Loss Prevention Standards – Cross Classes

Cyber - Social Engineering

Version: 1.4
Date: 24th October 2024

This document provides guidance on detecting and mitigating cybersecurity risks from manipulation and deception tactics aimed at exploiting human trust.

AVIVA

Cyber - Social Engineering

Introduction

The National Cyber Security Centre (NCSC) defines Social Engineering as: *Manipulating people into carrying out specific actions, or divulging information, that is of use to an attacker*.

Cyber criminals use social engineering tactics to convince people to open email attachments infected with malware, persuade unsuspecting individuals to divulge sensitive information, or even scare people into installing and running malware. The NCSC and Action fraud and cybercrime, constantly report on cybercrimes, and see actions by an individual which result in criminals gaining access to email, networks, systems, and sensitive data.

The individual:

- May be unaware they have given access or,
- They could have been coerced into giving access, or even worse,
- They could be aware there is a risk, but they have still gone ahead.

One common misconception when it comes to cyber security is to misunderstand the threat. Smaller businesses, and individuals often think *"We are too small to be of interest to cyber criminals," "I have nothing of value to cyber criminals" or" Cyber security costs a lot of money "*. The reality is exactly what cyber criminals would like you to think!

Misconceptions

"We are too small to be of interest to cyber criminals."

Unfortunately, that could not be further from the truth. Cyber criminals will look at any possibility to get hold of key data, bank details, etc., anything they can use for financial gain. Cybercrime is certainly not just aimed at the large multi-national companies.

Cyber criminals will endeavour to identify the easiest targets and those with less awareness or understanding of the threat. In such cases, there will be less cyber-based protections in place. As a result, instead of attempting to obtain, say £100,000 from a single targeted attack, a mass untargeted attempt could garner many smaller successes, and rather than grab media headlines a lot of this may well go unnoticed.

"I have nothing of value to cyber criminals."

One may think so, but everyone and all businesses, have a wealth of data and information that cyber criminals can earn money from. They are looking for anything they can be used to maximise financial gain. This could mean such things as household bills; passport information; photographs; social media accounts; online purchases; family details and bank information. Even a small business with a perceived small value at risk, will have employee personal details including salary records, and may well have links to suppliers and customers that may be the bigger target for the criminals.

"Cyber security costs a lot of money."

Some protections that could be required may well have a cost involved, but tackling the social engineering aspect can be key and involve minimal, if any, costs.

Raising employee awareness to social engineering and how to avoid doing the wrong thing, will be essential. Training days and phishing tests, etc. can bring the subject to life, and show great increases in awareness.

Also, robust procedural controls should be established which should result in improvements in cyber security. Password management, Multi-Factor Authentication, and making it imperative employees activate software updates on their devices, which include security updates, should not cost anything to introduce, but will make it much more difficult for systems to be infiltrated.

Cyber crime is not only committed by highly organised teams of hackers.

Types of Social Engineering and Attacks

Phishing

As mentioned in several Aviva Risk Management Solutions Loss Prevention Standard documents, phishing is a mass untargeted attempt by cyber criminals, to obtain valuable information. The attempt is usually by text message or email and hopes to get people to visit fake websites or click on links that introduce malware to devices.

Spear phishing and whaling are more targeted attacks with similar purpose:

- Spear phishing would be targeting a specific individual(s)
- Whaling would be directly targeting a key person in a prominent position in an organisation.

Baiting

Baiting can be online or physical and is the act of a criminal offering a person(s) some form of reward for taking a course of action. This course of action, such as *"click on this link to claim your £25 discount"* etc. will allow criminals access to key data or systems.

Physically, a USB stick marked CONFIDENTIAL could be left in a position where a person would find it, for example, and insert it into a computer, taking the bait to see what the confidential information is, and so introducing malware into the system. Other such examples include USB sticks being given away free, or provided containing information one may perceive as important, interesting, or containing a reward or prize.

Another example would be requesting completion of an online form, to go into a prize draw for a *"holiday of a lifetime."*

Pretexting

This is the use of a story or pretext to grab a person's attention, before taking it further. Once the target is hooked, personal information is obtained, or other items of value, cash, or key data is taken.

An example could be an email advising a person they are a beneficiary in a will. They will then need to provide personal information to prove their identity to ease the process of inheritance, and doing so could result in criminals getting information regarding bank details, etc.

Vishing

Effectively the voice version of phishing. The most common attack being an urgent voicemail requesting that you call back as soon as possible with a key detail, to avoid a set of circumstances. Example will be *"call back on the following number to avoid a £80 parking fine before 5pm"*

Complying would see criminals gain access to bank accounts, etc. This type of attack results in success because of the threat aspect.

Quid Pro Quo

This scam involves an exchange, giving the target the impression that it is legitimate and gives them a good deal. One example seen is a request for computer login details by an IT Consultant calling to fix an issue, software, programming, etc.

"If you can supply X, I can give you Y" always making it look a deal slightly loaded in the target's favour.

Tailgating

This is a basic type of social engineering and involves actual physical access into a building, by following closely behind someone with an accredited access. This act relies on the trust of the target, weak security measures or access systems, or the fact that few people would challenge others.

Contact Spamming

This is a commonplace scam that gets into an individual's email or social media account, and messages the contacts, usually with links or advice to visit a website, etc. As a result, any person doing so introduces malware onto their device and further.

This scam relies on people being more likely to act upon a message from a person or business they know.

Water-holing

This is where criminals infiltrate and infect a target website. Then when any person visits that website it then invites malware into their own systems.

The Human Element

All these examples of social engineering rely on the actions of a person or persons, either consciously or subconsciously, to allow a criminal to proceed and obtain the valuable items they require. They can be very believable and use recognisable company logos, online stores, large supermarkets, clothing brands, GOV.UK, World Health Organisation, etc.

How Can You Minimise Infiltrations Due to Social Engineering?

The key to protecting against this type of cybercrime is awareness, both as a business and as individuals. Time spent providing training to employees on what to look out for will be invaluable.

Either careless, accidental, or wilful provision of access to systems can be catastrophic for a business or a person. Ransomware attacks are becoming more commonplace. On a personal level anyone and everyone could be a target, so ensuring no personal, sensitive, bank details or data, etc. are passed on is imperative. The following are a few tips:

- ✓ Have an employee training event, advising everyone on what type of things to look out for.
  - Raise awareness of what social engineering can look like.
  - Repeat the training and provide refresher training.

- ✓ Restrict access to USB ports in company provided equipment.
  - Not allowing USB access reduces the chance of a virus being installed.

- ✓ Use Multi Factor Authentication (MFA)
  - If a password for example, is compromised – MFA provides other levels of access control before systems are breached and information could be at risk.

- ✓ If it sounds too good to be true**…** It probably Is!
  - Basic but true.
  - If you cannot remember entering a competition to win a sports car or holiday, do not click on any unsolicited links telling you that have won it.

"Complete these 3 easy steps to your £1000 prize"

- Seems like an effortless way to a nice windfall, but it's highly unlikely.

"Just provide your passport number as proof of your identity to claim your prize"

- Few competitions require divulging this type of detail - so why does this one?
- The Government are not likely to text you, so this type of activity should put people on alert!

Key Actions

✓ Antivirus Software

- Installing antivirus software will help protect your systems from most forms of attack, should criminals get past your access credentials.

✓ Be Vigilant

Many phishing attempts come from overseas, so check things such as:

Spelling and grammar

- While it seems a simple step, this might be an indicator to the fact that what you are reading is not genuine.

The email address, where did the email come from?

- If you hover an email address, it highlights the actual email address/string and not the 'dummy' name in the 'from' field.

A recent phishing attempt on customers of Nationwide Building Society asked for responses to a '.com' email address while all the Nationwide email addresses are '. co.uk.'

- If it does not look quite right do not click on anything, check it, and report it.
- Cybercrime on search engines or with Action Fraud
  - There may be reports of the same type of attack or similar.

Specialist Partner Solutions

Aviva Risk Management Solutions can offer access to a wide range of risk management products and services via our network of Specialist Partners who are reputable companies offering agreed discounted rates for Aviva customers.

For more information please visit:

Aviva Risk Management Solutions – Specialist Partners

Sources and Useful Links

- The National Cyber Security Centre
- ActionFraud

Additional Information

Relevant Loss Prevention Standards include:

- Cyber Security – Top 12 Tips to Protect Against a Cyber Attack

To find out more, please visit Aviva Risk Management Solutions or speak to one of our advisors.

Email us at riskadvice@aviva.com or call 0345 366 6666.*

*Calls may be recorded and/or monitored for our joint protection.

Please Note

This document contains general information and guidance only and may be superseded and/or subject to amendment without further notice. Aviva has no liability to any third parties arising out of ARMS' communications whatsoever (including Loss Prevention Standards), and nor shall any third party rely on them. Other than liability which cannot be excluded by law, Aviva shall not be liable to any person for any indirect, special, consequential or other losses or damages of whatsoever kind arising out of access to, or use of, or reliance on anything contained in ARMS' communications. The document may not cover every risk, exposure or hazard that may arise and Aviva recommend that you obtain specific advice relevant to the circumstances.

24th October 2024

Version: 1.4

ARMSGI1212024