Tackling

cybercrime guide

for advisers

358%
increase in malware attacks in 2020 compared to 2019.

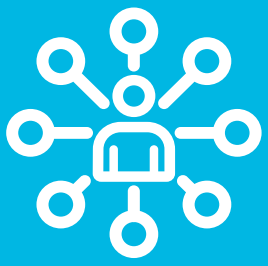
$8 trillion
cost of cybercrime in 2023

300 billion
number of passwords used online worldwide

39 seconds
frequency of ransomware attacks in 2021

700 million
attempted cyber frauds worldwide in 2020

85%
of data breaches involved a human element such as errors, privilege misuse or social engineering



6 billion
internet users in 2022

800%
increase in Russian-based phishing attacks since the invasion of Ukraine.

Sources
https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/
https://www.cybintsolutions.com/cyber-security-facts-stats/
https://www.idagent.com/blog/10-essential-facts-about-cybercrime-in-2020/
https://www.verizon.com/business/en-gb/resources/reports/dbir/

INTRODUCTION

Cybercrime, or online fraud, is one of the biggest threats faced by individuals and companies.

This guide is designed to help you identify and prevent attacks by explaining the steps you can take to protect your business and your customers.

Cybercrime is here to stay and we all need to be aware of how it can happen and the impact it has.

In 2020, it was estimated that a cyber-attack was attempted every 39 seconds and 700 million people were targeted (ID Agent). In 2023 cybercrime is expected to cost the world USD8 trillion (Cybercrime Magazine).

The staggering scale of cybercrime, and its increasing complexity, means that many organisations are struggling to keep up.

The rush to enable staff to work from home (WFH) when the pandemic first struck means that many companies focussed on ensuring staff had access to systems and information, sometimes to the detriment of security. The FBI estimates that cybercrime has trebled since March 2020.

And unfortunately there's more bad news for you, the financial adviser.

Companies working in financial services are particularly attractive to cyber-criminals, given those companies tend to have high net worth clients and hold personal (including financial) data about those individuals.

Small/medium sized businesses, like many adviser firms tend to be, are often seen as vulnerable targets to criminals, who believe those companies will have less sophisticated technology and processes to detect or prevent online fraud.

The reputational and financial consequences of a successful cyber-attack could be devastating. So what can you do to protect your business and your clients?

WHO ARE CYBER CRIMINALS?

Cyber criminals are not the lone keyboard warriors we might have imagined in the past, and their tactics have moved on from the crude emails supposedly from an African prince who requires your help to move their millions that are locked in their domestic accounts.

While the lone hacker is still around (as well as disgruntled employees and internet stalkers), cyber criminals are increasingly part of more organised and dangerous groups – whether this be for terrorism, state sponsored hacking or criminal networks.

Organised cybercrime is extremely well equipped and funded. Their methods are subtle and professional and the fruits of this crime are hugely lucrative. Organised Crime Groups (OCGs) view hacking individuals and businesses as a relatively low-cost and low-risk proposition.

OCGs will employ coders and malware developers to write malicious code to infect your computer or gain access to your network, intrusion specialists who exploit the networks they've successfully penetrated, data miners to steal information in bulk, and then money specialists who identify the nest way to make money from the data they've stolen.

HOW TO COMBAT CYBERCRIME

While most cyber-crime can be easily avoided, there is no magic bullet, no single solution to protect your business and customers. Instead, you will need a combination of measures.

Criminals are constantly evolving new, and more sophisticated methods, so it will be a constant race to keep a step ahead of them.

Our defences can be split into 3 main areas – which collectively provide a strong defence against cyber-attacks.

01 Technology

1. **Use appropriate Malware protection software**
   make sure to have comprehensive Anti-Virus software that protects your web browsing, email and scans your devices on a regular schedule. Remember, you generally get what you pay for so it's worth choosing a good one. And using 2 different systems will increase your chances of detecting threats.

2. **Control who has access to your systems**
   Make sure only those people that really need access to your systems are given it. And then ensure it is only those individuals who do actually access your systems. There are a variety of measures you can take, such as using Multi Factor Authentication, separating Admin and User accounts and using biometric security (touch ID/Face ID) on phones and any other devices where it is available.

3. **Ensure your software and security is up to date**
   Keeping on top of managing updates/patches ensures your software runs smoothly but also fixes vulnerabilities on your software that is susceptible to cyber-attacks.

4. **Establish an effective firewall**
   Firewalls create a buffer between your internal network and other, external networks. Firewalls monitor all network traffic and can identify and block unwanted or harmful traffic, such as criminals trying to breach your network.

5. **Secure configuration**
   Manufacturers often set default configurations for new software and devices to be as open and multi-functional as possible. While this makes it easier to start using new software it's not particularly secure, and is one of the most common gaps that criminals seek to exploit. Ensure that you don't use default or factory settings and passwords. And review the features available on the software and lock down those that aren't required.

6. **Email**
   It's estimated that email is the source of 80% of the viruses or ransomware that get into an organisation. Ensure your email security is set correctly – this can depend on the size of the company and which email service is being used.

7. **USB and drives**
   Though less common now, a USB drive is a convenient method of storing and sharing or transferring larger files. However, USB drives can be used to distribute viruses. If a USB drive is misplaced, lost or stolen, sensitive information can also be disclosed.

8. **Testing and monitoring:**
   Ensure that your IT team or your external IT consultants are carrying out regular tests to assess your systems vulnerability to attack. If you do have a virus, it's best to identify and deal with it as soon as possible.

   While the above tips are a starting point, we strongly advise you to seek expert help to set up and monitor your technology measures.

   If you're not sure about what you need to do, or how well protected your business currently is, a good starting point is to take the NCSC questionnaire https://getreadyforcyberessentials.iasme.co.uk/questions/

02 Your staff

There's an old saying that "prevention is better than cure". This is particularly true with cybercrime, given the serious impact a successful attack can have on your business.

So, while technology may be your first line of defence, your own employees are a second barrier to criminals. Human intelligence, and intuition, are often the most effective way to identify more subtle and sophisticated cyber-attacks.

Build a Cyber Smart culture

It's important to create a company culture where staff know and understand what is expected of them and feel empowered and encouraged to report any suspicions.

Are your staff suitably educated about the danger and different types of cybercrime? Is it easy for staff to report suspicions? Do you reward staff who identify and prevent cyber-attacks? How up to date are you with the latest cyber threats and methods employed by criminals?

Training

To successfully fight cybercrime, your staff need to know what they are looking for. A focus on general awareness and the common types of cyber-attacks will help them identify and prevent threats.

This training may take different forms, depending on the roles and responsibilities of different staff. It is particularly important for new members of staff, whose lack of knowledge of your systems and processes often make them most at risk.

It's also important that training is carried out regularly, and is constantly updated. This will ensure your staff are up-to-date with the latest information as criminals frequently change tactics and methods to target businesses.

Training should focus on some specific points too, such as:

1. helping staff to recognise "spear phishing" emails, and to not click on suspicious emails or the links or attachments on these emails.
2. encouraging staff to be sceptical and to act on their intuition if they feel something isn't right
3. explaining how staff should report any suspicions and how the company will handle any suspicious activity they report
4. the importance of following checking procedures and to not take short-cuts if they are stressed or busy
5. making sure staff use strong passwords. Passwords should be 8 or more characters, and contain a mix of numbers, letters and symbols.

Make working from home (WFH) as safe as working from the office:

The COVID-19 pandemic has led to a sharp increase in remote work, which has created new challenges for cybersecurity.

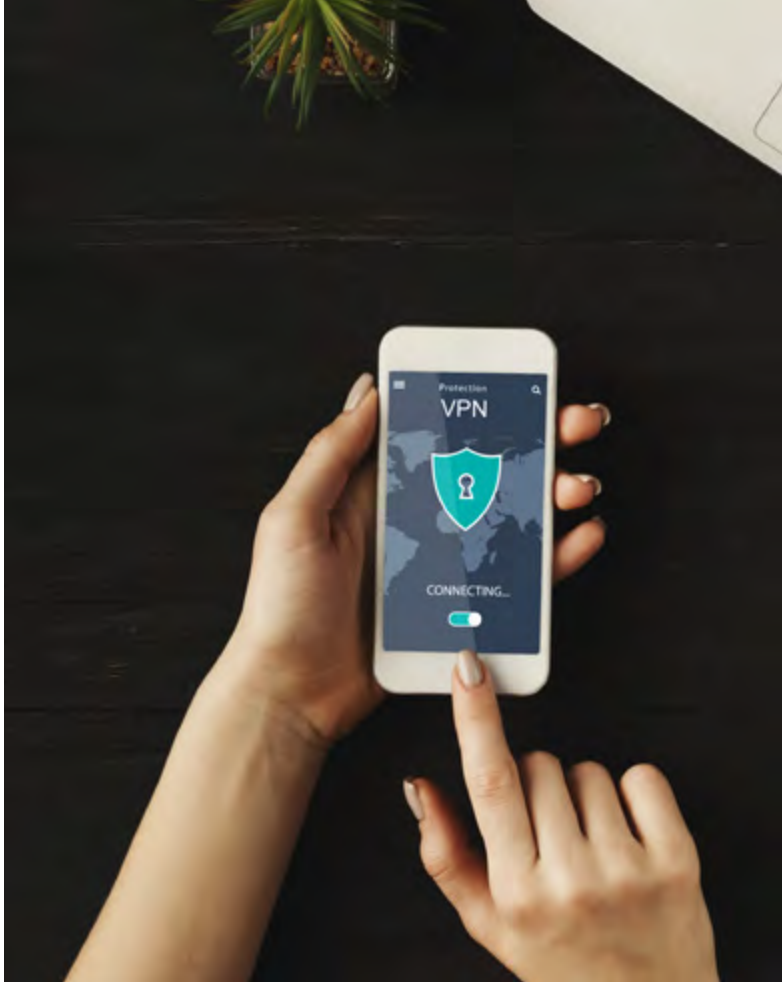
Employees who work from home are often using personal devices and internet connections, which can make them more vulnerable to attack.

The key to protecting your systems while working remotely is to use (and ensure your staff always use) a Virtual Private Network (VPN).

A VPN establishes a secure connection between you and the internet, encrypting your data traffic and disguising your IP address when using the internet. And while business travel has been significantly restricted recently, this is starting to change as restrictions are eased around the globe.

So it's vital that staff take their cybersecurity training with them when they're working away from the office.

Staff should know never to leave a portable device unattended when they are in public because the theft of that device will almost certainly lead to misuse. Even if you are vigilant, accidents can still happen, so staff should turn on the security features on their devices when they travel.



03

Extra vigilance around money in/money out

The ultimate goal of most cyber criminals is to steal money from their victims. It therefore makes sense to ensure that you are at your most vigilant when you receive requests to move or transfer money to new or different bank accounts.

We are all on the lookout for badly worded phishing e-mails from scammers that ask for personal/account information and these are often easy to spot. Much harder to identify are emails that appear to come from a person or business that we know and trust.

There has been a significant rise in so-called 'man in the middle attacks' during the pandemic. Hackers intercept email conversations using either the genuine email address of the victim or by setting up a new email address which is very similar but very slightly different to the genuine address. They then use the email address to impersonate the victim and correspond with businesses to scam the victim.

Very commonly the criminal will attempt to change the payment details in an otherwise legitimate request, and redirect the funds to another account.

What should you be looking out for?

1. Has a bank account changed unexpectedly? This normally happens shortly before or during the transaction process.

2. How was the change communicated and to you and by who? Was it in keeping with how the person/business normally communicates information? Is anything about the communication unusual?

3. Is the language used in the correspondence consistent with that used in other emails from the person or business?

4. Have any other details changed? For example, have contact phone numbers and email addresses of the person/business recently changed?

5. In particular, check the email address carefully. Has it been altered in any way? Have any new characters/numbers been added/removed or have any of the characters been replaced with a number or vice a versa? These may all indicate fraudulent activity

6. If you are replying to emails on a mobile phone please be extra vigilant as your phone may not display the full name/email address of the person you are responding to

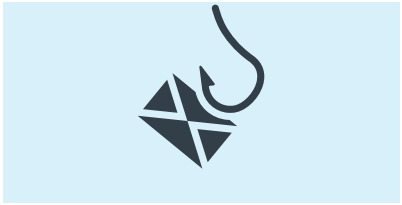
7. Has an attached form/invoice been tampered with? Are there changes to bank account details and signatures? Are there irregularities in the document – for example, typos and inconsistencies in typeface and font size? Is the formatting and text in the correct position and in-line with the rest of document? Does information look to have been copied or pasted in?

BE VIGILANT AND ON ALERT.

All of the above signs are red flags. If you are in any doubt, raise these concerns immediately and take action.

TOP 4 TYPES OF CYBERCRIME

Source: CyberSmart

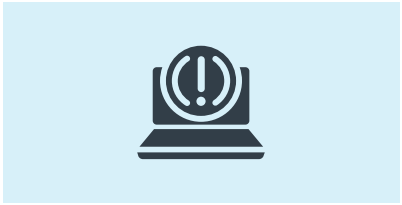


PHISHING

Web sites, phone calls and spam emails that appear legitimate, but are actually scams designed to acquire private data. 'Spear phishing', where an email appears to be from a known person or organisation, is particularly dangerous as it is harder to spot.

MALWARE

Malicious software installed inadvertently, usually by visiting a malware-infected (but otherwise genuine) website, or by opening an attachment from a phishing email. Malware can be used for anything from spying on keyboard input to infiltrating secure networks.



DISTRIBUTED DENIAL OF SERVICE (DDoS)

A mass orchestrated attack that floods a computer system with countless requests for information, rendering it incapable of responding to real users. DDoS attacks typically rely on 'botnets' – vast networks of hacked and remotely controlled computer systems.

HACKING

Hackers break into your computers and networks to access data. This unauthorised access can be via brute force to guess your passwords or software like spyware.

How to spot phishing emails

- Emails that look official but where the email address is from a common provider like Gmail or Yahoo
- Bad grammar and numerous spelling mistakes or typos in the subject line or body
- An email that appears to be from an authority like the bank or the tax office
- Strange links or attachments that you were not expecting

If you receive this type of email, report it to your IT team/partners immediately.