InfoSec 101

Here at The Verve Group, we take information security seriously, being in the financial sector means that we can be an attractive target for cyber criminals looking to steal sensitive and confidential information such as financial details, client records, login credentials and more.

By completing these steps, you are helping to limit our overall attack surface making it much harder for cyber-attacks to succeed and protecting the overall integrity of our data.

You are the front line

To get serious about information security you need to first understand that you are the front line, a high majority of successful cyber attacks start with the end user. Always stay vigilant with your emails and web use, hover over links before clicking to check they are going to the website you expect and if you think an email is suspicious or you are unsure, please report this to the IT helpdesk to check for you.

5 minutes of checking an email can save a Business from a hack attack or even worse, ransomware. We will cover phishing attacks later in this guide so you know what to look out for.

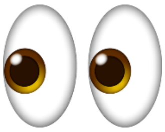
Strengthen your creds

It's important to use strong passwords for your accounts, whether these are online accounts or local. Did you know that a password including 3 words is stronger than a randomly generated password?

Follow these steps to avoid being a victim of brute force attacks.

- 12 characters long

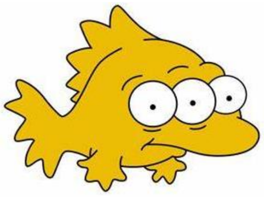
- Try to keep a 3-word format or sentence
- Include a special character (!"£$%^&*()_+)
- Include a capital letter
- Include at least 1 number
- Use 2FA wherever possible



Lock your screen

This is good practice for infosec, simply locking your screen when leaving your PC unattended avoids people around you from viewing any sensitive information or taking control over your PC.

This is good practice to follow in the office but more so when you are in a public place like Starbucks or on public transport.



Phishing attacks

Phishing is the number one strategy used by cyber criminals to infect PC's and networks, cyber criminals most commonly use email for their phishing attempts but this can also happen via phone and web.

Phishing is an attempt in where a hacker tries to convince the end user into clicking a link or opening an attachment which includes malicious software, the email is usually composed of clever wording in an attempt to convince the user that the email is legitimate and will likely come from a spoofed address your familiar with ie your colleagues email address however there are still key signs we can pick up on to know it's malicious.

Avoid getting hooked by checking the following...

- The message is sent from a public email domain

No legitimate organisation will send emails from @gmail.com or outlook.com.

- The domain name is misspelt

Some phishing attacks use slightly misspelt domain names to try and trick the user, ie support@gooogle.co.uk or noreply@facebouck.com – these could also be links like www.hmrc.ru/invoice.pdf or www.linkedinn.com/joboffer.docx

- The email is poorly written

Often the email is poorly written and contains grammar errors and typos.

- It includes suspicious attachments or links and is urgent

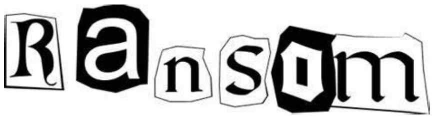
Phishing emails include a payload, this is either a link or attachment that contains malicious code. Most likely the sender has worded the email to sound urgent, perhaps there is an invoice that has not been paid or your company is facing a fine – these are not true but used to scare the recipient into clicking the attachments.

If you do not expect an email from that specific sender or do not recognise where they claim to be from – contact IT to investigate and move to deleted items to avoid accidentally clicking on the link or attachment.

We can always recover the email from deleted if it is legitimate.

- Legit companies don't request your sensitive information via email

Chances are if you receive an unsolicited email from an institution that provides a link or attachment and asks you to provide sensitive information, it's a scam. Most companies will not send you an email asking for passwords, credit card information, credit scores, or tax numbers, nor will they send you a link from which you need to login.



Ransomware

Ransomware is currently the highest threat to information security and can be very sophisticated. Ransomware is a type of malicious software or code that once exploited will encrypt all documents on a PC and spread on the network, this means that all your company data is now technically corrupt and unreadable. Ransomware has also been known to target backups as well, the only way to restore the data is by paying the Ransom fee set by the attackers or restoring from an intact backup.

The UK Government, NCA, GCHQ, NSA, CIA & FBI have all advised against not paying the ransom, this is because you are technically funding cyber-crime and there is no guarantee you will receive the decryption keys to restore your data. It is therefore extremely important that we keep up to date backups and an air-gapped backup that is not connected to the network.

The best thing to do if you think you have become a victim of ransomware is to disconnect your PC from the network, power off and report it to IT immediately. Some things to look out for is if you receive a pop up on screen demanding a ransom fee, your document icons change and your documents end in a weird format such as important-doc.encrypt or important-doc.docx.wcry.

Here are some statistics about Ransomware to show how serious this is…

- Last year Ransomware attacks cost businesses an estimated £14Billion.
- Businesses lost around £6,000 an hour due to Ransomware.
- 4.6% of world-wide Ransomware attacks were targeted at financial companies.
- 20% of Ransomware victims are SMB's.
- Malicious emails are up 600% due to Covid-19.
- The average Ransomware fee requested is approximately £144,000.
- In 2021, Ransomware attacks occur roughly every 11 seconds.
- The average downtime a company experiences after a Ransomware attack is 21 days.
- The most common tactics hackers use to carry out ransomware attacks are email phishing campaigns, RDP vulnerabilities, and software vulnerabilities.
- 65% of employers allow their employees to access company applications from unmanaged, personal devices.
- 29% of respondents stated their companies were forced to remove jobs following a ransomware attack.
- 71% of those who are affected by ransomware have been infected. Half of the ransomware attacks that are successful infect at least 20 computers in the organization.
- About 1 in 6,000 emails contain suspicious URLs, including ransomware.
- In 2021, the largest ransomware pay out was made by an insurance company at $40 million, setting a world record.
- 53% of companies who were victim of a Ransomware attack experienced revenue loss and their Brands were damaged as a result.

I hope you enjoyed this guide covering some basic security tips and give you a bit more insight into the importance of protecting ourselves against these attacks. If you have any questions feel free to contact me josh@weareverve.co.uk