

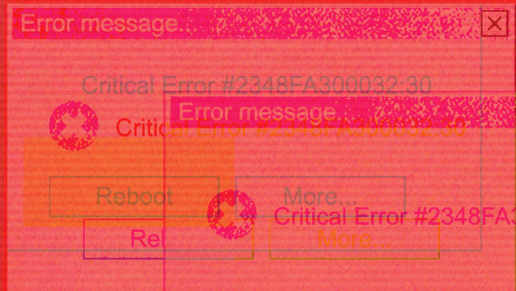
JM FINN

Investment | Wealth

Cyber crime awareness

Don't
always
believe
what
you read

More...



Reboot

More...

Error #2348FA3000

More...



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 is a potential target for this underworld of crime. Online phishing attempts are also increasing rapidly. A mind boggling 1.76 billion phishing emails were sent in 2023, a 51% increase from 2022¹ as the criminals look to circumvent the

¹ <https://www.vadesecond.com/en/phishers-favorites-2023-ebook>

measures put in place. Over £1.2 billion was stolen through fraud in 2022 – with the vast majority (80%) of this starting online². It is also worth considering that the number of internet users has now increased to 5.5 billion as of April 2024 – equivalent to 67.1% of the world’s population up from four billion in 2018. 63% of people globally are now also on social media.

Individuals might well think that the rise in online fraud is a good reason not to have online accounts or to 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.

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 offers 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 create a secure password, taking some advice from JM Finn’s Head of IT, Jon Cosson. 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.



² <https://www.ukfinance.org.uk/news-and-insight/press-release/over-ps12-billion-stolen-through-fraud-in-2022-nearly-80-cent-app>



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 Fujitsu, Dell and JP Morgan Chase 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 you 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.

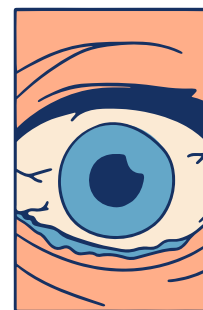
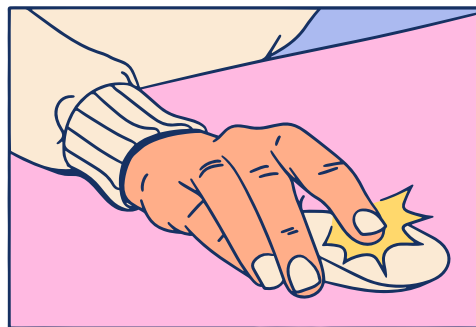
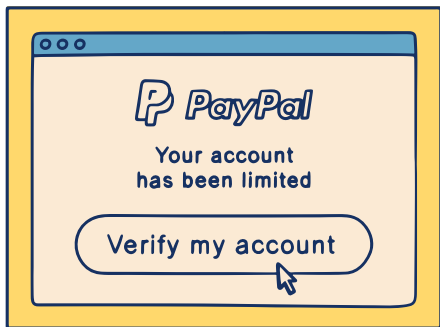
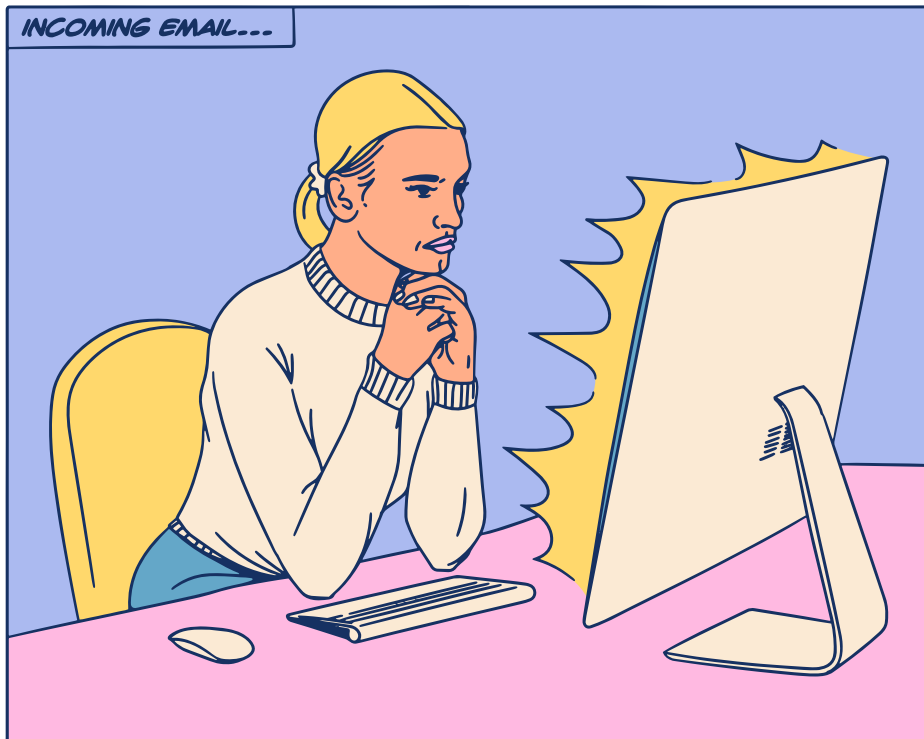
If a cyber criminal is able to socially engineer or hack your email account, they will have access to your personal correspondence and your contact list. Once a cybercriminal has your email account under their control, they are able to manipulate your messages and send emails to any of your contacts, 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 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 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, an understanding of the techniques used to perpetrate these crimes and the realisation that we are most likely the weakest link.



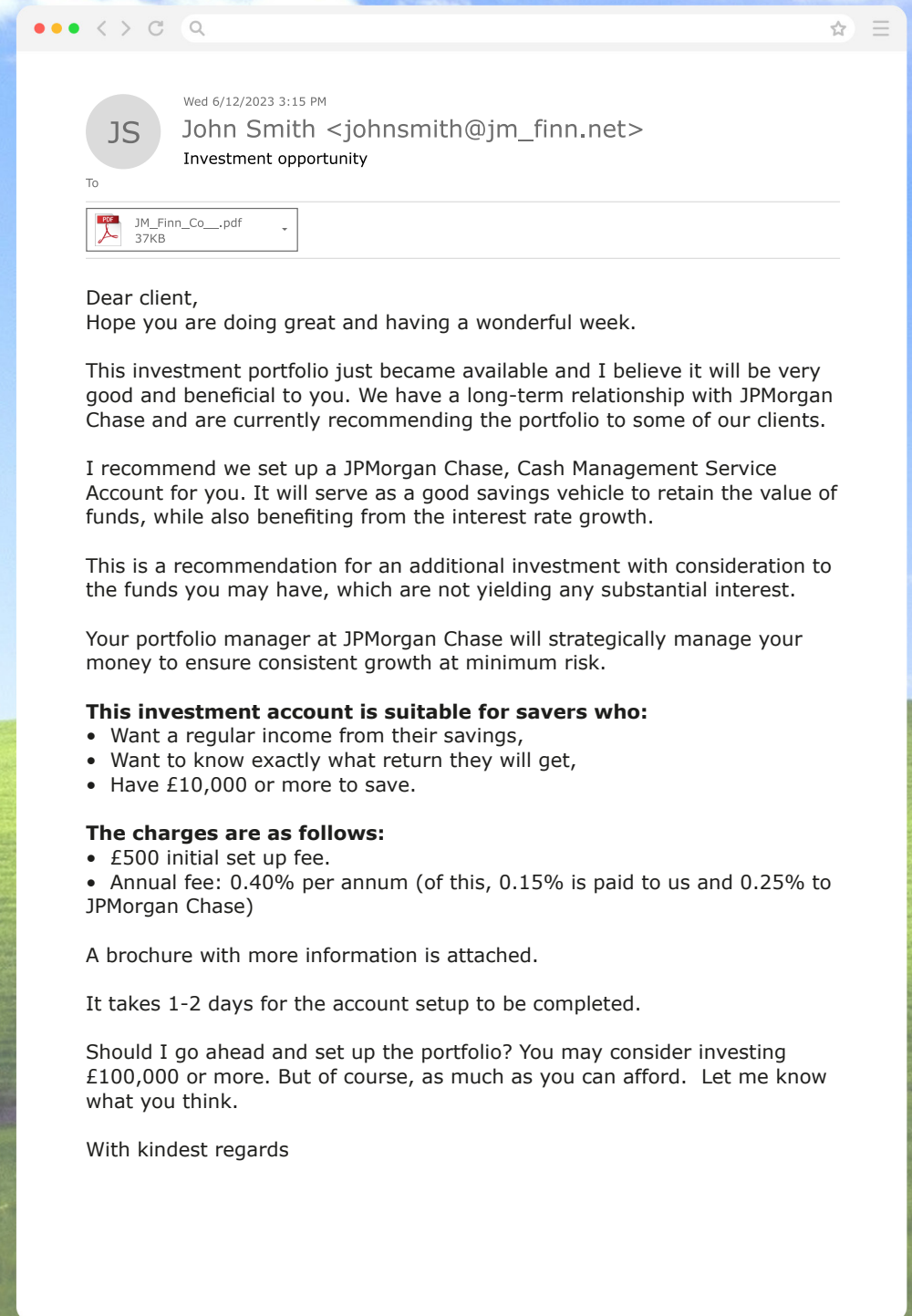
Case Study

While names have been changed, the email on the following page is a real email that was received by a JM Finn client from a scammer after having their email hacked.

You should be aware that if you are hacked, scammers can change details such as phone numbers, account details and email addresses within your emails, therefore it is important to check against those on the website or existing documentation you have that is kept outside of your email account.

 **This is a highly convincing email.**

In this case, the client avoided losing money by contacting their investment manager using the phone number on the JM Finn website to check whether the email was genuine.



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 becoming 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 to offer your devices an important extra layer of security.

Always back up your most important data 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. Even if an email looks like it has been sent from an organisation you know or trust, do your own independent research. Check the company's website 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 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 wording 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 by calling them on a number you have verified before opening links or downloading a file.

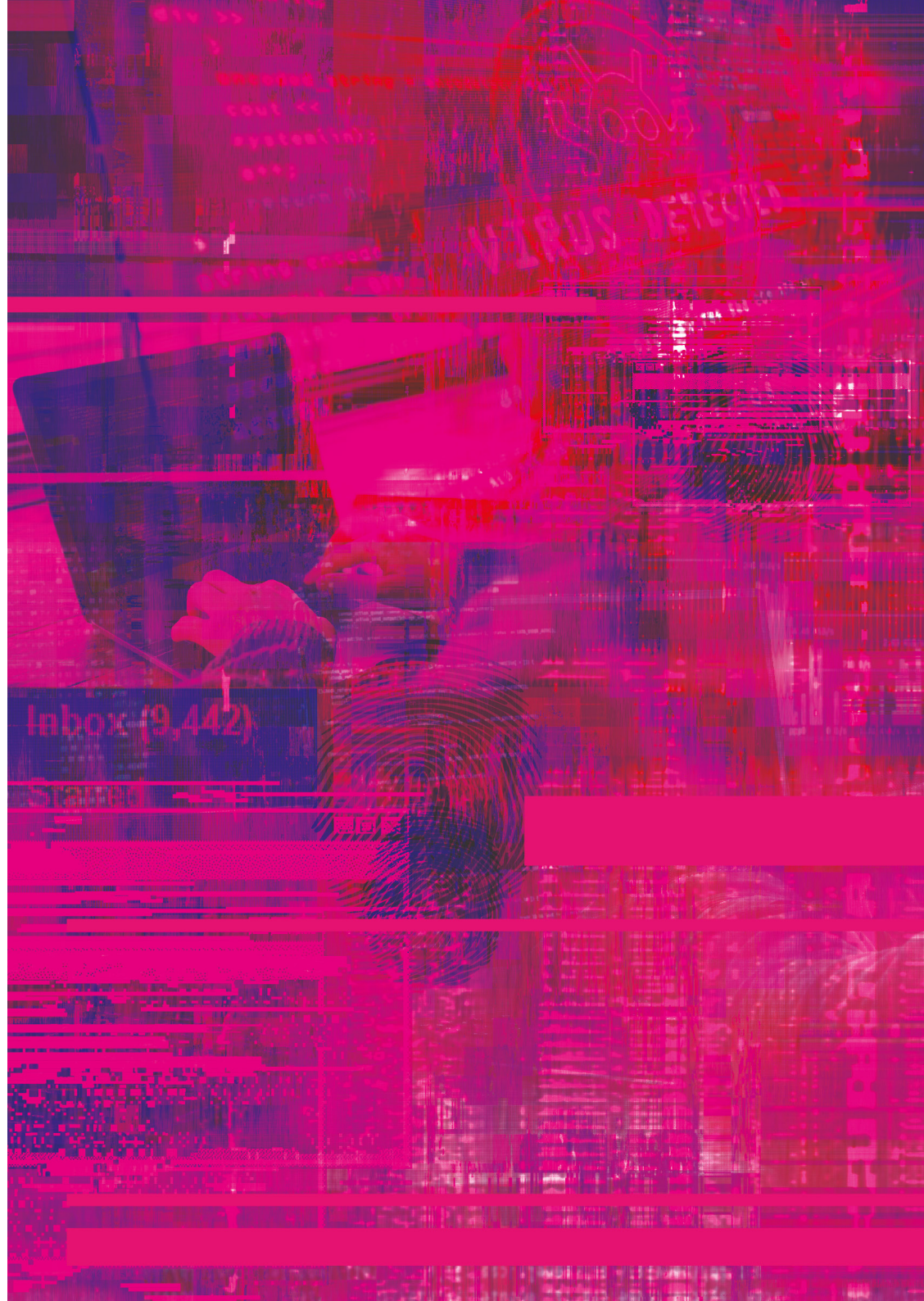
Never trust an unsolicited download.

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

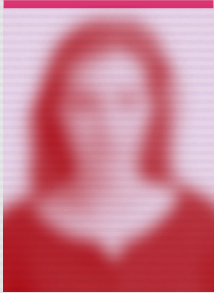
Sound too good to be true? If you receive an unsolicited email, or call from a lottery syndicate, inheritance from a distant or unknown relative, or maybe a request to transfer funds for a share of a bounty, it is almost certainly a scam.

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



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 boys' 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 I believed 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.



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.

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.

What does a 'strong password' actually mean?

Using a weak password can make you far more susceptible to having your email account hacked. While we may hear a lot about the importance of creating a "strong password", it is important to understand what a strong password actually is. The best passwords are those that are truly random in nature and cannot be guessed as they don't conform to any language in any dictionary or phrase. Below are some tips for best practice when creating a password:

A strong password should meet the following criteria:

- Be at least 12 characters long.
- Include a combination of uppercase and lowercase letters, numbers, and special characters.
- Avoid using common words or phrases.
- Avoid using personal information such as your name, birthdate, or address.

Use combinations of unrelated words into your password (or passphrase)

As a general rule the longer your password is and the more complex, the harder it is to crack by a hacker. Combining 3 or more random dictionary words is good

practice, as long as you include random numbers and special characters. This makes it much easier to create and remember whilst difficult for hackers to attack due to the sheer number of combinations of 3 random words.

Do not use dates within your password

Avoid using guessable dates, such as the birthday of a child, a pet or a memorable date in history such as 1066, 1966, 1767, 1666.

Do not use sequential numbers or letters within your password

Numbers such as 123456 or 78910 can easily be guessed by attackers or auto built into automated password cracking software.

Do not reuse your password across multiple online accounts

One of the reasons so many accounts are hacked is due to individuals using the same password across multiple accounts. It is highly likely one of your accounts will get compromised at some point in the future.

Use a password manager (vault)

As it can be difficult to remember numerous passwords, using an industry recognised password manager (or vault) across all your devices will significantly reduce the risk of your online accounts being compromised.

Never disclose your password to anyone

Absolutely never disclose your password to anyone. Remember banks, financial institutions or online businesses will never ask for your password. If they do it is highly likely that they are fraudsters, however convincing they sound.

How long does it take to crack a password?

The table on the right shows the length of time it will take hackers to crack passwords using modern 'brute force' techniques:

1. Shorter passwords:

Passwords with fewer than 10 characters can be cracked very quickly, often in minutes or even instantly, especially if they are not using a mix of different character types.

2. Character mix: The use of upper and lowercase letters, numbers and symbols significantly increases the time required to crack a password.

3. Longer passwords:

Passwords of 16 characters or more, using a full mix of character types, can take trillions to quadrillions of years to crack with current technology, making them extremely secure.

How long does it take a malicious cyber criminal to break your password?

Number of characters	Numbers only	Lowercase letters	Upper & lowercase letters	Numbers, upper & lowercase letters	Numbers, upper & lowercase letters, symbols
4	Instantly	Instantly	3 secs	6 secs	9 secs
5	Instantly	4 secs	2 mins	6 mins	10 mins
6	Instantly	2 mins	2 hours	6 hours	12 hours
7	4 secs	50 mins	4 days	2 weeks	1 month
8	37 secs	22 hours	8 months	3 years	7 years
9	6 mins	3 weeks	33 years	161 years	479 years
10	1 hour	2 years	1k years	9k years	33k years
11	10 hours	44 years	89k years	618k years	2m years
12	4 days	1k years	4m years	38m years	164 years
13	1 month	29k years	241m years	2bn years	11bn years
14	1 year	766k years	12bn years	147bn years	805bn years
15	12 years	19m years	652bn years	9tn years	56tn years
16	119 years	517m years	33tn years	566tn years	3qd years
17	1k years	13bn years	1qd years	35qd years	276qd years
18	11k years	350bn years	91qd years	2qn years	19qn years

Source: Hive Systems

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 believed 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.



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 take 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 a 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 check 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 on the Financial Services register that the companies with which you deal are authorised by the regulator – in JM Finn's case this is the Financial Conduct Authority (FCA).

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.



10:02:30

Alert

Error message ...



Critical Error

Reboot ...