Cyber Security Threats

By Mark Gillan

scoosh media

10 Cyber Security Threats to consider

1. Phishing
2. Ransomware
3. Synthetic Identities
4. Deep Fakes
5. Social Media Misinformation
6. Cloud Jacking
7. Machine Learning Poisoning
8. AI powered Cyber Attacks
9. 5G Vulnerabilities
10. Internet of Things

Phishing

- Not a new threat, but evolving with more elaborate methods of attack
- Text message, email, phone call, letter, web pages; almost every means of communication
- Appear legitimate and ever closer with attention to detail containing links to a third-party with criminal intent to capture personal data for theft or fraudulent purposes
- Cyber criminals using every opportunity, including politics and health incidents
- Business communications should provide the recipient with a means of knowing it is legitimate

Ransomware

- Grown from ransomware attacks upon individuals and the private sector, we have witnessed large-scale attacks upon the public sector
- As governments move towards online portals for the majority of public services, no doubt we will see an increase in attacks of this nature to compromise and gather private information for illegal activities through the extortion of ransomware
- It is essential for all organisations, including public bodies to have regular backups and a plan of action for when something goes wrong – to avoid paying the ransom

Synthetic Identities

- People that do not exist!
- One of the fastest growing crimes
- Stolen personal data could be used by a criminal to create a synthetic identity for the purposes of illegal financial activities
- It can cost the victim thousands and many months to resolve the very damaging situation
- Impacts upon credit reference files, reputation and financial health
- The grab happens with snippets of personal data pieced together, such as name, address, date of birth, mother's maiden name, social security numbers
- Individual criminals tend to create multiple synthetic identities, sometimes hundreds, if not thousands of accounts
- Monitoring personal data, bank accounts, new accounts, strange activity on credit reference files and considering security of personal data

Deep Fakes

- It has often been said … “Don’t believe everything you see or hear!”
- Deceptive videos / audio are everywhere nowadays due to the accessibility of video editing software and Computer-Generated Imagery CGI that is very life-like
- Criminals can use deep fakes to blackmail or extort by falsely depicting a victim within a video
- As people rely upon social networking for news and especially concentrating upon video as entertainment, the use of deep fakes for criminal activity is increasing
- Legal advice and expensive tracing, along with knowing who might be capturing your image are some ways to fight against this crime

Social Media Misinformation

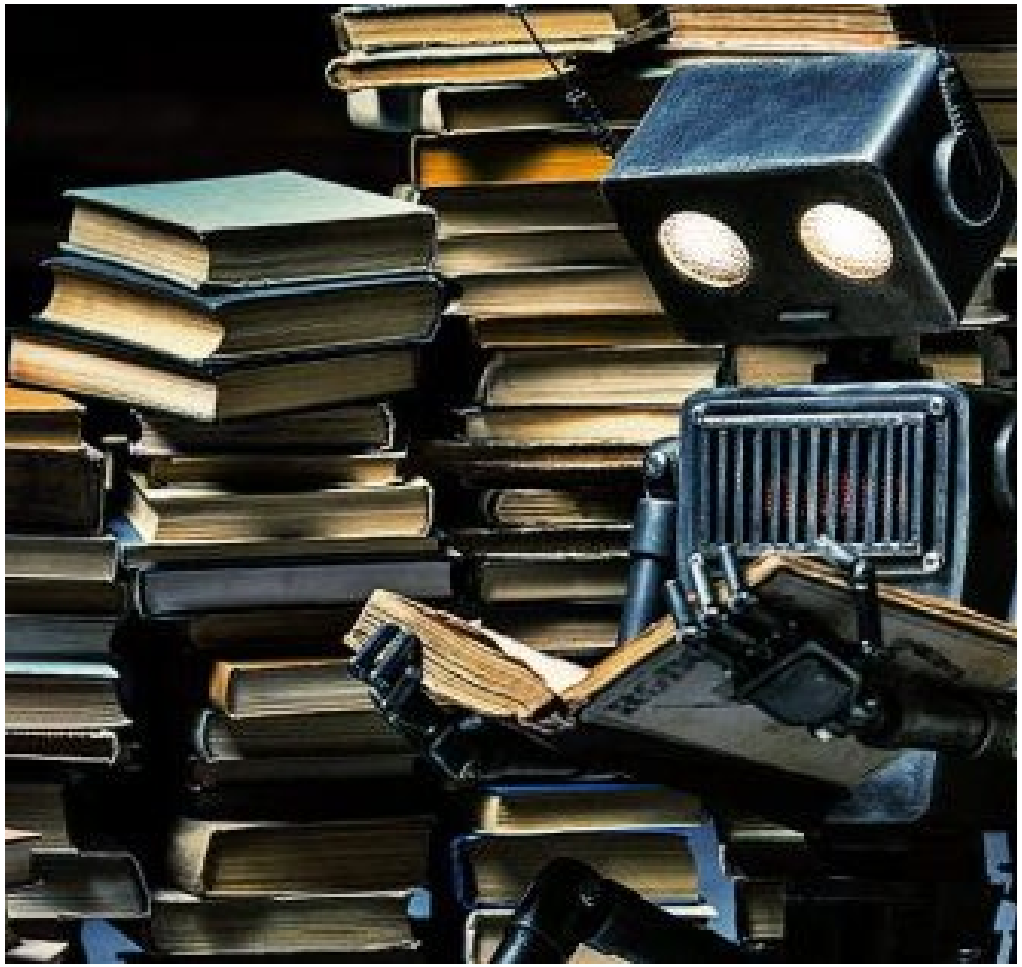
- It is so difficult to separate fact from fiction nowadays
- Fake news, misinformation, half-truths and downright lies
- Social media is full of misinformation that is shared before you can say "Jumping Jehoshaphat"
- Business can be damaged by vicious false reviews of products or services
- It is important we call out fake news as best we can, without destroying the possibility of it being correct
- Fact checking
- Businesses can monitor reviews and search social media on a regular basis for anything that could be damaging to reputation and respond to valid reviews

Cloud Jacking

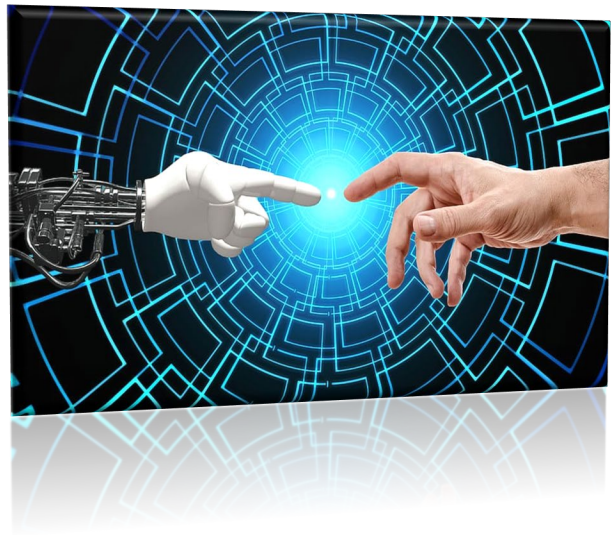
- Increased usage of the cloud means criminal and aggressive online swindlers target cloud services and data held on the cloud
- Large cloud computing centres are ideal for bitcoin and other cryptocurrency miners to mine data at a faster rate and increase their profits
- Cloud Jacking is the illegal control of a cloud server
- Causes severe and potentially devastating consequences by blocking and taking away important resources for all that rely upon the server or network for their computing needs
- Data centres / cloud operators and users need to maintain a high level of security, monitor and action any threat of intusion
- IDS – Intrusion Detection Software must be used to monitor, report, block, protect and organisations must have an evolving Cyber Security provision

Machine Learning Poisoning

- Microsoft piloted a machine learning program a couple of years ago and had to pull the plug days later due to the machine learning to be foul-mouthed and racist – it had been poisoned
- Machine learning can be beneficial in understanding clients by providing personalized recommendations based upon shared data
- Criminals will try to exploit by spamming systems with false or bad data, causing the machine learning to fail
- Systems could be a target for malware or malicious trojans, impacting upon the system and users alike
- All machine learning systems should be checked for accuracy, vulnerabilities and false activity by checking spikes of activity or unusual activity



AI powered Cyber attacks



- Is Artificial Intelligence able to fool us?
- Could we think an AI device is a human?
- Cyber criminals use the technology of AI for automation to trick us into lowering our guard, thinking AI won't do us harm. In the wrong hands, any technology can do financial harm and obtain personal data for the purposes of illegal actions
- Scammers improve their performance and utilise any form of technology that will do the job better and quicker for them
- Tapping into the power of Artificial Intelligence means the scamming, fooling and gaining of data is easier and certainly more efficient
- The power of AI learns to work harder at working with us and not against us, meaning we trust the technology
- It is essential we are better educated and employees are trained to identify the sophisticated operations of scammers using AI, for us to identify the difference between human and machine, to understand the workings of the criminals
- It is necessary to identify these types of attacks

Mobile Computing Vulnerabilities

- Movement into mobile computing and with telecommunication companies looking to increased speeds and bandwidth over the airwaves
- Increased data traffic combined with new technology that contains initial vulnerabilities means criminals are seeking new ways of operating online and attack any vulnerability
- With so many devices connected nowadays to wi-fi, it is difficult to keep trace of them all and to monitor traffic, but it is necessary to keep an eye on security for mobile devices
- The large increase in amount of data being sent and received over new wifi technology linked to mobile devices, it is just a fact there are more hacking attempts because there is more opportunity for hackers
- New technology, new ways of working, new reliance upon mobile technologies means it is even more important to be aware of the security issues and to monitor networks more than ever

Internet of Things (IoT)

- Smart TV's, smart devices and near enough everything seems to be connected to the internet nowadays
- Home and office, easy access to the internet for so many devices during our whole day means increased internet traffic
- Varied devices, varied security and possible less security on some of the devices that are new to internet connections don't have the best of hardware security
- Newest items seem to be higher risk, until they become targets on a regular basis for hackers, the manufacturers don't see a need to upgrade security because they appear safe – for the now
- Security that we have at home and office has to work even harder due to the number of connected devices and traffic being sent / received. Security is even more important now and even at home it is important for upgrades as well as monitoring. Increased knowledge is required for everyone as to security and our defences