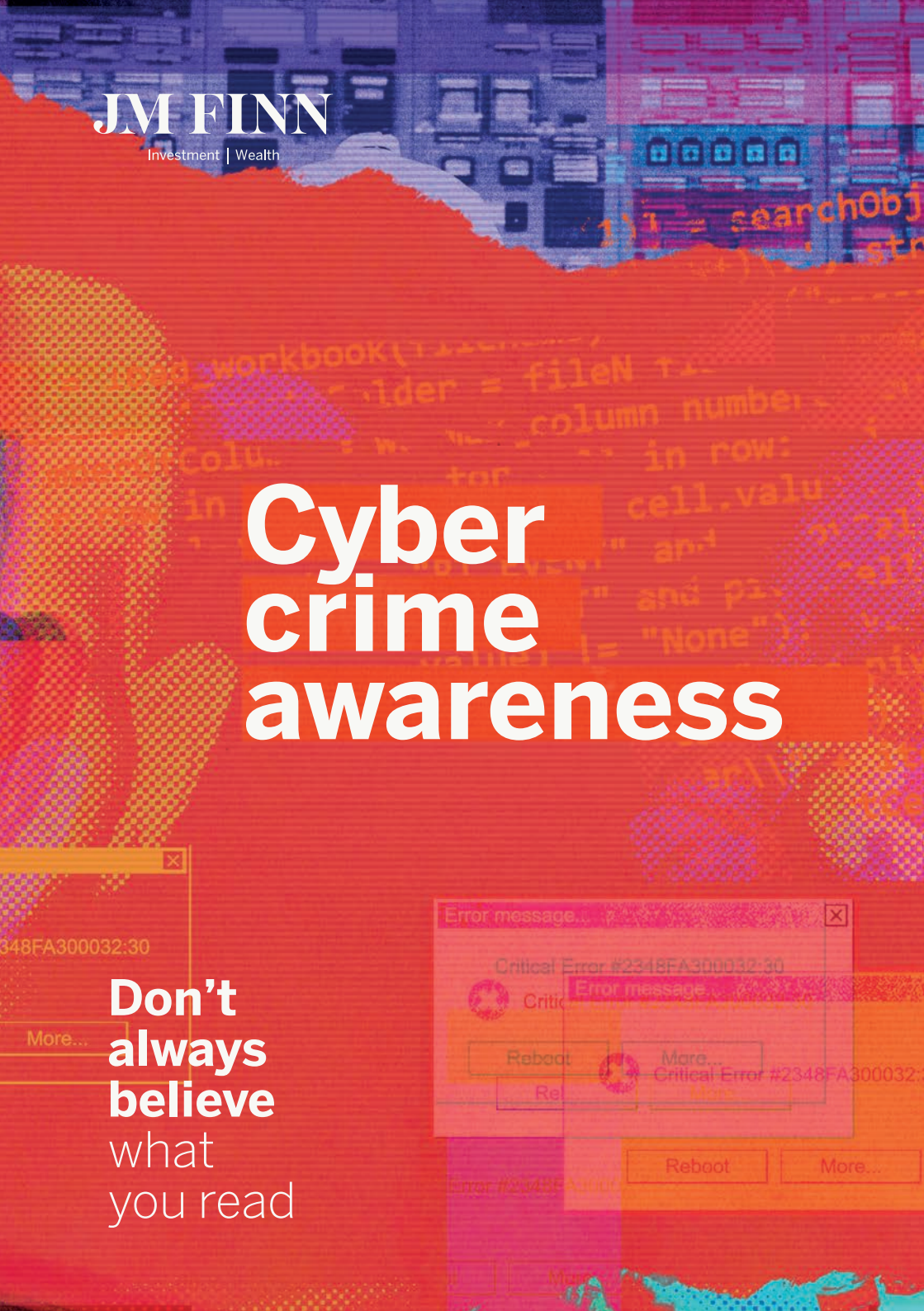
JM FINN
Investment | Wealth

Cyber crime awareness



Don't always believe what you read


Purchase Authentication
We've sent you a text message to your registered mobile number ending in 2920
Confirmation code
Confirm payment

The rise of cyber crime

Cyber crime, or crime that uses the internet or a computer to carry out the crime, is a term used to cover a whole host of different criminal acts. Most of them are not new. Fraud and scams have been around since time began but what makes cyber crime such a huge issue is the access to huge amounts of data that is provided by a network. And the fact that within any network there can be vast amounts of people.

In the 1980s it was boiler room scams that made the headlines, which soon progressed to customer fraud and pension scams, when a caller rang professing to be from a trusted source and persuaded you to invest in x, y or z scheme. The premise today is very much the same, with the most prevalent type of cyber crime being phishing.

Phishing is when someone attempts to steal your personal information by sending, typically, an email purporting to be from a legitimate website that you may have previously interacted with. Often it will ask you to validate your user details and password, resulting in you unwittingly giving your password to someone who should not have it. And given how many of us use the same passwords for each site, it is possible that the organisation or individual who is committing the fraud now has access to all your online accounts.

Many of us think that crime such as this is something that happens to other people. But anyone who has a bank account or investments for example is a potential target for this underworld of crime. With 80%[1] of businesses estimated to have come under attack at one time or another in the UK alone, and an estimated cost to the UK economy of £27billion[2], this is not something that can be ignored.

Online fraud and crime is also increasing rapidly. Google recently announced that they have seen 18 million hoax emails sent about Covid-19 on a daily basis, highlighting how fraudsters look to take advantage of crisis situations. As well as becoming more prevalent, fraud attempts are getting more sophisticated

as the criminals looks to circumvent the measures put in place. In the *Annual Cost of Cybercrime Study*, Accenture and Ponemon Institute (2019) reported that company security breaches were up 67% over the last five years. It is also worth considering that the number of internet users doubled in just three years from two billion in 2015 to four billion (nearly half the world's population) in 2018.

Individuals might well think this is a good reason not to have online accounts or use the internet less. Whilst this might protect you somewhat, it does not make you immune to cyber fraud, as your details will be held online somewhere and bank fraud is still carried out over the phone, as one of our case studies reveals, with payments made online and easily "lost" in the world wide web.

This guide is by no means an exhaustive resource to beating cyber crime but it does highlight many of the different tactics used by the fraudsters and offer up some tips as to how to limit your risk. If you only take away one thing from this series of articles, it is worth remembering that fraudsters are most likely to play on our own weaknesses. If we adopt an approach that questions the authenticity of any requests we receive, we will likely spot the fraud attempts.

We have also included some guidance on how to keep your business safe, taking some practical examples from the cyber security investment that JM Finn makes in a bid to retain its clients' privacy and fight the relentless attacks that come our way.

With social media being the mainstream communication tool for many of us, particularly, teenagers, we have included an article about how to protect your personal reputation online. One mistaken post can have long-term repercussions for an individual. According to Ofcom, 83% of 15 year olds have at least one social media account so it is important this cohort of web users are appropriately educated in how to protect themselves.

One thing this guide is not designed to do, is to scare users away from the internet. Since its founding in the early 1980s the world has embraced digital as its go to communication tool, allowing for faster, more efficient information flow that has served to enhance our lives. With careful and responsible use, we can continue to leverage the web in a safe and secure manner.

[1]Department for Digital, Culture, Media and Sport report

[2]UK Government (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf)

18 million hoax emails sent about Covid-19 on a daily basis, highlighting how fraudsters look to take advantage of crisis situations.

— Google

Social Engineering – the cost of human error

The fear of becoming a victim of cyber crime has been amplified of late due to its portrayal in the media. With recent data leaks involving major organisations such as British Airways, Equifax and Travelex, it can be incredibly hard to escape the constant coverage in the media surrounding the impact of cyber-attacks and its subsequent effect on society.

The deployment of advanced cyber security defences has not gone unnoticed by cyber criminals so they continue to attack the weakest link within an organisation; cyber criminals are bypassing the advanced defences deployed by many businesses and targeting their clients using techniques such as social engineering, as people are considered easier prey.

Social engineering can be described as the art of manipulating people so they give up confidential information or are persuaded to undertake an action for the benefit of the perpetrator. The types of information these criminals are seeking can vary, but when individuals are targeted by the criminals, they are usually attempting to trick them into revealing passwords or financial information. Cyber-criminals often use social engineering techniques to access the victim's computer, which may allow them to secretly install malicious software that will give them access to passwords and sensitive information.

It is considered easier to exploit a person's natural inclination to trust as it is much simpler to trick someone into revealing their password than it is for them to try to hack or guess the password.

Security professionals constantly state that the weakest link in the security chain is the person who accepts an individual or scenario at face value. It is irrelevant how many locks or deadbolts are on your door, or if have an alarm, floodlights, guard dogs and security personnel, if you trust the individual at your door who claims to be the delivery person and you let them into your home without confirming they are legitimate, you are completely exposed to whatever risk they pose.

If a cyber criminal is able to socially engineer or hack your email account they will have access to your personal correspondence and your contact list. Once a cyber-criminal has your email account under their control, they are able to manipulate your messages and send emails to any of your contacts, enabling them to impersonate you for malicious purposes. Research shows that cyber criminals are regularly monitoring compromised email and social media accounts to build a profile of their target. Once they have enough information they are able to use the data collected to impersonate the victim. For example, to communicate with your financial adviser or bank to extract money.

"Cyber criminals are bypassing the advanced defences deployed by many businesses and targeting their clients using techniques such as social engineering, as people are considered easier prey."

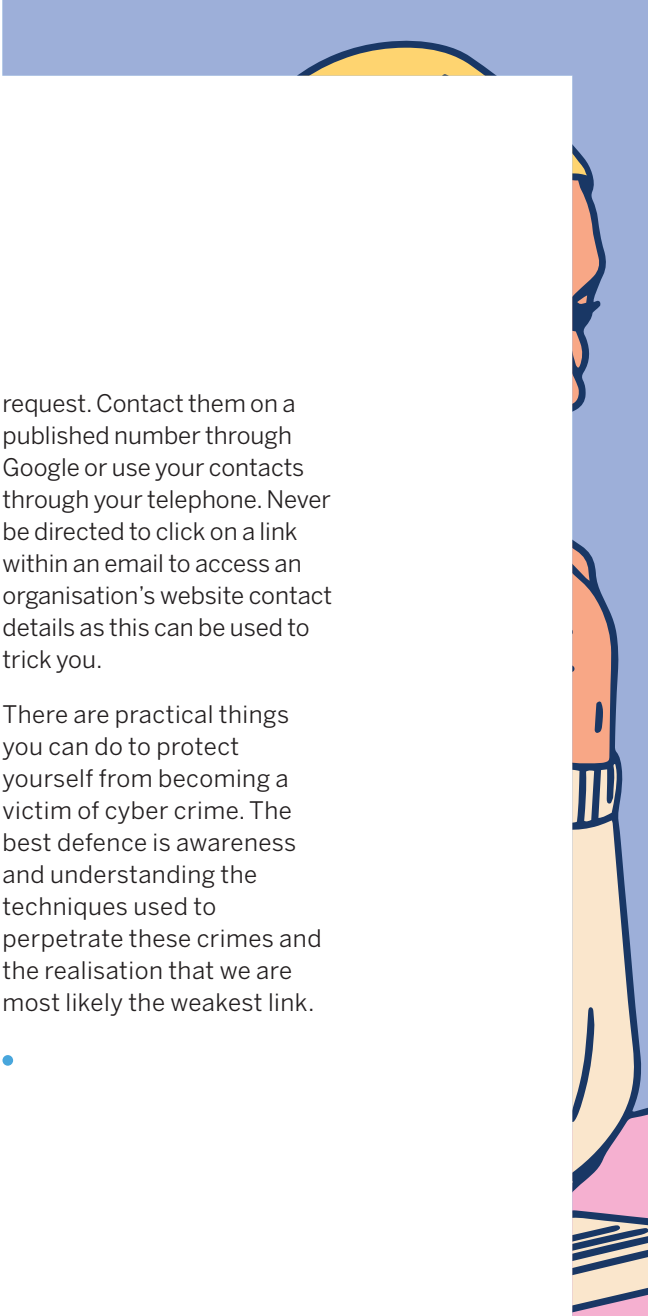
Even if you do not use online banking, email or social media, you could still be a target of social engineering fraud. Cyber criminals are able to manipulate the telephony system to impersonate any telephone number. It is relatively easy to impersonate


INCOMING EMAIL...
PayPal
Your account
has been limited
Verify my account
System HACKED

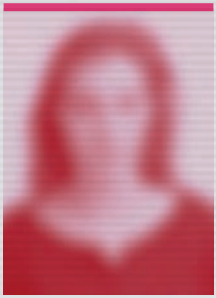
anyone within your contact list. You must never assume the call you receive is your bank because the number displayed matches your contact. Always verify the caller by dialling them back on a trusted number you know.

It is important to remember that cyber criminals may use a variety of techniques when targeting a victim. Their main objective is to force a target into making a decision or taking an action that they would not otherwise take. They can be masters of deception, using social engineering techniques to manipulate their victim. Cyber criminals will attempt to use urgency in various guises to force their victim into making a snap decision. Do not allow any individual to rush you into a forced action and always verify independently. For example, if you are contacted by your bank or financial institution, try to seek a known trusted individual within the business to confirm the request. Contact them on a published number through Google or use your contacts through your telephone. Never be directed to click on a link within an email to access an organisation's website contact details as this can be used to trick you.

There are practical things you can do to protect yourself from becoming a victim of cyber crime. The best defence is awareness and understanding the techniques used to perpetrate these crimes and the realisation that we are most likely the weakest link.



Case Study



Veronica – 39.

Founder of small clothing business and mother of three children, 9, 7 & 5

Being a fraud victim isn't something you imagine will happen to you – it's definitely something you read about and presume it's only those more vulnerable members of society who get sucked in. In hindsight, I still can't believe how easy it was to be tricked into giving away £20,000 - a significant portion of our savings for the children's school fees.

I was driving back from one of the boy's football matches and I got a call from someone purporting to be from the bank. He sounded familiar and convincing and asked me to confirm several transactions, which isn't unusual – their fraud prevention team is sometimes frustratingly efficient, ringing to confirm payments that are seemingly out of the ordinary. The last time they called was when I booked a hotel in Spain for a weekend trip. So I thought nothing of it when the chap asked me if I'd tried to buy a Mercedes in Manchester for £10,000.

Between us, we agreed this was definitely a fraudulent transaction and it was to be stopped. We carried on the conversation and he went into quite a lot of detail about how my cards and other accounts had probably been compromised and he should have a look into it, which seemed the sensible thing to do. Now I know to never give my PIN number to anyone but at some point in the conversation, I must have done. Remember I was driving and I got a bit flustered so I asked him to call me back in half an hour by which time I would be home.

I got home and immediately logged into my online account and sure enough two new accounts had been set up each showing a balance of £10,000. He called me back at the appointed time by which point I was feeling properly concerned. I asked him to prove his identity and he asked me to check the number on the back of my credit card with the number

showing up on my mobile – and sure enough, they were the same, so he was definitely calling from the bank.

He then persuaded me, that to cancel the two new accounts, I needed to make a payment to the central bank account, details of which he gave me. By this time, I was completely falling for his advice and unwittingly paid £20,000 into an account, which I thought was the bank's own account. It wasn't until the next morning when we got a call from the real fraud team that I realised I had been completely duped and gone against all the advice I'd ever known.

He had, by sounding knowledgeable about my account and talking like a bank manager, persuaded me to hand over my PIN. Once in my account he had changed the names of two accounts by using the nickname function and made some internal transfers so these two accounts had £10,000 in each. All he then needed to do was persuade me to make the payment. Seeing that my accounts had been "hacked" I was convinced something had to be done.

I asked him to prove his identity and he asked me to check the number on the back of my credit card with the number showing up on my mobile – and sure enough, they were the same.

I now know, and encourage anyone else in this situation, that what I should have done is called the bank back on a different line to verify their identity. Fingers crossed it won't happen again and that no matter what I'm doing at the time, I am clear-headed enough to challenge any instructions.


System message
Ok
MALWARE

Cyber Security Best Practice

Protect your email and online accounts by using a strong and separate password, as cyber criminals can use your email to access many of your personal accounts, leaving you vulnerable to identity theft or a target of fraud.

Install the latest software and app updates, which contain vital security updates to help protect your devices from cyber criminals.

Ensure your home computer system is supported Microsoft have now ceased support for Windows XP and 7 so pcs running these older, unsupported Operating Systems are susceptible to viruses and malware.

Turn on two-factor authentication on your email and other online applications to make sure your data is secure.

Use a password manager to help you create and remember passwords.

Secure smartphones and tablets with a screen lock offering your devices an important extra layer of security.

Always back up your most important data by backing them up to an external hard drive or a cloud-based secure storage system.

Slow down. Cyber-criminals want you to act first and think later. If the message conveys a sense of urgency or uses high-pressure tactics be very sceptical. You must never let urgency influence your careful review.

Be suspicious of any unsolicited messages or calls. If an email looks like it is has been sent from an organisation you know or trust, do your own independent research. Check the company's website, or a phone directory to find their phone number and call them to verify. Here are some tips on spotting phishing emails:

- Many phishing emails have poor grammar, punctuation and spelling.
- Is the design and overall quality what would you would expect from the organisation the email is supposed to come from?
- Is it addressed to you by name, or does it refer to 'valued

customer' or 'friend'? This can be a sign that the sender does not actually know you.

- Does the email contain a veiled threat that asks you to act urgently? Be suspicious of words like 'send these details within 24 hours' or 'you have been a victim of crime.
- Look at the sender's name. Does it sound legitimate, or is it trying to mimic someone you know?
- Your bank, or any other official source, should never ask you to supply personal information from an email.

Do not follow a link within an email or text message. Always be in control of where you are directed online by verifying the organisation.

If a sender appears to be someone you know and trust, if you are not expecting an email from that individual, particularly if the message contains a link or an attachment, always confirm with the sender before opening links or downloading a file.

Never trust an unsolicited download. If you do not know the sender and you are not expecting a file, never open or download it.

Sound too good to be true? If you receive an unsolicited email, or call from a lottery syndicate, inheritance from a distant or unknown relative, or maybe a request to transfer funds for a share of a bounty, it is almost certainly a scam.

Should I pay a ransom to unlock my computer? If your device has become infected with ransomware, the police encourage individuals not to pay the ransom. If you do pay:

- There is no guarantee that you will regain access to your data/ device
- Your computer will still be infected unless you complete extensive clean-up activities
- Attackers may assume that you would be open to paying ransoms in the future
- You will be funding criminal groups


Inbox (9,442)

What to do if you have been a victim?

The realisation that you may have been a victim of fraud can be extremely unnerving. There are a number of actions you can do to help limit the impact, both financially and emotionally.

Gmail, Facebook, Twitter... it does not matter what the service is, from time to time someone will find a way in. If one of your accounts has been hacked, do not panic, use these steps to help you regain control and protect yourself against future attacks.

Being locked out of the account is an obvious indication that something has gone wrong, but the signs can be more subtle. Things to look out for include attempted logins from strange locations or at unusual times. Changes to your security settings and messages sent from your account that you do not recognise are also giveaways.

1

Update your devices
The Operating Systems and apps on the devices you use should all be updated. These updates will install the latest security fixes. If you have it installed, run scan with up-to-date antivirus software. This is not usually necessary for iPhones and Apple tablets but should be applied to Android devices.

2

Contact your email provider
If you cannot access your account, go to the account provider homepage and find a link to their help or support pages. These will detail the account recovery process. Once you have regained control, check your email filters and forwarding rules. It is a common trick for the person hacking an account to set up an email-forwarding rule that sends a copy of all your received emails to them. Information on how to do this can usually be found in your provider's help pages.

3

Change passwords
Once you have confirmed there are no unwanted email forwarding rules in place, change the passwords on all accounts that have the same password as the hacked account. Then change the passwords for all the other accounts that send password reminders/resets to the hacked account.

4

Set up 2-factor authentication
This provides an extra layer of protection against your account being hacked in the future.

5

Notify your bank or other service providers
If you believe you have been the victim of an investment scam, alerting your bank, wealth manager, accountant or other professional services firm that might be a target for a hacker is essential. They can place a temporary freeze on your accounts designed to limit access to the hackers.

6

Notify your contacts
Get in touch with your account contacts, friends or followers. Let them know that you had been hacked. This will help them to avoid being hacked themselves.

7

If you can't recover your account
You may choose to create a new one. Once you have done this, it is important to notify your contacts that you are using a new account. Make sure to update any bank, utility services or shopping websites with your new details.

8

Contact Action Fraud
If you feel that you have been affected by an online crime, you should report a cyber-incident to Action Fraud using their online fraud reporting tool at **www.actionfraud.police.uk**

Protecting yourself from investment scams

The FCA ScamSmart website offers helpful support about what you can do to spot investment fraud.

Information on pension scams can be found at www.pension-scams.com

It is important to check that the companies with which you deal are authorised by the regulator, in JM Finn's case the FCA. These can be checked at the Financial Services register.

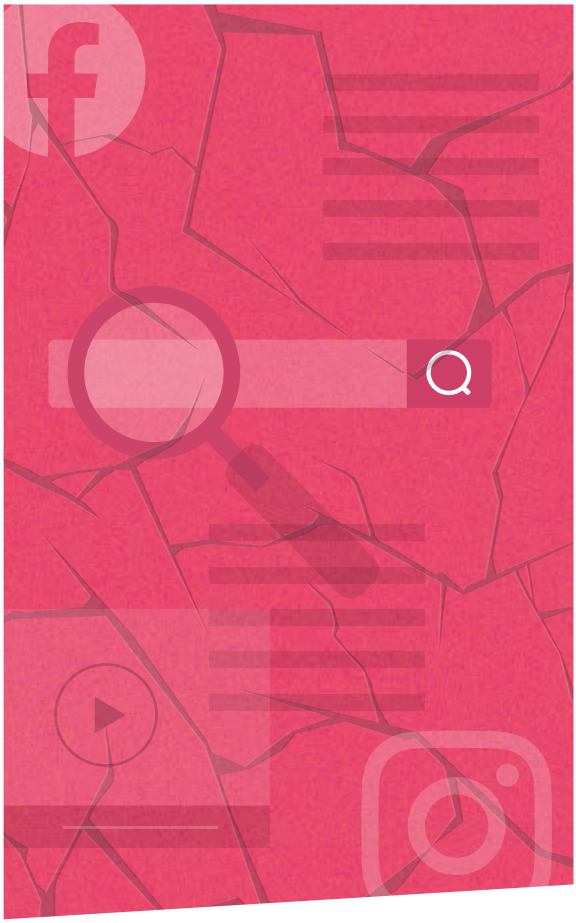
Fraud and cyber crime can be reported via ActionFraud, the UK's national fraud and cyber crime reporting centre. They also list the different types of fraud.

Protecting your personal reputation... online

Beatrice Giribaldi Groak
Client Director, Digitalis

Performing online research has become an innate reflex for millions of people. The latest Google study claims 3.8 million searches are conducted globally every minute. This data point tells us much about our reliance today on the internet to find information.

We trust Google to give us the answers to questions such as the "best restaurants in London", "top works of fiction" or "nearest supermarket", most likely never questioning the composition of the results we see. Indeed, online search engines influence the most menial choices we make every day. Opinions are moulded by a quick glance of online search results, with 98% of users never clicking past page one of Google. So, what happens when we start 'Googling' people we are sitting next to at a corporate dinner? And what happens when they start searching for you? This practice is increasingly more common and, as such, it is essential for us all to assess and protect our reputations online, to ensure that what is returned on search engines is accurate, contemporaneous and faithful to reality.



Digitisation and data shared everyday

With the world increasingly moving online and the digitisation of archives and records, the amount of information uploaded every day is staggering. Spurred by the omnipresent 'internet of things', our smartphones and the use of connected devices, we are most probably unaware of how much data we share per second. According to Raconteur's 2019 research, users generate 28 petabytes of data daily only from wearable devices, such as Apple watches. That equates to over half of all the entire written works of mankind, from beginning of recorded history, in all languages. That still pales in comparison to the number of photos, movies, messages, voice and video calls shared

and stored. Every day, we upload 95 million photos and videos on Instagram, we send 65 billion messages over WhatsApp and we make two billion minutes of voice and video calls. It is therefore unsurprising that around 40% of online information related to a person or a firm is unknown to the subjects themselves and that risks of reputational damage originating online are increasing.

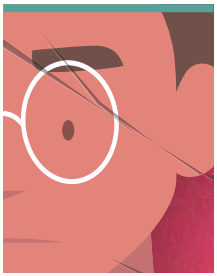
The 'cracks' in your digital footprint

Bishop Joseph Hall, 17th century clergyman and academic, famously said, "a reputation once broken may possibly be repaired, but the world will always keep their eyes on the spot where the crack was." The origin of the crack today is your digital footprint. Companies house records, old digitalised planning applications, open Instagram accounts, geo-tagged posts, public Facebook pages, old Twitter feeds are all great sources of 'publicly available information' easily found online.

"A reputation once broken may possibly be repaired, but the world will always keep their eyes on the spot where the crack was."

— Bishop Joseph Hall

They can also be a starting point for a sensationalist story. So much so that investigative journalists are increasingly turning to tech-powered tools to source articles in a time-efficient manner by mining the web and social media. The news site Vocativ and The Press Association's RADAR project (Reporters and Data and Robots)



even incorporate artificial intelligence (AI) to trawl the deep web for the information not readily returned by search engines.

While it is fair to say that every individual could be the victim of his or her own digital footprint, it is those more publicly visible who are more at risk. Younger generations of affluent families end up featured on the front page of the Daily Mail as a result of inflammatory photographs posted on certain Instagram accounts, which are monitored by journalists. Chief executives come under fire for lavish lifestyles and offshore structures, found out via information pieced together and harvested online. The examples can go on.

The media however is not the only source of concern. Ensuring you are well represented online is vital to your direct career and commercial networks. A negative due diligence report can be the cause of a business deal going sour. For the younger generations, an 'unkept' online profile can result in an unsuccessful college or job application.

Kintsugi, protecting your reputation online

Bypassing the obvious security and physical risks linked to oversharing online, remediating a reputation is harder than it appears. It is difficult to remove unsavoury information online which you do not have control over.

To mitigate reputational risks online, the best practice is first to exhaustively assess your digital footprint, next to find the vulnerabilities and finally to repair the cracks. Start by running an audit of you and your immediate

family circle's digital footprint, what we call the 'second layer', so that you are aware of what can be found out about you online. Address, if necessary, via legal means, any information which should not be available online. Then, ensure your profile is suitably developed, that your personal narrative appears clearly and correctly online, amending all inaccuracies. Develop it by creating appropriate online assets, such as official family websites and professional social media accounts, to help build a strong digital footprint while retaining privacy. Finally, always review your privacy settings on social media platforms, to restrict your updates and information to those who should be able to access them. Your profile will then be more resilient to online reputation risks.

> **"Opinions are moulded by a quick glance of online search results, with 98% of users never clicking past page one of Google."**

The Japanese call it the art of 'Kintsugi', repairing cracks and filling areas of weakness in a precious bowl using powdered gold.

•

digitālis

Digitalis is a digital risk and online reputation firm, primarily focussed on the specialist areas of narrative management, reputation risk and mitigation. Digitalis has no connection to JM Finn.

Case Study

Anonymous
Client of JM Finn

Being a fraud victim makes you feel labelled as making a mistake or committing a foolish act, so we tend to keep it to ourselves. My experience is one that I'm keen to share to ensure others do not fall into the same trap and because, I don't feel I made a mistake, I just chose to believe a highly professional con man.

Two days before Christmas last year I received a call from a chap who identified himself as the senior fraud investigator at JM Finn. He had some terrible news – that the firm who'd looked after my assets for many years was at the centre of a sophisticated fraud with my bank and that part of the process of catching and prosecuting him was to withdraw my funds from the firm and wire them to my bank account. I knew it was real as I was called from my investment manager's direct number, which showed up on my phone.

I was devastated – I'd known and trusted this chap for many years but my instant reaction was to protect myself so I called him up and told him to sell all my holdings. He was clearly stunned, which I felt was tantamount to alarm bells ringing in his ears but he did try his utmost to persuade me not to sell and went so far as to remind me that by selling all our joint holdings I was going to incur a significant capital gains liability and lose our long-built ISA allocations. Nonetheless, I gave my instructions.

He clearly felt uncomfortable about this and, to my irritation at the time, he continued to press me as to why I was doing this. Eventually, I relented and explained that I'd been called by his colleague and told about the investigation. That was when alarm bells went off. There was no such colleague and no one at JM Finn had called me. A fraudster had cloned a number, so it looked to

me that I was being called from a number I knew, and made false representations and asked me to transfer funds to my bank account, which turned out to be compromised.

I did lose some funds that were in the hacked bank account, but thanks to the perseverance of my investment manager, my investment funds were not sold and more importantly, the proceeds were not wired to a compromised account. The lesson I've learnt is to double check any instructions that are out of the ordinary, even if it comes from a number that you recognise.

A fraudster had cloned a number, so it looked to me that I was being called from a number I knew.

How to safeguard your business from cyber crime?

The threats faced by businesses are from cyber attacks by highly evolved criminals, many operating with relative impunity of prosecution. The risk to organisations can be multi-faceted, with attack vectors such as malware, viruses, ransomware, social engineering and the numerous other commonplace threats.

Whatever the maturity or the size of a business, there are practical things they can adopt to build stronger defences that can reduce the risk and impact of a cyber attack.

Assessment

Many organisations may not fully understand the threats to their business. An independent assessment would help them evaluate their current risk posture, which is offered by many cyber security companies.

Develop a cyber hygiene strategy

A plan should be formulated to address current policies, procedures and budget, as well as staffing and technology improvements. No matter the size and maturity of the business, a cyber hygiene plan should be considered essential if the risk of a cyber attack is to be effectively controlled.

Effective controls

Additional controls may be required to mitigate the risks identified by the assessment. If the business does not have the skills to identify the type of controls and technologies required, they should seek trusted, external advice to ensure the right controls are implemented.

> **"Businesses need to ensure their employees understand how cyber criminals operate and how staff can be manipulated."**

Staff training and awareness

Cyber criminals are experts at exposing a point of entry into an organisation's computer system or through its network. Businesses need to ensure their employees understand how cyber criminals operate and how staff can be manipulated. Regular cyber security seminars and computer based training sessions are essential.

Effective regular patching regime

Out of date applications are more susceptible to malware and cyber attacks. These can lead to an attacker penetrating an organisation's network and instigating a data leak that may cause significant reputational damage. All applications should be checked on at least a weekly basis. Consider implementing a vulnerability management solution that can check for vulnerabilities and apply missing patches.

Create and test an incident response plan

Whatever protective controls are implemented they can never fully mitigate the risk of a successful cyber attack. Businesses should plan for the worst-case scenario by deploying a well thought-out and robust incident response plan that outlines an effective

reaction to a cyber attack. The plan should be regularly assessed and updated, ensuring any changes to the business are incorporated. Consider the adoption of a framework for policies and procedures: Best practice procedures can be enforced through the adoption of an independent framework such as ISO-27001, Cyber Essentials, NIST or SANS CIC 20. ISO-207001 and Cyber Essentials have the additional advantage of an independent certification process that may be desirable for many organisations.

Conduct regular external security assessments

Once cyber security controls have been implemented, the controls should be independently verified by a specialist company that holds industry standard accreditations such as Crest and Check.

Create a culture of good cyber security hygiene

Perhaps the most important element of any effective cyber security programme is the ability to embed good cyber security hygiene into the fabric of the business. Cyber security should be driven from the senior management and enforced at all levels of the organisation.