
Link to Article on website

**Cybercrime is growing every year both in scale and complexity. We thought it would be useful to create a cyber security checklist to highlight some of the areas that RMs and others can look at to reduce their chance of becoming the source of a cyber breach.**

**ON 26TH MARCH 2018 EUROPOL ISSUED A PRESS** release with a head turning title of "Mastermind behind EUR1 billion cyber bank robbery arrested in Spain." Their statement went on to explain that "The leader of the crime gang behind the Carbanak and Cobalt malware attacks targeting over 100 financial institutions worldwide has been arrested in Alicante, Spain, after a complex investigation conducted by the Spanish National Police, with the support of Europol, the US FBI, the Romanian, Moldovan, Belarussian and Taiwanese authorities and private cyber security companies.

Since 2013, the cybercrime gang have attempted to attack banks, e-payment systems and financial institutions using pieces of malware they designed, known as Carbanak and Cobalt. The criminal operation has struck banks in more than 40 countries and has resulted in cumulative losses of over EUR 1 billion for the financial industry. The magnitude of the losses is significant as the Cobalt malware alone allowed criminals to steal up to EUR 10 million per heist."

Whilst Europol celebrates the arrest of this individual, the case with its eye watering values underlines the real, ongoing and substantial threat to the financial services industry, and why Risk Officers across the globe lose sleep over the ever increasing and international threat of cyberattacks. and other cyber security breaches. The costs associated with Cybercrime damage will continue to rise with costs predicted to hit EUR 6 trillion annually by 2021.

Cybercrime is growing every year both in scale and complexity, with novel ways of carrying out crimes being designed by highly funded

and organised criminal gangs who exploit the anonymity and speed of the Internet to commit criminal acts on victims located anywhere in the world where there is a computer connection to exploit.

There are a number of common ways in which a cyberattack can be deliberately or inadvertently facilitated including:

- Dishonesty,
- Human Error,
- Disclosure or selling of confidential company information,
- Social engineering attacks where attackers may use telephone to impersonate employees to persuade users/administrators to give user name/passwords
- Attackers persuade users to execute Trojan Horse programs
- Abuse of privileges/trust
- Viruses in programs, documents, e-mail attachments
- Weaknesses in IT systems or policies or controls

As you sit at your desk now and mull the potential consequences of such an attack on your financial institution, you may think that this is not your problem, but moreover an issue for the IT and technology teams to worry about. That would be very naïve thinking, because often the source of a cyber security breach arises from basic mistakes made by employees through lack of understanding of cybersecurity risks and how they can be reduced. In addition to dealing with the pervasive threat from criminal activity, the regulators are also expecting financial institutions to provide the right type of infrastructure, and also notify them whenever there is a breach. The significant risks are getting more and more attention from Government's around the world. As an example, on Monday the 5th February 2018 the Singapore Parliament passed a Cybersecurity Bill to respond to the pervasive threats.

With that in mind, we thought it would be useful to create a cyber security checklist that would be assist in highlighting some of the areas that Relationship Managers and others can look at to reduce their chance of inadvertently becoming the source of a cyber breach.

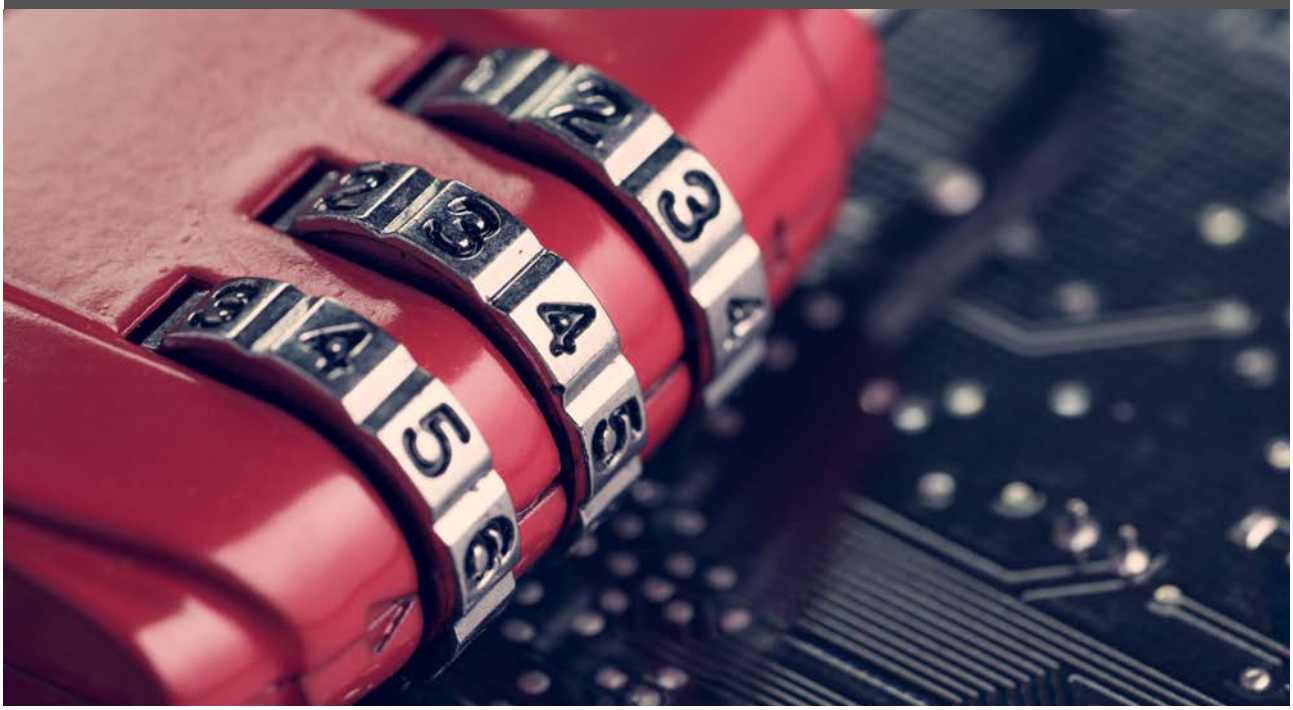
# POLICIES & PROCEDURES IMPERATIVES


- Make sure you are fully aware and comply with your organisation's IT, cyber security and data privacy policies
- Make sure you receive training on these at least once a year or whenever you are given new equipment that you might be unfamiliar with.
- Make sure you receive yearly training on current cyber security attack methods such as phishing and pharming, and threats including ransomware and other new cyber threats as they develop
- Make sure you fully understand how the company policy works in respect of use your own equipment for work purposes. Particularly important where there is remote or home working.
- Follow policies and procedures covering the management of personal data privacy
- Make sure you understand how to connect securely remotely to the company's IT system
- Connect securely to the work IT system carefully following the protocol outlined by your IT team
- Follow any policies covering laptop or other mobile device physical security. E.g. how are they to be stored when not in use.
- Follow any policy for identifying the retention of information (hard/soft copies)
- Follow procedures for protecting data during personal equipment repairs
- You should understand what the policy and procedure is when there has been a cyber breach and follow that procedure
- Follow procedures for disposing of waste material
- Understand and implement the organisation's Data Retention policy
- Understand the local and international laws that govern cybersecurity.
- Your organisation should undertake interactive cyber risk reviews from independent parties (separate to your penetration tester provider)
- Your organisation should undertake "table-top" training / simulation of a cyber incident that includes all internal (IT, HR, Legal, Communications) and external (government / regulator, media, customers, third-party vendors) parties




hubbis

# SOFTWARE



- Make sure you use anti-virus & anti-malware software directly from the publisher or vendor and make sure you use the up to date version of each as this software is updated regularly to take into account new threats
- Make sure you also run anti-virus and anti-malware on any media that is inserted into your computer e.g. USB thumb and external hard drives
- Activate real-time protection features and have regular full computer scans
- Pay attention to unusual symptoms that might show a malware infection, e.g. battery drain and unusual large data usage
- Pop-up security alerts of fake anti-malware software can be used to install malware on your computer
- Do not download unauthorised software or link unauthorised hardware to the IT system
- Make sure you operating system is up to date on your computer, tablets and smartphones
- Install only applications that have been approved
- Make sure all software installed on your computer is kept up to date
- Activate auto-updates of the software products you are using - always restart your computer to finish installing the updates
- Only use software products that have security updates
- Download software only from reputable sources
- Download and apply security patches
- When downloading apps, pay attention to what access you grant the app and only download from trusted sources

# PASSWORDS


## DO NOT

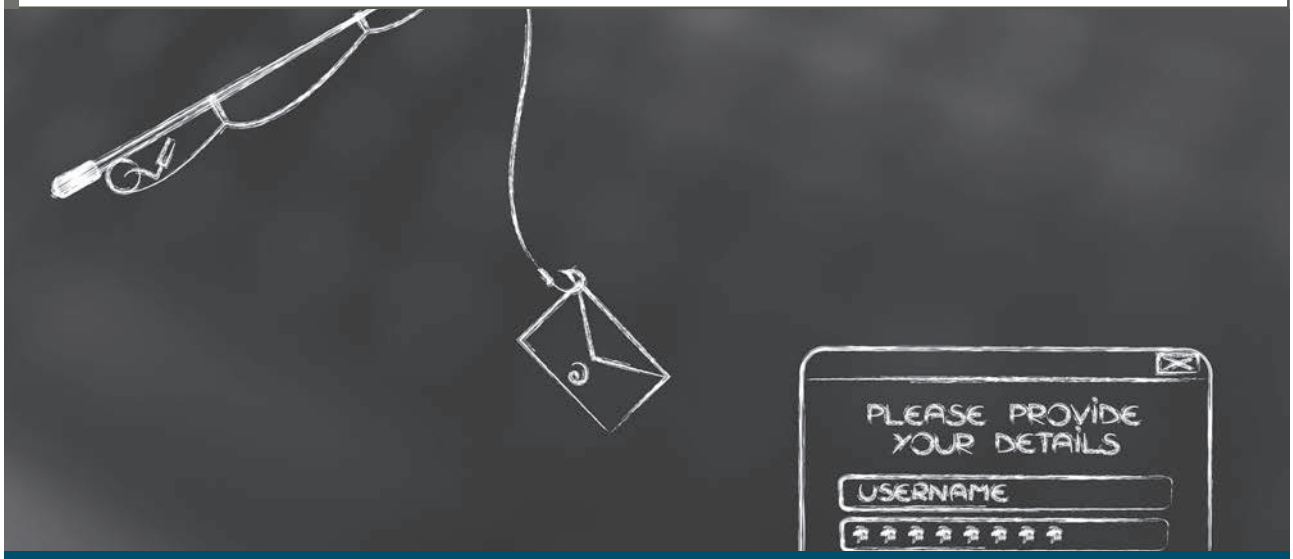
- × Use your personal login name as a password
- × Use your first, middle, and/or last name
- × Use your spouse's/ child's name
- × Use other information easily obtained about you (e.g. ID card numbers, birth dates, etc.)
- × Use a password with the same letter, for example "aaaaaa"
- × Use consecutive letters or numbers, for example "abcdefgh" or "23456789"
- × Use adjacent keys on the keyboard, for example "qwertyui"
- × Use a well known abbreviation
- × Use a password with fewer than eight characters
- × Reuse recently used passwords
- × NEVER provide your login, password or confidential information over the phone and to people you don't know.
- × When changing your password don't just change the final number in the sequence e.g. Password 1 to Password 2.
- × Don't share your password with anyone including secretaries, your boss or people in the IT team.
- × Don't let anyone watch you entering your password.
- × Do not call a friend at work and give them your password when you are sick.
- × Don't use the same password for your work devices as your personal devices.
- × Do not reuse your password
- × Do not write down your password
- × Do not use the same password for every system

## DO

- ✓ Make sure you choose strong passwords and change them regularly. at least eight characters with a combination of upper and lower case letters, numbers and special characters. Avoid using common words, phrases, or personal information and update regularly.
- ✓ Use various passwords for different systems with respect to their security requirements and value of information assets
- ✓ Use a password that is difficult to guess but easy for you to remember
- ✓ Have a strong password for your account
- ✓ A weak password increases the risk of unauthorised access to your computer
- ✓ Use a password manager
- ✓ Use a strong password to lock your phone or tablet
- ✓ Make use of two-step authentication wherever offered and change your password if you used it while connected to an unfamiliar network
- ✓ Use Dual/Two Factor Authentication or Two-Step Authentication on websites and services that offer it

# ACCOUNT PRIVILEGE

- Have separate user and administrator accounts
- Have separate passwords and use the administrator account only when necessary, e.g. when managing other user accounts or installing/ removing software
- Guest accounts on computers might provide information to attackers
- Assess the risk to using guest accounts and establish passwords for guest accounts which by default do not need a password

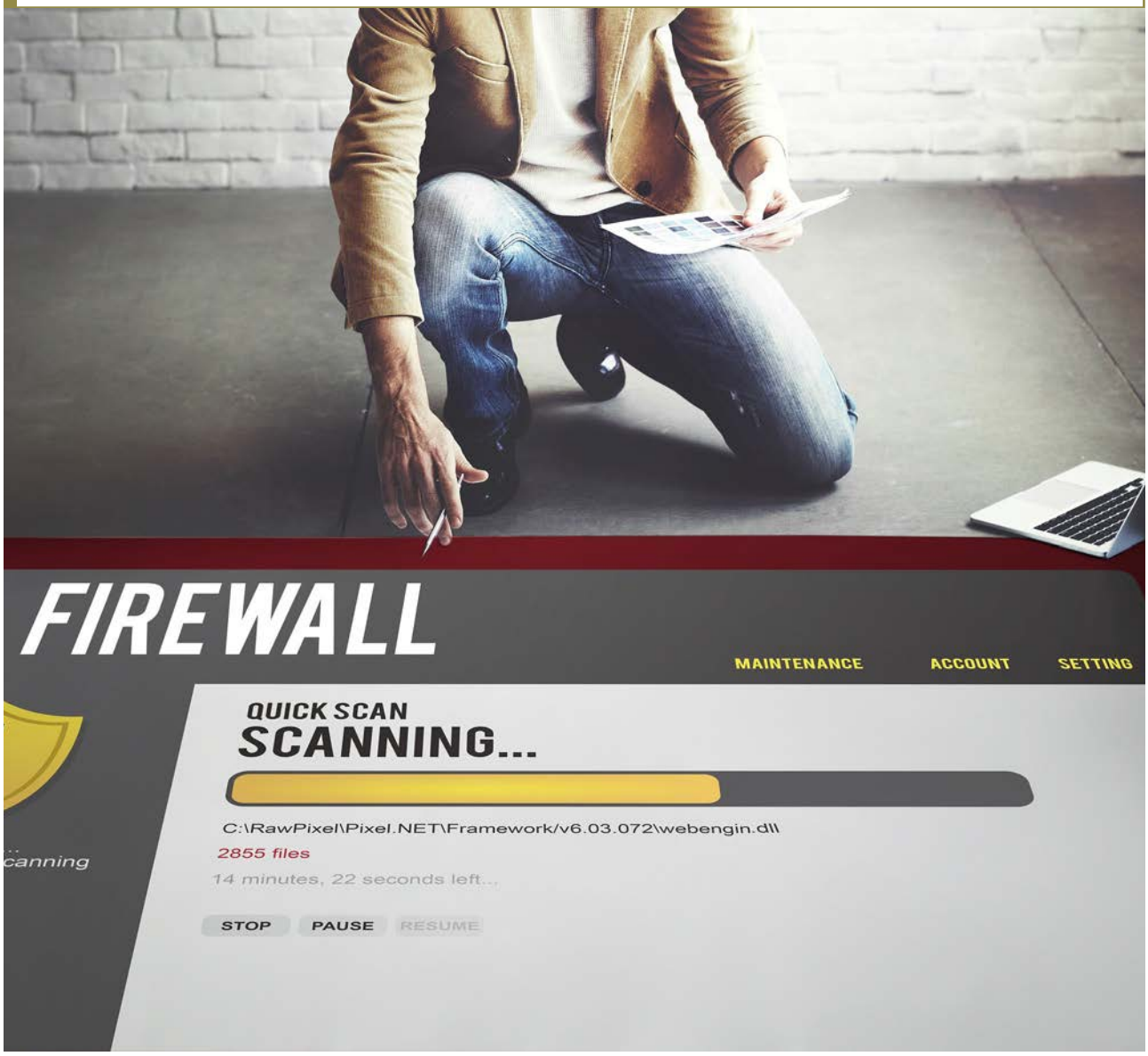



# SCREEN SAVER

- If you are not at your seat and using your computer, you need to protect it with screen saver passwords
- Enable the password protected screen saver at all times and never leave your computer unattended, particularly in public areas
- Use Automatic Screen Lock - when you move away from your computer or mobile device make sure that they are set to lock after a short idle time

# PERSONAL FIREWALL

- Enable your computer's firewall at all time to protect you from attacks from the internet
- Enable the built-in firewall of your router
- Make sure your firewall is turned on



# WEB BROWSER

- Check the security settings of your web browser
- Make sure you clear private data from Web browsers
- When connected via a public or unsecure connection, try to not use websites that require personal information
- Do not visit suspicious websites or follow links provided in suspicious emails from senders you don't know/ trust
- Always check a website's security certificate before sending sensitive information over the internet
- Pay attention to the URL of a website, as malicious websites at first sight might seem legitimate but the URL might use a slight variation in spelling or a different domain than the original website
- Use any anti-phishing features offered by your email client and web browser
- Check carefully website URLs. Malicious websites sometimes use a variation in common spelling or a different domain.
- Do not allow application to track or publish your location data to social media sites
- Disconnect your computer from the Internet when not in use
- Learn how to hover over an email link before clicking or to look at email properties to see if the sender's email address matches.
- Do not enable any option that allows downloads of applications from untrusted sources.
- Check for the https and lock sign when banking or shopping online
- Do not Open URLs or emails from untrusted sources
- Do not use wireless connections from unknown/ un-trusted sources to mobile devices
- Configure your system to use OpenDNS (with web filtering) to help prevent malicious content while browsing the web
- Look for HTTPS when visiting sensitive sites
- For e-mail you should disable the option to automatically download attachments.
- Understand the risks of using public wifi
- Do not do any confidential work on public WiFi and only connect to Wifi for firm work if you are sure it is authentic.
- Switch off Bluetooth and WIFI connections when not using them

# WEBCAMS AND MICROPHONES

- Physically cover the webcam lens on workstations, laptops, tablets, smartphones, televisions or games consoles when not in use
- Disconnect power supply and turn off and disable all appliances when not in use to prevent remote access to webcam or microphones on devices
- Use a smartphone book style cover so that the phone camera can be fully obscured when not in use

# DATA BACKUP

- Backup your data on a regular basic and protect the backups
- Test that you are able to restore your data from the backup data Use a VPN service when accessing public Wi-Fi

# DISPOSE OF DATA/ EQUIPMENT PROPERLY

- Use digital shredding software before getting rid of a computer
- When disposing of personal equipment make sure the hard drive is physically destroyed to eliminate the chances of data being recovered
- Make sure the shred bin is locked at all times
- Don't discard confidential documents in the regular waste bin at work, home or elsewhere
- When you no longer need certain data, delete it based on the relevant security requirements and data retention policy
- Don't part exchange an old smartphone or computer unless you are sure the data has been cleared and disposed of properly first

# UNUSUAL ACTIVITY

- Be suspicious of unsolicited phone calls, visits, or email messages from people asking about internal information or specific employees. If a person you don't know claims to be from a legitimate organisation, try to verify this information
- Be suspicious of unsolicited contact from individuals seeking information on internal employer data or personal information
- Do not provide personal information or information about your organisation, such as its networks or organisational structure unless you are absolutely sure the person is allowed to have this information
- Do not reveal personal or financial information in emails or react to emails asking for this information. Similarly, do not follow links in emails from unknown senders
- When in doubt, try to verify an email request by contacting the company directly
- Take particular care when you receive unusual e-mails
- Delete, without opening, e-mails from unknown sources
- Delete communications you receive that seem suspicious
- Verify the authenticity of requests from companies or individuals by contacting them directly
- If you see someone acting suspiciously don't just ignore it. Report it to management for further investigation
- Don't allow workstations to run in administrator mode as it can expose that machine to more security threats and can lead to the entire network being infected.
- Do not click on or open suspicious attachments in e-mails. If in doubt send it to the IT team for checking
- When you receive an e-mail from a client to carry out any actions on their account you should use a separate means of verifying the communication came from them such as a phone call to the client

# LOST OR STOLEN EQUIPMENT

- Back up data on a regular basis
- Be alert to possible security breaches
- If a device is lost, stolen or damaged notify IT team and follow their instructions
- For lost or stolen equipment, erase all firm data from the mobile devices remotely wherever possible

# PHYSICAL SECURITY OF DEVICES

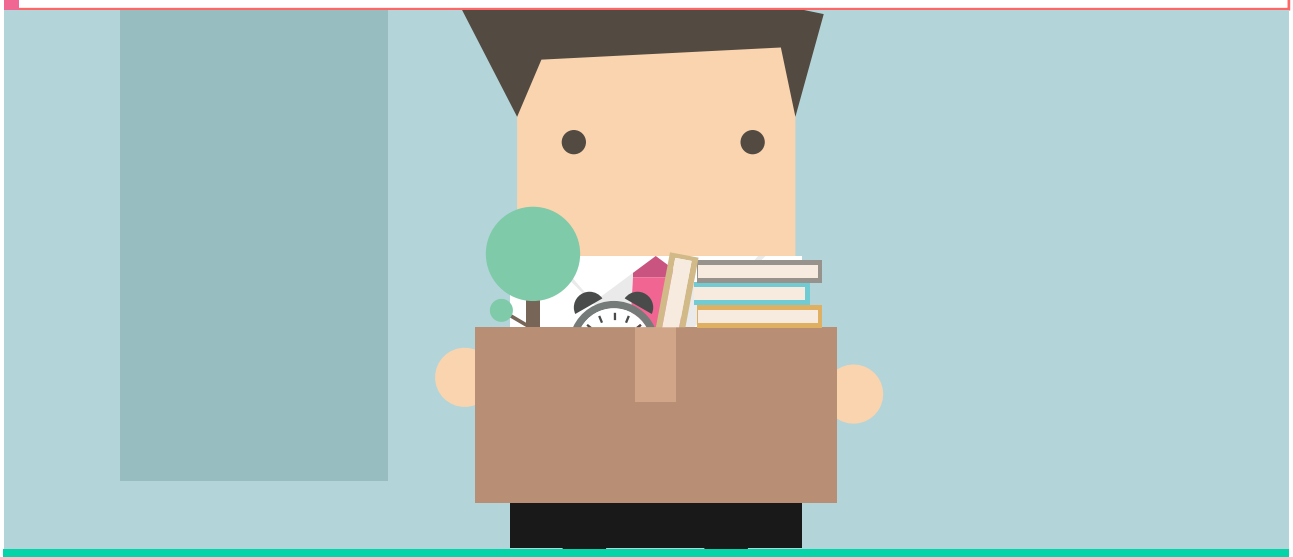
- Keep track of all your devices
- Keep a record of everything you use to store data e.g. laptops, tablets, smartphones, thumb drives, external hard drives and cloud storage
- Secure devices in terms of lock up any portable devices
- When using security passes to open doors, make sure that the doors are closed after entry to reduce the chance of unauthorised entry
- You should challenge anyone that is in the office that you don't recognise
- Keep the device in a secure place. Its physical security is your responsibility
- Don't let anyone use your equipment who is not authorised to use it
- Don't store sensitive data on USB drives

# ENCRYPTION

- Ensure data drives are encrypted. Encrypt backup data
- Use the built in disk encryption utilities on your laptop
- Secure send and receive e-mail using encrypted e-mail solutions
- Passwords and encryption should be done on all devices and not just the work computer
- Enable and configure security features of the operating system
- Use the encryption feature or a secured connection when processing sensitive data

# LEAVING AN ORGANISATION

- When you leave an organisation make sure that all firm data is removed from any personal equipment and that all other equipment is returned and fully accounted for



# INSURANCE

- Consider personal cybersecurity insurance and don't just rely on any organisation insurance coverage

# MOBILE PHONE

- Create a SIM Lock or PIN to prevent unauthorised use if your phone is lost
- Back up all data on a regular basis
- Directly report incidents such as loss of mobile device
- Do not synchronise classified/personal data from your mobile device with your own privately owned IT resources
- Don't leave your devices unattended and unsecured
- Do not store classified or personal data on your mobile devices, except in the case where appropriate security measures are put in place
- Do not keep sensitive information on your phone

# HOME WORKING

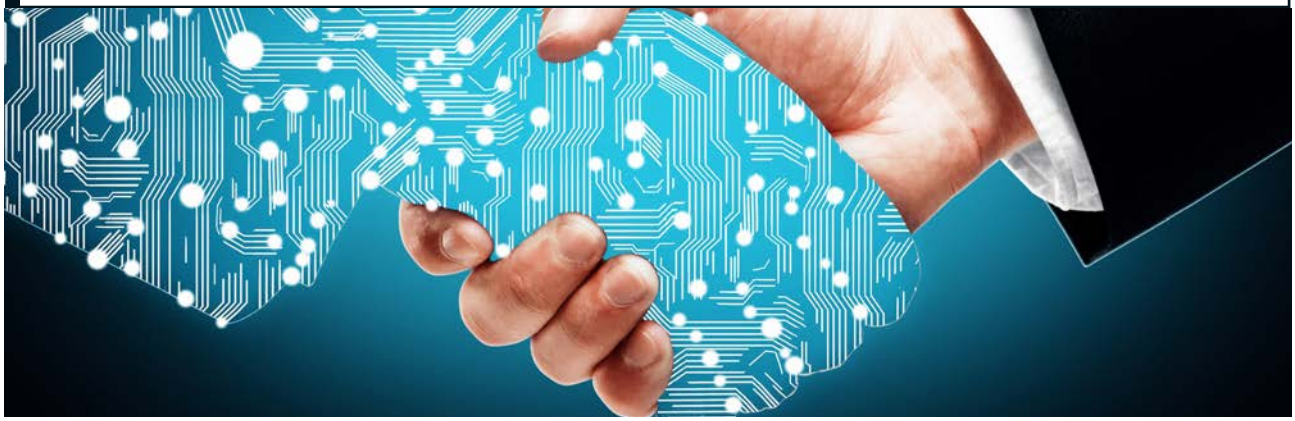
- Secure your home router by using strong wireless encryption and updating firmware
- If you need to work outside the office, try to minimise the amount of data you are taking
- Directly report incidents such as computer theft from home

# IDENTIFY AND PROTECT CLASSIFIED DATA

- Understand how to identify and protect classified data, including paper documents, removable media, and electronic documents
- Categorise pieces of data as highly confidential, confidential, just to make sure that you actually deal with it in the right way

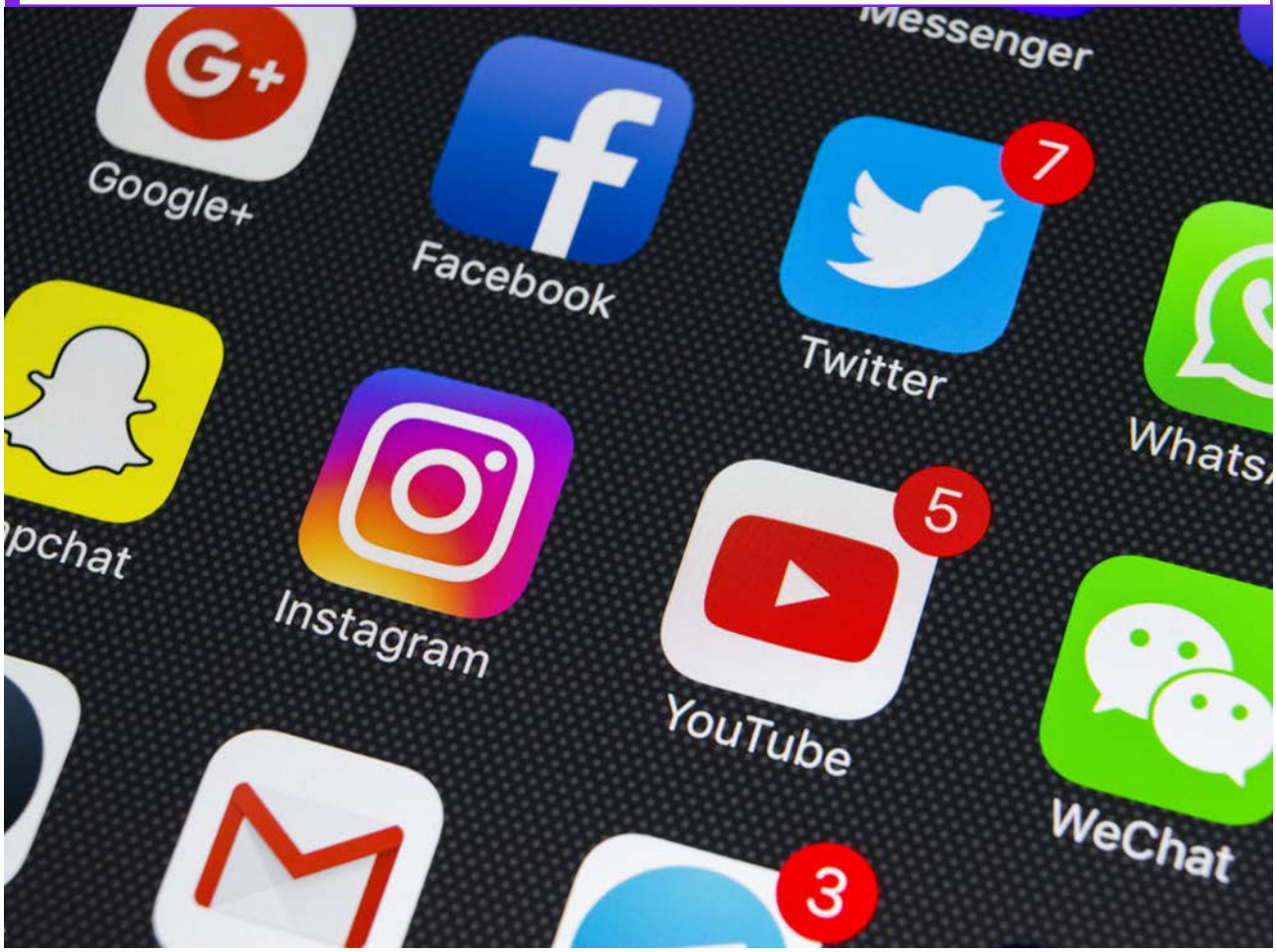

# HELPING YOUR CLIENTS

- Not only may you and/or your organisation become the victims of cyber criminality, but your clients may also fall victim to such crimes. You should provide your client with recommendations on how to use online banking services securely
- Security threats that can arise when using online banking:
  - *Your client's authentication information (e.g. username and password) can be stolen through spyware, phishing, and other cyber-attacks*
  - *Malware might be able to intercept messages of online sessions and steal information such as one-time passwords (required for transactions) and steal money through online transfers*
  - *Cyber criminals might employ malicious mobile applications to steal one-time SMS passwords*



# AS FAR AS USE OF SOCIAL MEDIA IS CONCERNED:

- Use common sense and judgement
- Always remember that what you post or publish may be public information for a long time and is available to everyone
- Never post information or news that you know is false (or that you have not verified)
- Be respectful of fellow co-workers, customers, suppliers and other stakeholders of the company you work for
- Be sensible. Avoid statements, photos, video or audio that reasonably could be viewed as malicious, obscene, threatening or intimidating
- Be transparent and - if so needed - disclose your relationship to your company
- Maintain the confidentiality of business and proprietary information
- Refer media, press, and investor inquiries to authorised company spokespersons if an official response is needed
- Respect intellectual property rights
- Minimise security risks
- Adhere to the code of business conduct, ethics and values of your organisation



# PROTECTION MEASURES FOR YOUR CLIENT FOR ONLINE BANKING

## DO NOT

- × Use hyperlinks from emails
- × Access online banking through results from search engine
- × Enter your personal or financial information in any suspicious looking pop-up windows
- × Disclose your log-in details to anyone or in any form

# DO

- ✓ Access online banking by typing in the URL directly or by using bookmarks
- ✓ Check that your connection is secure (watch out for the ‘s’ in https plus the padlock symbol)
- ✓ Pay attention to unusual occurrences such as unusual pop-up screens, abnormal slow responses, or unexpected information required or steps in the process needed for log in
- ✓ Use a strong password (do not write down or share it) and change it frequently
- ✓ Use different password for different online banking accounts
- ✓ Check your account and bank statement regularly for any suspicious activities
- ✓ Access online banking only over a secure connection
- ✓ Secure your computer with anti-malware software and firewall
- ✓ Always log out properly after using online banking
- ✓ If offered by your bank, activate account notifications (SMS/ email) sent out when transaction is executed that exceeds a specified threshold
- ✓ Protection measures for your client for online banking
- ✓ Always use a separate means of verification of client instructions received by email before you action a request