, but every pen you try has run out of ink, so you run around like a mad person, frantically scribbling on any and every piece of paper you can find in an attempt to make one of the pens work? Well, this is nothing like that. Pen-testing is short for penetration-testing and it is a tool used to identify the vulnerabilities in your systems.

By conducting this 'ethical hacking' procedure, organisations can spot and close security gaps before attackers find and exploit them. The more businesses open themselves to new technologies and digitised solutions, the more exposed they become to potential security breaches and so, according to Forbes's Technology Council, regular pen-testing is vital.

Pen-testing follows a five-step procedure:

1. **Reconnaissance:** the legally employed hacker gathers information about the target system.
2. **Scanning:** the attacker scans and gathers further knowledge of the system.
3. **Gaining access:** the attacker uses the knowledge gathered in the first steps to exploit the targeted system.
4. **Maintaining access:** the hacker remains within the target environment gathering as much data as possible.
5. **Covering tracks:** Any and all traces of the attack are covered.

5 CS OF EFFECTIVE CYBER-SECURITY IMPLEMENTATION

Change; Compliance; Cost; Continuity; Coverage. If you keep up with the latest trends and terminology and follow the 5 Cs, you should manage to stay on top of your company's cyber security… **with the help of Itec Central of course.**

CHANGE

Being agile and responding to shift in your industry, new regulations and technological developments.

COMPLIANCE

Following the latest regulation and policies, measuring and transparently reporting on how they are being followed.

COST

Researching and implementing the most cost-effective security for your company, without compromising on quality.

CONTINUITY

Making sure that your security is scalable for organisational expansion.

COVERAGE

Ensuring that you have the right system in place to ensure redundancy and resilience.

ITEC Central

+2711 731 6600 • john.considine@itecgroup.co.za • www.itecgroup.co.za