CYBER CRIME & INTERNET SECURITY

COMMON TYPES OF SECURITY BREACHES

In 2017, the World Economic Forum rated cyber security as one of the top risks facing the world today. Independently, business leaders prioritised cyber security as a strategic initiative demanding further focus, awareness and investment. Below, we highlight some of the more common cyber attack methods that individuals as well as organised syndicates are using to commit crime, malicious damage and insurance fraud in the market.

COMMON SECURITY BREACHES

MALWARE

PHISHING

PASSWORD ATTACKS

RANSOMWARE

IDENTITY THEFT

CYBER SCAMS

MALWARE - The term is a contraction of malicious software. Put simply, it's any piece of software that was written with the intent of doing harm to data, devices or to people. Viruses, Worms, Trojan Horses, Spyware, Adware are all forms of malware.

PHISHING – Cryminal syndicates target individuals and institutions by contacting them via email, telephone or text message, by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personal and insurance policy information, banking and passwords.

PASSWORD ATTACKS – Cyber criminals run a program that tries multiple passwords in order to gain access to your data. Brute force attacks or combination attacks are utilised to crack unsecure passwords.

RANSOMWARE – This is a very popular type of security breach that mostly affects businesses that need access to sensitive data in a timely manner. Data on a victim's computer is locked and payment is demanded before access is returned.

IDENTITY THEFT - Attackers can conduct countless criminal activities with a person's identity. They can seize control of a victims' banking credentials, apply for new banking accounts, commit insurance fraud and much more.

CYBER SCAM - Due to the high use of the internet, cyber scams and cyber fraud have disrupted organisations, bank institutions, sent viruses, and stolen personal information. In many cases, they convey an enticing offer that attempts to trick users into sending money or divulging personal information.

By exercising vigilance and following security best practices, users and organisations can take measurable steps in protecting themselves against cyber crime. But as we all know, nothing is stagnant on the web. Cyber crime is continually evolving, which is why organisations must continually train their employees and help them build upon their awareness of IT security threats in the market.

SOURCES: https://www.metacompliance.com/blog/5-types-of-cybercrime-and-how-to-protect-against-them/
https://emrisk.com/cpt-blog/5-security-breaches-risk-management/

#OrganisedDisruption