DIGITAL SECURITY THREATS AND SOLUTIONS

BY MARK GILLAN

VIRUS

Threat

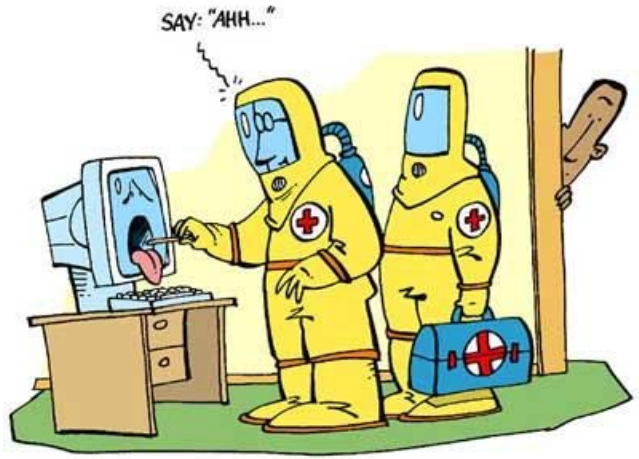
- Viruses come in various shapes, sizes and level of threat
- Can replicate themselves
- Install and infect devices without permission
- One of the most common means of transmission is for users to accept a prompt on their screen without reading or thinking it through
- Software, apps, downloads and certain files can carry a virus

Protect yourself

- Run anti-virus software on a regular basis
- Install important Operating System, Security Software and application updates as soon as they are released from valid sources
- Anti-virus software uses a library of known virus signatures and cross examine patterns with your files
- Ensure anti-virus libraries is updated to remain as protected against virus threats as is possible
- Purchase or use good solid security software

BY MARK GILLAN

PAYLOAD



- In digital security, payload refers to the part of a virus which performs a malicious or unwanted action
- Actions could include:
  - Switching off anti-virus software
  - Disabling a full security application
  - Accessing address books and send email messages with copies of itself to people known to the user, thus preying on trust and spreading the virus
  - Making changes to the operating system or utility software
- Viruses can be annoying, disruptive, malicious or all evils

BY MARK GILLAN

SPYWARE

Threat

- Type of malware
- Monitors your activity and can take control of your computer
- Usually secretly installed
- Installed without consent
- Normally unknowingly downloaded with software or installation of software

Protect yourself

- Anti-malware or Internet Security offering malware monitoring
- Security software to monitor all incoming network traffic and block likely threats
- Anti-malware is not the same as anti-virus software
- Anti-virus deals with older, more established threats and anti-malware targets newer threats

BY MARK GILLAN

WORRYING ESTIMATION

- **150 million** PC's connected to the internet are estimated to be in the control of hackers

SOCIAL ENGINEERING

Threat

- Social engineering is when a criminal uses publicly available information to compile a profile of you
- Can be used for fraudulent purposes

Protect yourself

- Lock down your social media accounts
- Be careful sharing information such as your birthday, location and even pet names
- Releasing pieces of information about yourself online can increase your chances of being targeted by cybercriminals

BY MARK GILLAN

DATA BREACHES

Threat

- Sometimes it is possible for third-party organisations to hold your data then experience a data breach
- Exposes all of the personal information to the public or another party
- Data can be used by other parties for criminal activities

Protect yourself

- Limit the number of organisations holding your data
- Shred snail mail to prevent any information being stolen by 'bin raiders' or anyone else
- Strengthen passwords
- Obtain dark web monitoring service to alert you of the use of information being sold or traded illegally
- Web watch services offer a monitoring service of illegal activity and actively seeks out any data use

BY MARK GILLAN

CLICKING HAPPY

- **78% of people are aware of the risks of unknown links in email messages but click it anyway!**

BY MARK GILLAN

PHISHING

Threat

- Exactly as the name sounds like – the setting of bait for a consumer disguised as a familiar organisation
- Contact via phishing scam an lead to malicious content being sent back in return or data stolen
- Phishing can also happen over the telephone (vishing) and text (smishing)
- Makes you believe it is the real thing when in fact it really isn't what it seems

Protect yourself

- Phishing, smishing and vishing rely upon deceiving the user to get access to information, including bank accounts and being talking to others might mean being clued up as to the most recent scams
- Be vigilant by always being suspicious of unexpected contact or anything that just might ring alarm bells
- Never click on a link within an email, type the link into the web browser address bar yourself
- Look out for spelling or grammar errors and carefully check web addresses and email addresses

BY MARK GILLAN

TYPICAL PHISHING SCAMS

- "You have won the lottery" or "My uncle died and left tonnes of money in a bank account" … the lottery scam is a common phishing scam known as advanced fee fraud
- "Verify your account" … Businesses or banks should not ask you to send passwords, account details, logon information or user names, Social Security numbers, or other personal information through email
- "If you don't respond within **48** hours, your account will be suspended" … these messages convey a sense of urgency so that you will respond immediately without thinking, sometimes they might suggest it is in the interests of security

SOCIAL MEDIA

- **1.6 billion social network users worldwide with more than 64% of internet users accessing social media services online**

TROJAN HORSE

Threat

- As in Greek Mythology, a Trojan horse conceals the threat inside a legitimate task
- Can lurk inside or ready to pounce based upon an action such as downloading a legitimate app or whilst updating the operating system
- Usually installed through backdoor programs that provides hackers with a secret doorway access to your device

Protect yourself

- Anti-virus security software, if up to date and respected on the market place usually picks up Trojans and blocks them or deletes files containing them or isolates them
- Clear temporary internet files
- Run anti-virus software on a regular basis and certainly before installing any file after downloading online

BY MARK GILLAN

SPAM

Threat

- Electronic junk mail and unwanted / unsolicited email is known as spam
- Spam is not only annoying but can be dangerous
- Can include malicious software as attachment, link to malicious online content or files

Protecting yourself

- Be cautious with unsolicited email messages
- Be cautious of email messages from family or friends or colleagues that are unexpected or contain strange wording
- Always be cautious of email attachments
- If it is too good to be true then it probably is too good to true
- Use alternative email address when signing up for anything online that might cause spam, just in case
- Check the 'from' field to ascertain exactly who sent the message
- Look for spelling mistakes, grammar errors
- Do not send personal or banking information by email

BY MARK GILLAN

LEGAL IMPLICATIONS

- **Inside jobs can account for data theft, including sensitive corporate data**
- **Inappropriate use of technology can lead to prison or heavy fines**
- **Scotland has strict laws relating to data protection as well as strict laws relating to online activity (communications act) with a number of people landing in criminal trouble for their online communications that threaten or abuse others**

BY MARK GILLAN

WORMS

Threat

- Computer worms are self-standing (standalone) malware programs that are self-replicating
- Unlike most viruses, it does not require a piggy-back or attachment to any other program to spread
- Usually uses a network to send copies of itself to other computers
- Exploits bugs in legitimate software to infect

Protect yourself

- Keep software, especially operating systems up to date to avoid known bugs being exploited by worms
- Use updates that are official from official sources
- Use software from official sources and with valid security updates / bug fixes

SCAREWARE AND RANSOMWARE

Threat

- Scareware is deception software
- Scareware is also known as "rogue scanner" software or "fraudware" with the purpose of frightening people into purchasing and installing it
- Quite often a pop-up will announce a virus on the system and offer to help the user with the non-existent threat
- Other scareware can advise the user to take false actions, sometimes the actions can damage a system when no threat was actually present
- Ransomware is virus software aimed at freezing a system and threatening to destroy data unless a ransom is paid

Protecting yourself

- Do not download any "Internet Security Software" that appears to be official or claiming to be fixing a device when in fact it is "scareware" in disguise
- Do not click on any pop-up that offers help or support with remote access to the machine, reboot the machine and execute officially purchased security software
- Avoid installation of any unofficial software, check online to see what other users are saying and any advice from more mainstream computer security companies
- Do not be frightened by scareware and do not pay ransoms, seek professional advice if required
- Ensure valid security software is kept updated and run on a regular basis – definitely checking any downloads prior to installation

BY MARK GILLAN

KEYSTROKE LOGGING

Threat

- Malicious keystroke logging software often installed via Trojans or virus
- Captures information by recording your keystrokes
- Criminals can get access to important information such as passwords, card numbers and other data to be used at some point

Protecting yourself

- Keystroke loggers don't tend to damage computers because they want to be working away doing their job capturing sensitive information, so anti-spyware and security software should be used at all times with being updated along with the operating system
- Anti-spyware applications can detect and remove keystroke loggers
- Sometimes devices such as computers slow down and take time to record keystrokes behind the scenes and then send to criminals, keep an eye on anything strange happening on your device and run anti-spyware immediately if things slow right down
- Be aware of your surroundings too

BY MARK GILLAN

MORE FACTS

- **600,000 Facebook accounts are compromised every single day**
- **More than 4,000 ransomware attacks have occurred every day since the beginning of 2016**
- **70% of Millennials admitted to bringing outside applications into the workplace in violation of IT policies**
- **The average time attackers stay hidden on a network is over 140 days**
- **Two-thirds of small businesses don't think they are vulnerable to cyber crime**
- **It's estimated half of SMB's could be hacked in under an hour**
- **35% of security professionals don't know if mobile malware is present on their network**

- **Facts sourced from Heimdal Security, Friedrich-Alexander University, HP**