

A young woman with curly hair and a man are looking at a laptop screen together. The woman is on the left, leaning in, and the man is on the right, looking at the screen. They appear to be in a home or office setting. The background is bright and slightly blurred.

THE FAMILY GUIDE TO

Staying Safe Online

Produced by
One Brightly Cyber

Published by One Brightly Cyber
© copyright 2023

We would like to acknowledge their thanks to the following sources:

National Cyber Security Centre (NCSC)
National Crime Agency
UK Office of National Statistics Digital Partners
Cifas AARP



CONTENTS

CHAPTER 1: INTRODUCTION	5
The Pace of Change	5
CHAPTER 2: THE 6 WAYS TO STAY SAFE	8
1. Password Security	8
2. Updating devices	11
3. Anti-malware protection software	12
4. Preventing Data Leakage.....	14
Using public WiFi networks	17
Beware Smart Devices.....	19
CHAPTER 3: IDENTITY THEFT	21
CHAPTER 4: RANSOMWARE	25
CHAPTER 5: FOUR TPES OF SCAM	27
Phishing	27
Spear Phishing	28
Smishing	28
Imposter Scams	29
CHAPTER 6: TOP SCAMS AND WHAT TO LOOK OUT FOR..	31
The Parcel Scam	31
Property Fraud	32
The Tax Fraud.....	33
The Fake Charity	33
Job Scams	34
Romance Fraud	34
Pensions And Investment Fraud	35
CHAPTER 7: A FINAL WORD	37
Our Recommendations	37

FORWARD

This guide originally started life as a training manual put together by our fraud investigators at One Brightly Cyber Inc., the cyber fraud resolution experts who have been successfully resolving data breach incidents for US consumers and well known corporates for over twenty years and who now have a presence in the UK through One Brightly Cyber Ltd.

Cyber fraud is now so much a part of everyday life that we felt this information should be made available to a wider readership and so we have updated and modified the content for our UK audience.

For more information about One Brightly Cyber and the protection and resolution services we provide, please see www.OneBrightlyCyber.com



CHAPTER 1

Introduction

Everyone is at risk

Over the years, our Fraud Advocates have helped many thousands of individuals who have been scammed and one thing we know for sure is that anyone can be a victim, no matter who you are or whatever your educational or professional attainment.

Young, poor, rich, successful...from seasoned business executives to medical professionals, police officers to academics, no one is immune and everybody is a potential victim.

Every day, we hear stories about individuals losing money to clever new tricks and scams and how banks and financial institutions often refuse to cover the losses because they consider the victim, not their systems, to be at fault.

But the situation does not have to be quite so alarming. Most frauds occur because individuals are simply unaware of some fairly simple and easy steps which they need to implement.





Here, we explain what these steps are. We will also outline how most scams work and what you should look out for; and finally, we'll explain what you should do if you, or someone you know, might have fallen for a scam.

Many people who have been scammed report feeling a deep sense of shame for having been so easily suckered and prefer to keep their experience secret for fear of ridicule, which can make the ordeal even harder to bear.

Scammers play on emotions and have a lot more success when targeting individuals who are going through big upheavals in their lives, such as a change in employment, separation, moving home, health

issues or the loss of a friend or family member.

Stressful life events can lower defences and make it much harder for the individual to spot a scam.



THE PACE OF CHANGE

For an idea of how far things have progressed, try guessing how many floppy disks it would take to install Windows 10. Quite a few, right? Maybe fifty? Even one hundred and fifty? More?

The answer is an incredible fourteen thousand. Yes, you read that right; fourteen thousand, one hundred and sixty seven floppy disks (each containing 1.44 megabytes of data) would be required to install Windows 10 (which contains around 20,400 megabytes of data).

Put another way, the most basic (32gb) smart phone

is over a million times more powerful than the Apollo 11 guidance computer used to land on the moon landing; and well over one thousand times more powerful than the Cray 1, the world's leading supercomputer launched in 1975 at a cost of \$7.9 million, equivalent to around \$34 million (£27 million) today.

Back in the nineteen eighties, the amount of data that could be transferred over the internet was usually around 1,100 'bits' of data per second (bps) and, in the home, you only dialled up a connection when required in order to minimise connection costs and keep the line open for voice calls.

Today, broadband speeds can easily exceed 100 megabits per second (mbps) which means that connection speeds are around one hundred thousand times faster and are set to become rapidly faster still.





These days, there are a great many cyber tools and services which promise to keep you safe and it can be very hard to decide what you really need and how to decide between them. We make some recommendations at the end of this guide which can be divided into ‘tools’ and ‘services’:

TOOLS

These are the tools we recommend for the best online protection:

- Anti-virus software (see page 24), particularly if you use Android (non-Apple) devices
- An App providing access to a virtual private network (VPN), if you frequently use the free public WIFI provided by cafes, restaurants etc.
- Dark-web scanning App: automatically scans the dark web (the part of the internet used by criminal gangs) for any of your personal information being offered for sale to criminal gangs (see page 39)
- Keylogging prevention software: this prevents a hacker installing software which sees exactly what you type, including passwords (see page 33).

SERVICES

- An Identity Theft Resolution Service: having your identity stolen can prove expensive, frustrating and extremely difficult to rectify. Having a trained fraud investigator working on your behalf to quickly put things right can provide considerable peace of mind
- Technical Support: if you don't already have someone who can readily help you with technical issues or questions – no matter how simple – then you should consider subscribing to a service which offers full technical support to assist you with whatever issue you face on any one of your devices or connected devices such as your TV, security cameras or console



Cyber Gangs Today

When most people picture a cybercriminal or hacker, they usually think of a hooded teenager holed up in some bedsit or barricaded in the bedroom of their family home.

But today's cybercriminals are increasingly a different breed altogether. They are often young, university-educated professionals who work from comfortable and well-appointed offices in organisations based mainly in Russia, former Soviet bloc countries like Ukraine, China and North Korea.

They typically work regular hours, have line managers, targets and even fringe benefits, like cars. Many of these 'companies' are franchises, or affiliates, of more significant gangs who sell ransomware data and proven scams to them.

In a ransomware attack, data is listed for sale on the dark web, which is the hidden part of the internet used by criminal gangs and is only accessible via a browser known as TOR; this stands for The Onion Ring and refers to the many layers of anonymity.

Gangs - with their branding - post their wares on bulletin boards and advertise their stolen data for sale,

illustrated with samples to prove they have what they claim ('the finger in the box'): copies of passports belonging to a company's employees; payroll details; medical records etc.

Rival gangs are invited to bid for the data and are often asked to leave customer reviews, rating the merchandise and quality of customer service.



Most companies who are victims of ransomware never let the authorities - or their customers - know since there is no UK legal requirement to do so. Incredibly, too, on average, a company takes 200 days even to notice a data breach has occurred and that their customer's details are being traded on the dark web (IBM)

As a result, should, say your local solicitor be a victim of ransomware - and all your confidential data be offered for sale as a result - then the first you'll know about it is when you are targeted in an attack.




Seven Ways To Stay Safe

1. IMPROVE YOUR PASSWORD SECURITY

THE PROBLEM

Managing passwords can feel like a real headache, especially when you're told that they should all be different and changed on a regular basis.

Many people find it impossible to follow this advice and instead stick to a choice of two or three passwords (possibly with some slight variations) for every situation where a password is required, including email, banking, shopping and entertainment.



This lack of variety makes it so much easier for a hacker to do their work.

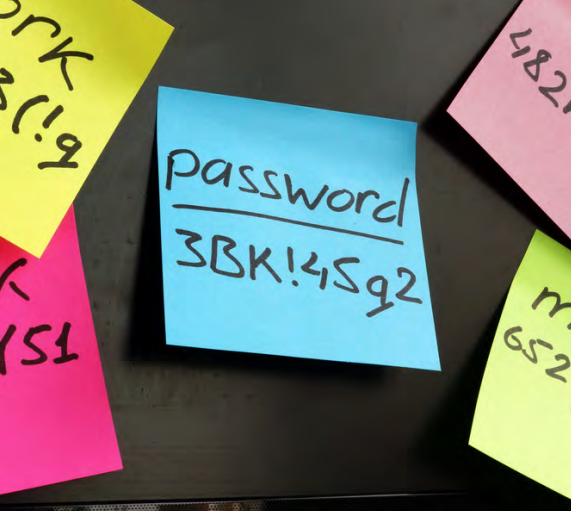
Suppose you signed up with some long-forgotten site several years ago, a site which (unbeknown to you) was subsequently hacked with all its customer data stolen.

Using that same password today, or something similar, is like leaving your front door wide open and inviting cyber criminals to wander in and rifle through all your details... your emails, shopping habits, medical records, finances...



Password





important to avoid words which make it any easier for the hacker to predict.

THE SOLUTION

1. Save Passwords In Your Browser

The first thing to realise is that your passwords do not have to be memorable.

But even if you use different passwords for different accounts, you are still potentially vulnerable since many passwords are easy to guess.

Take a look at the passwords below, listed below by the National Cyber Security Council (NCSC). Do they look like the kind of passwords you might use?

**arsenal22 1v7Upjw3nt
p@55w0rd
victoria! 20111977**

You might be surprised to learn that all five of them appear in the top 100,000 of compromised passwords.

Hackers have access to sophisticated software which quickly scans through tens of thousands of password possibilities to discover the one which works and so it is



Instead, let your browser (like Chrome, Safari or Edge) remember them for you; it is much better to have a strong password stored in your browser than a weak password which you find easy to recall.

You might also consider using a 'Password Manager' which can safely generate, store and automatically deploy passwords when you need them. Many companies providing these offer free versions, but you should be

aware that if your 'master password' should ever become compromised, then all your accounts and passwords will be revealed. This is why it is essential to ensure that your master password is as complex and secure as possible.

2. Use unique, complex passwords for different sites

Now that you realise your passwords do not have to be memorable, it is much easier to set strong passwords.

Sometimes a site will automatically generate a unique and complex suggestion and offer to save it too, which is a good option.

But when you need to come up with a password suggestion yourself, be careful: avoid anything containing

personal information, such as an anniversary date or name of a pet.



3. Use Three Random Words

One of the best ways to create a secure yet memorable password is to combine three random words,.

For example: **DogFenceGreen**

Avoid words that can be guessed, like your street name or the name of your pet.

Adding a number or symbol can make it even more robust, and many websites insist that you use a combination of characters anyway:

DogFenceGreen4\$



2. UPDATE YOUR DEVICES

THE PROBLEM

Cybercriminals constantly probe technology providers for chinks in their armour. When they think they might have found a weakness they can exploit, the technology provider will, in turn, quickly create and distribute a 'patch' as soon as they become aware of the threat.

THE SOLUTION

This is why it is vital to ensure that all your devices are continually updated and upload the latest updates as soon as they become available.

The easiest way to achieve this is to check your settings and ensure that "Automatic Updates" is selected; you

can also choose when this should occur (for example, overnight or only when connected to the internet to avoid paying mobile datacharges).



Some devices (and software) need to be updated manually. You may get reminders on your phone or computer, and you should not ignore these alerts because otherwise are leaving yourself to known vulnerabilities.

How to turn on automatic updates

- [Apple - Mac \(opens in a new tab\)](#)
- [Apple - iPhone and iPad \(opens in a new tab\)](#)
- Microsoft Windows 10 (opens your MS settings)
- Windows 7 is no longer supported. You should upgrade to Windows 10
- [Upgrading to Windows 11](#)
- [Android smartphones and tablets \(opens in a new tab\)](#)
- [Android apps \(opens in a new tab\)](#)



3. INSTALL AND UPDATE ANTI-VIRUS PROTECTION SOFTWARE



THE PROBLEM

Hackers and cyber criminals are continually trying to install malware on your devices so that they can either steal your data or hijack your device in return for a ransom payment.

Malware is usually installed because the owner of the device accidentally, or inadvertently, clicked upon a malicious link in an email message or visited a rogue website where the virus software was installed. Once it's on your computer or laptop, malware can steal your data, encrypt it so you can't access it, or even erase it altogether.



For this reason, it's important that you always use anti-virus software, and keep it up to date to protect your data and devices

Malware can take many forms and is usually designed to exploit a vulnerability in a program or operating system; this is why you should allow your devices to install regular updates since these contain fixes (or 'patches') for known weaknesses which have come to light. Sometimes the malicious software is known as 'spyware', which watches and records everything you type or speak.

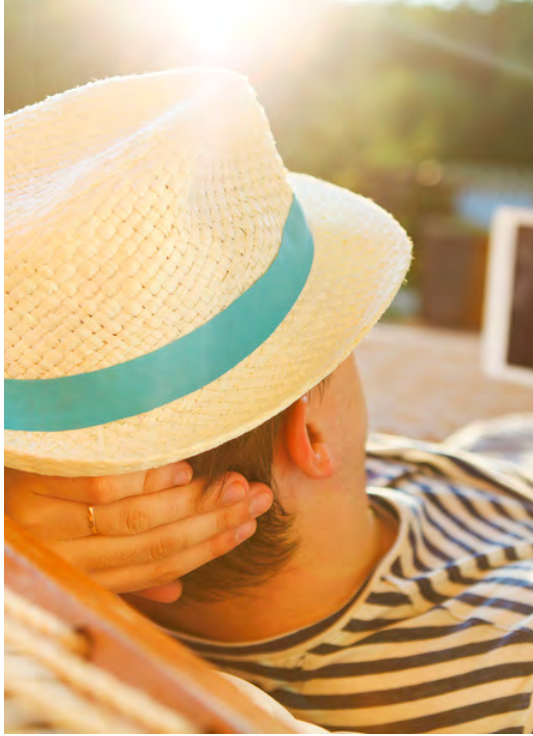


THE SOLUTION

Anti-virus software can neutralise many of these attacks, though it needs to be continually updated (in real time) to counter all the latest dangers and known threats.

Such protection is particularly critical if you use Android (non-Apple) devices since Apple's operating system (known as iOS) should keep you relatively safe, although threat levels are now so significant that even Apple devices can be compromised.

Often, new devices like tablets or laptops will come ready-installed with virus protection software (such as Norton or McAfee). Yet, after the initial free trial period (usually a year) expires, the onus is upon the user to renew.



Many people ignore the constant reminders and assume that their device continues to be protected, but this can often mean their protection software is stuck in the past and is not being continually updated to meet the continually evolving threats.

Keeping up-to-date is essential, and there are some free products, like Total AV or AVG.

For a list of free providers, visit the page [here](#).

Cyber crime
accounts for an estimated
50% of all UK crime
with a estimated
£130 billion stolen

UK Crime Agency &
Office of National Statistics



How Do Anti-virus Programs Work?

Anti-virus software is a program designed to detect and remove viruses and other kinds of malicious software from your computer or laptop.

Malicious software (or malware) is code that can harm your computers and laptops and their data. It can infect your device by inadvertently opening a malicious attachment linked to a dubious email, or hidden on a USB drive, or even by simply visiting a dodgy website.

Once it's on your computer or laptop, malware can steal your data, encrypt it so you can't access it, or even erase it. For this reason, it's important that you always use anti-virus software, and keep it up to date to protect your data and devices.

These products work by detecting, quarantining and/or deleting malicious code, to prevent malware from causing damage to your device.

Modern anti-virus products update themselves automatically to protect against the latest viruses and other types of malware.

However, as the sophistication of attacks increases, there is growing evidence that anti-virus products alone no longer offer sufficient protection, with some estimates suggesting that they can only prevent around 30% of attacks. It is therefore worth obtaining additional protection as well and two products are particularly recommended:

- Keylogger protection (this prevents criminals being able to see everything that is typed on a PC or mobile (see page 33))
- Dark Web monitoring (which alerts you to any suspicious activity concerning any company emails or domains; see page 28)



4. AVOID DATA LEAKAGE



THE PROBLEM

Data leakage refers to potentially compromising information disclosed from social media accounts. In most cases, the individual is totally unaware that they might have let slip some valuable suggest of information which can be used against them.



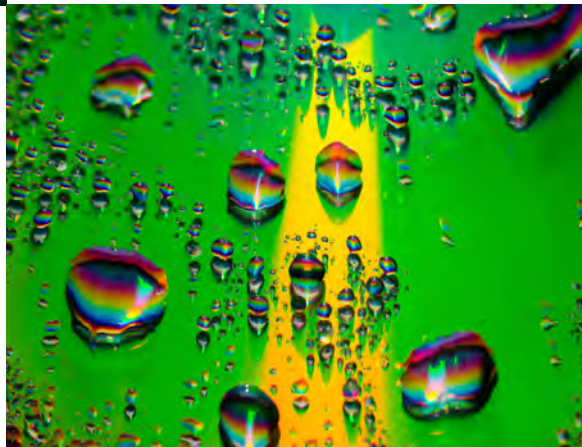
But you would be wrong.

Hackers use Artificial Intelligence (AI) programs to automatically scan posts for anything they consider interesting and then piece together the snippets to create a detailed profile.

This could include the names (and maiden names) of your family and friends, their birthdays, where you plan to holiday, items you have recently bought, car registration details, subscriptions, employment details, the name of your pet, your anniversary date, your home address, your hobbies, interests, your hopes and dreams.

You might think that most of what you post is all harmless.

Why would a hacker would be remotely interested in the fact that you have just got a puppy called Honey; or that you start a new job on Monday at a charity which you name?



That pet name? It might form part of your password, or memorable information when asking for a password prompt; or maybe they could send a fake email from a local vet offering free pet insurance for the first year: just click the attached document to find out more...

And that new job you mentioned? An increasingly popular scam is based upon information exactly like this, often obtained from looking through social media accounts such as LinkedIn.

Here's how it works: a new employee is emailed by, say, their Sales Director and asked to urgently purchase twenty £50 Amazon vouchers because they are needed to 'close a sale'.

The new employee is keen to impress and, realising the urgency of the situation and being unfamiliar with the company's procedures, they

decide to use their own credit card, certain that they will later be reimbursed. They then reply to the original email as instructed with the voucher codes.

Only it later turns out that it was a scam and that the request originated from a fraudster, not someone within the company.



And the company might also decide that the new employee was entirely at fault and refuse to reimburse them, even though they might have spent a couple of thousand pounds on their personal credit card.





Although many retailers place limits on the number of vouchers an individual is able to buy in one transaction, there are numerous stories of 'keen-to-impress' employees showing their initiative through circumnavigating such restrictions by, for example, using multiple tills at checkout.

THE SOLUTION

Always double check if contacted with any request to make any kind of financial transaction; call the person involved first before you do anything else. Be particularly suspicious if some form of time-pressure is being applied.

And if you can't get hold of the person purporting to be contacting you and you have to email them instead, begin a fresh email or text 'string' since replying to the original message could simply mean you are emailing the scammer back; asking whether they are for real is plainly not going to be of much help.

You should also be aware of an increasingly popular scam designed by fraudsters to extract as much valuable personal information from you as possible: the job scam (see page 34). This is where a fake online advert for a highly attractive position invites applicants to upload all their personal information, including CV, and often - to add insult to injury - pay a fake "admin processing" fee too.

”

UK Experiences

15 FOLD INCREASE

”

in online scams over the past year

The National Cyber Security Centre, June 2021



5. TAKE CARE WHEN USING PUBLIC WIFI NETWORKS



THE PROBLEM

Logging into the free WiFi provided by a hotel, café, bar, or airport might feel just the same as using your network at home or in the office, but there is a big and significant difference: your connection is not private.

There are several ways in which you can be compromised. The most common is the Man-in-the-Middle Attack, with the attacker positioned between you and the server you're trying to access, with you none the wiser.

Sometimes criminals establish fake WiFi hotspots which mimic the name of the restaurant, café or bar so that customers are tricked into using them. The criminals thus gain

complete access to your device and without you even being aware.

The attacker can then capture all of your traffic, which they can use to steal your personal information, swipe payment details, such as credit cards, and even install malware or spyware on your device.

The National Cyber Security Centre (part of HM government) has created an excellent video which illustrates the dangers. Take a look (*opens in a separate window*).



THE SOLUTION

There are two possibilities:

1. Create a Mobile Hotspot

A good way to protect yourself is to use your mobile device to create your very own Mobile Hotspot, a private network generated by your phone and which is password protected.



Unlike free WiFi, mobile data communications are encrypted and so no one will be able to access your device or the data you transmit.

You should, however, be aware that you may incur additional data charges, depending upon your mobile phone contract, particularly if using data-heavy applications such as live-streaming a video. (If you want access to films whilst out-and-about, consider downloading them from your home WiFi network first to avoid any possible mobile data charges).

2. Subscribe to a Virtual Private Network (VPN).

A VPN protects you by routing all your traffic through its own server, secured with end-to-end encryption, before it reaches your device.

This extra security means the attacker can't see any of your traffic, despite being connected to the same public WiFi hotspot. VPNs are widely available for sale, easy to download and install, and can be switched on and off as required.



6. BEWARE SMART DEVICES

In practice, this is really a password issue once again but, because so many people do not realise the potential dangers to which they are exposed, the subject deserves special consideration.



THE PROBLEM

These days, an increasing number of common household devices are described as 'smart', meaning they connect to the internet via your home network so that, for example, you can control or monitor them remotely. This is referred to as the Internet of Things (IoT).

And this is especially true of household devices where the factory-set passwords are rarely reset.

This means that a hacker can often easily gain access to, say, a baby-monitor and eavesdrop on conversations taking place within the home since they already know the default password.

Common examples include locks; security cameras; doorbells with built-in-cameras which allow you to see who's at your door; thermostats which you can re-set whilst away; and even fridges which allow you to see inside so you can check whether you are running low on eggs or milk.

It all sounds great, but such devices come with risks as well: the more devices you connect to your network, the more vulnerabilities you create.



THE SOLUTION

There is a concept in security called the 'attack surface'. This describes the sum of potentially vulnerable devices attached to a network, wirelessly or wired.

Regardless of actual security countermeasures in place, the more devices on your network, the greater the attack surface. I

f your security devices are up to

scratch and all of your connected devices are trustworthy, then you should be fine; but you really do need to be aware of what you're connecting and be sure that it's safe to do so.

This means changing the default password setting to something unique.

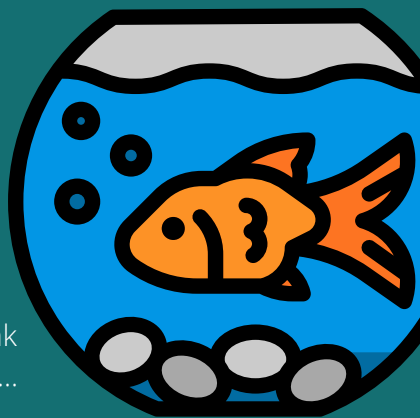
How a casino got hacked through its fish tank...

Here's a story which illustrates the threat posed by smart devices whose passwords have not been changed from the factory default setting:

In 2018, hackers discovered an unsecure fish tank thermostat which was connected to a wi-fi network... in a casino.

Because the password had not been reset from its original default, the hackers used this thermostat as an access point into the network, a tactic known as a 'pivot' and which is commonly used against wireless security cameras installed at home.

Once inside the network, they discovered and copied the casino's high-roller database, which they pulled right back out of the network through the thermostat.



7. TURN ON TWO FACTOR AUTHENTICATION



Two-factor authentication (2FA) helps prevent hackers from getting into your accounts, even if they have your password. This is done by getting you to provide extra information, such as a code that gets sent to your registered phone.

This means that a hacker is unable to access your account unless they can provide the code sent to your mobile phone.

How to turn on two-factor authentication:

For email

- [Gmail](#) (opens in a new tab)
- [Yahoo](#) (opens in a new tab)
- [Outlook](#) (opens in a new tab)
- [AOL](#) (opens in a new tab)

For social media

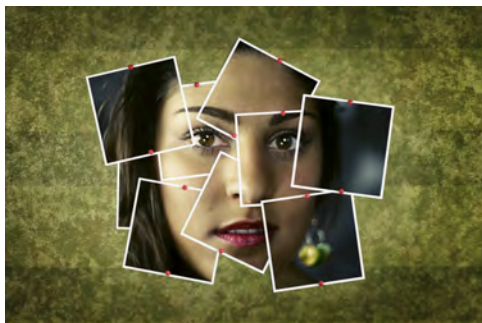
- [Instagram](#) (opens in a new tab)
- [Facebook](#) (opens in a new tab)
- [Twitter](#) (opens in a new tab)
- [LinkedIn](#) (opens in a new tab)



CHAPTER 3

Identity Theft

Identity Theft refers to the theft of your personal information - such as your name, date of birth, address and email - and using it without your consent. It can happen to anyone, and the effects can be far-reaching, expensive and difficult to put right.



Hackers routinely offer the data they have stolen for sale to criminals on the dark web. This data includes email addresses, passwords and bank details, often harvested from a major service provider who has been breached. Hackers also advertise complete Identities (known as 'fullz's) which they have compiled themselves through data leakage and which criminals can use to apply for credit cards, take out loans and even transfer property deeds.

THE PROBLEM

When a hacker steals information, they often list it for sale on the Dark Web.

This is the hidden collective of websites that is not visible to conventional web browsers and can only be accessed through a browser, most commonly known as Tor (which stands for The Onion Router because of the layers of encryption it uses). The Dark Web provides access to a vast secret cyber underworld where criminals openly sell drugs, weapons and stolen data.

To give you an idea of the size, you are only searching 0.03% of the web when you do a conventional internet search. The rest, all 99.97% of it, consists of the deep web (where confidential, non-public data is stored, such as payroll details) and the dark web.

Cyber crime

accounts for an estimated
50% of all UK crime
with a estimated
£130 billion stolen

UK Crime Agency &
Office of National Statistics



The more personal information, the higher the cost of the fullz but, on average each is worth around \$1,200 (£800) to the hacker since it can be sold several times to different gangs.

Criminals are even invited to leave their feedback on the quality of data and rate the overall service they have received (similar to Trustpilot).

Generally, older victims are preferred because they have good credit history and are less likely to have set up any alerts.

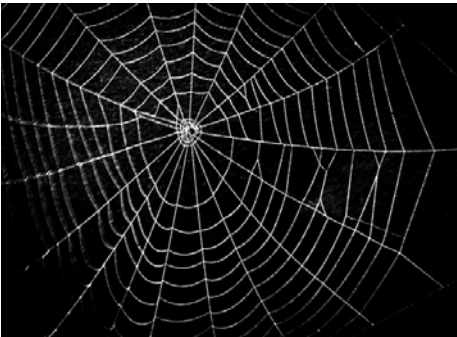
in the US, this means we now estimate that over 1 in 4 people aged 55 years or older are believed to have been victims of Identity Theft; figures are likely to be similar for the UK, though as yet they remain unverified.

Children, too, are popular because there is unlikely to be anyone monitoring their credit reports or identities:

Over just one year, we found that more than 1 million children in the US were victims of Identity Theft, costing an estimated \$540million in out-of-pocket expenses.

THE SOLUTION

In addition to the seven precautionary behaviours outlined earlier, there are several specific measure you can take to protect yourself from Identity Theft occurring and, should you fall victim, minimise the adverse effects.



Dark Web Facts

- 2 million active users connect to the Dark Web through the TOR browser every day
- Approximately one third of North Americans used the Dark Web in 2019
- About 60% of the information on the Dark Web could potentially harm organizations
- Dark Web use has increased by more than 300% in the last 3 years
- An estimated 2 to 5% of the global GDP is laundered on the Dark Web in one year
- 53% of organizations have had a data breach caused by third party information theft

Get Someone to Watch Your Back

Because your data may already be on the dark web, even if you haven't had a breach, you should consider subscribing to a dark web monitoring service which will alert you if your data is compromised before it is too late



More About The Dark Web

Bizarrely, Tor (the browser required to access the dark web) was originally developed by the US Naval Research Laboratory (pictured) to allow intelligence personnel to transfer information securely.

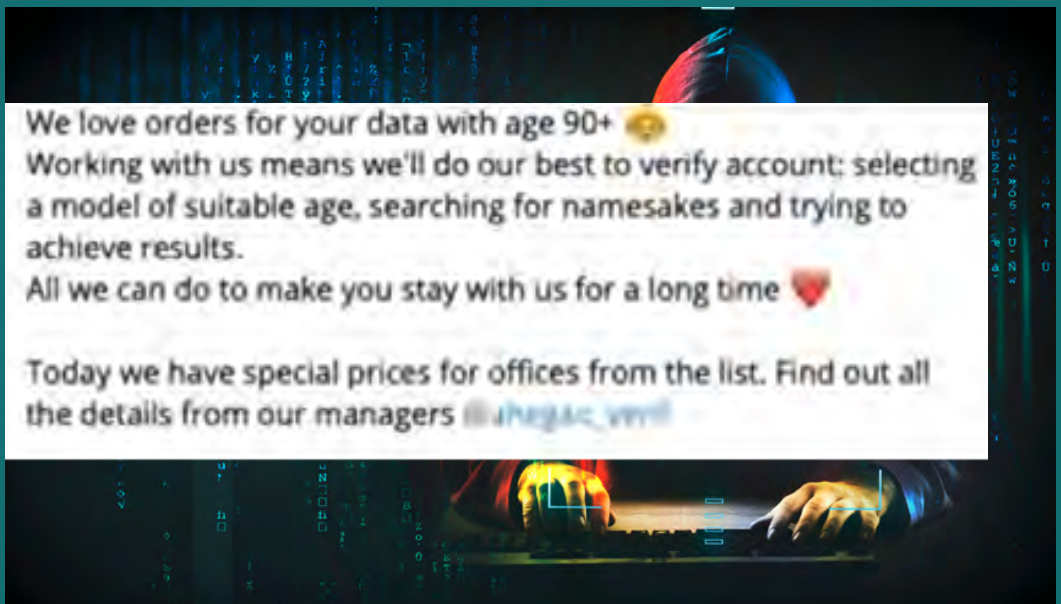


It was later released to the public where its use has been encouraged since the more people that use it, the easier it becomes to hide sensitive intelligence Communications; even to this day, Tor is still partly funded by the US government.

Although the information is often obtained through a data breach at an organisation with whom you have transacted, such as a subscription service, it can just as easily occur when an individual fails to take the necessary steps outlined earlier.

Tor therefore provides access to a vast secret cyber underworld where criminals openly sell drugs, weapons and stolen data.

Take particular care when using a public WiFi network or visiting an unsecured website.





People

AGED 61+

Are fast becoming

THE No. 1 TARGET

for

IDENTITY THIEVES

(because of their strong credit rating & poor security controls)

1. Subscribe to a powerful Dark Web Monitoring Service

A dark web monitoring service will alert you if any of your personal data is being listed for sale on the dark web. A good service will monitor at least two hundred sites and perform regular scans.

This means that you will be given advance warning of the issue as soon as it occurs, usually well before the cyber gangs have got around to targeting you, thus enabling you to change the compromised password concerned and avoid any trouble.

The App runs in the background and can cover all the emails belonging to yourself and your family

2. Keylogger

Another easily installed piece of powerful protection software that you can cheaply obtain is known as 'keystroke logger' or 'keylogger'. This prevents hackers (or employers) from installing software on your device which monitors every keyboard action you make, including your passwords.



Such spyware is becoming increasingly common and can be installed through clicking on a malicious link or visiting a compromised website. Some employees use it to monitor how active their employees are, especially when working remotely from home.

Keylogger prevention software is relatively inexpensive and, once installed, you won't even be aware of its presence since it won't slow your device or affect performance.

3. An Identity Theft Resolution Service

Sometimes, through no fault of your own, a determined hacker will manage to steal your identity and sell it to a criminal gang who will ruthlessly exploit it for maximum financial gain.

When your identity is stolen, reclaiming it can prove very costly, deeply frustrating and take a considerable amount of time and effort. The after-effects can last many months, even years, with unforeseen problems only coming to light when, for example, you apply for a loan or mortgage several years later.

IDENTITY FRAUD

rose over

40%

during lock-down

and now accounts for

50% of all UK fraud

Cifas

This is why you should consider subscribing to an Identity Theft Resolution service where highly trained Fraud Advocates are immediately on-hand to liaise with all the necessary parties on your behalf, including banks, credit card providers, lenders, credit rating agencies and government agencies such as HMRC, the Department for Work & Pensions, the Passport Office, DVLC, the NHS and the Police. Cybersure are pioneers in this field, with over twenty years experience (see www.cybersure.life).



Having my identity stolen cost me £10,000

"It just seemed to go on and on, it's just been really upsetting." Gemma Combellack, 30, is talking about her six month fight to reclaim her identity after it was stolen by criminals last year.

She discovered she'd become a victim of ID theft when she was refused a mortgage over a payday loan in her name that she knew nothing about.

A bank account had also been opened by fraudsters using her identity.

"I've been in tears at my desk at work in terms of the impact it's had on me and my stress levels.

"At the time it made me so angry, the fact that we were having to go through all this trauma and stress and no one could give me answer.

"It's just that it was so out of our control and that's the most frustrating thing about it."

Gemma's not alone. Last year ID theft happened more than 223,000 times, up 18% on the year before, <https://www.cifas.org.uk/>, the counter fraud organisation which runs the National Fraud Database and works with police and financial institutions to try to tackle fraud.

'Lucrative business'

Its chief executive, Mike Haley, says there are a number of factors fuelling that rise.

"Criminals are using more sophisticated methods, more of us are doing more things online and we're all using cash less which is something fraudsters are able to exploit.

"Criminals are targeting ID fraud as a lucrative business model and they're getting sophisticated in their use of social engineering [on the phone, text messages or on social media] which involves persuading people to give up personal information," Mr Haley said. Combined with large scale data breaches and data theft from companies and organisations, "and you have the raw ingredients [for ID theft]," he added.

Very often criminals carrying out these attacks on people in the UK aren't even based here. "This can all be done at a distance," he said. "Now you can sit behind a computer anywhere in the world and commit crime on a vast scale."

Also, there is very little risk of getting caught as "criminals are able to use the anonymity of the internet," he said.

Reported by the BBC in June 2020



THE PROBLEM

Sometimes criminals might use the data they have stolen to target you with a ransom demand. This usually means they have already infected your device with malware which threatens to delete all your files unless you pay the sum demanded, usually in the form of Bitcoin which is less traceable.

Probably the most recent famous example of this type of attack was that of Wanncry, which infected computers worldwide in 2017 by exploiting a weakness in Windows PCs.



Although the exact number of infections is unknown, it is believed to be well over 200,000 across 150 countries.

Victims were told that they would be unable to access their devices until they paid the ransom, initially set at \$300 in Bitcoin and later raised to \$600.

(Incidentally, setting up a Bitcoin account to pay a ransom is by no means easy and you should definitely allow this obstacle to deter you from deciding to cough up).



Should I pay a ransom to unlock my computer?

If your device has become infected with ransomware, we strongly recommend that you do not to pay the ransom.

If you do pay:

- There is no guarantee that you will get access to your data or computer
- Your computer will still be infected
- You will be paying criminal groups and supporting crime
- You're more likely to be targeted in the future

Far better to subscribe to a 24/7 Ransomware Resolution Service which will endeavour to resolve the situation without any money changing hands.

See [cybersure.life](https://www.cybersure.life) for further information

Should you decide to pay up (and we recommend you do not), there is no guarantee that the extortionist will honour their side of the bargain and remove the threat from your device (this was certainly the case with Wannacry where many people reported that they were still locked out of their computers even after the payment was made).

THE SOLUTION

To help prevent yourself experiencing this type of attack, you should follow the precautions already outlined in this guide and, in particular:



To help prevent yourself experiencing this type of attack, you should follow the precautions already outlined in this guide and, in particular:

1. Ensure you have installed up-to-date anti-virus software

For non-Apple (Android) users, this is your first line of defence; see page 14.

2. Back up all your data

The easiest way of doing this is to save your files on remote servers accessed via the internet and known collectively as Cloud Storage, or The Cloud.

Many tech providers (like Apple, Amazon, Microsoft, Google etc) offer a certain amount of storage space for free, with additional space provided for a premium.

Alternatively, you can copy your files on to a USB stick and perform regular updates (though be careful to remove the stick from your device since this too will be compromised if your device comes under attack).

3. Subscribe to a Keylogger service

Consider subscribing to a Key Logger service (see page x) which will prevent hackers installing spyware which copies everything your type or say. See page 23 for more details.

4. Subscribe to a Ransomware Resolution Service

Trained professionals will be immediately on hand 24/7 to help resolve the situation without any money changing hands. Because the same version of a ransomware is likely to have targeted large numbers of people worldwide, it is likely that they will already have come across the malware and understand the solution required



Four Types of Scam

1. PHISHING

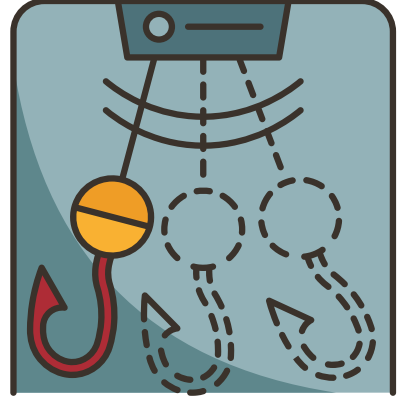
Cybercriminals will often send emails that pretend to be from someone else, and they can even mimic the email address, so they appear legitimate. This is known as 'phishing'.

The message will likely contain malicious software in an attachment that you are invited to open or via a link which you are asked to click.

This malware could prevent your device from operating unless you pay a ransom, or it might spy on your every movement so that passwords can be obtained; or it could simply bombard you with unwanted messages or adverts.

If you accidentally click an attachment or link, here's what you should do:

- Run a full scan and allow your anti-virus software to resolve any issues it finds
- If you've shared any passwords, change them immediately and make sure you also change them on any other accounts where the password is also used
- If you have shared any bank details, immediately contact your bank and let them know what has happened



**NEVER BELIEVE AN UNSOLICITED CALL FROM
SOMEONE CLAIMING TO BE FROM YOUR BANK,
CREDIT CARD PROVIDER OR LENDER**



2. SPEAR PHISHING

This is a more targeted type of attack where the criminal mimics an individual the target might know, like an IT manager at work or a friend or relative. They might also embroider the email with information they have obtained to make it seem more genuine, such as a restaurant recently visited. The intention, once again, is to persuade the target to open a malicious attachment or link so that you install malware.



This type of attack can be potentially ruinous, especially if it involves a hacker posing as an employee of a firm of solicitors during an important financial transaction, such as the sale of a house (see 'Property Fraud', page 40).



Deciding who is at fault can be contentious with the victim claiming the solicitors must have been hacked and the solicitors meanwhile maintaining that their systems were secure and that any breach must have originated with the victim and was because of their carelessness.

3. SMISHING

This is the SMS equivalent of phishing so that the message from the scammer is sent as a text. Again, the criminal will be able to mimic the telephone number of the sender they are imitating and even make the message appear as part of a string of real messages sent previously by the organisation they are pretending to represent.



4. IMPOSTER SCAMS

Cybercriminals will often call targets and pretend to be from their bank, credit card provider or service provider. The number they appear to be calling from might even mimic the organisation's genuine number.

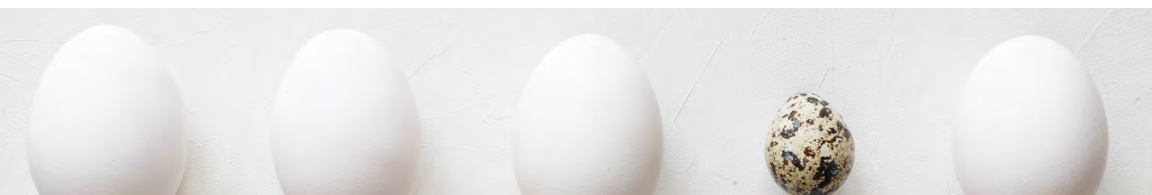
They can sound very plausible, and it is easy to be convinced that you really are speaking to who they pretend to be, especially when they might appear to know details of your recent transactions and basic account details.



But banks will never telephone you unprompted in this way, and so if you receive such a call, you should know it is a scam, hang up and report it.

Alternatively, you could ask for a reference number and tell the caller that you will phone them back on the number which appears on the back of your credit or debit card; if you do this, your bank will tell you that the call was not from them and that they never contact their customers by phone.

Sometimes the caller might even have engineered a situation previously which, should the target have fallen for it, is later revealed as a scam; and so, when the criminal later calls and explains that, for example, the £1.10 you just sent Royal Mail in response to their text message was really a scam, the victim might be grateful that their bank appears to be looking out for them and is primed to believe whatever they say.



The number of imposter scams is estimated to have doubled in the first year of the pandemic (or 'scamdemic' as many refer to it).



With more people shopping from home, the opportunities for scammers has grown; Scammers may communicate by text, email or WhatsApp, even attaching their messages to an existing thread to convince you that you are talking to the person they claim to be. The number of people falling for this type of scam is rising exponentially.

Other than bank or credit card scams, popular imposter scams include:

- A retailer such as Amazon, texting or calling about a product recently purchased; maybe they want to alert the purchaser to a 'fault' and offer a refund; or they claim there is excess to pay on a delivery
- A Tech Company claiming to have found a virus on your computer which they can fix for a fee; in the process they will gain access to your device and might even persuade you to take out a 'lifetime' insurance contract for several hundred pounds
- A close friend or relative claiming to need money urgently; perhaps they owe money to 'a dangerous loan shark' who is about to exact some punishment; or maybe they are about to be evicted from their home
- A competition announcing you have won some kind of prize, only you first have to pay an 'admin fee' for the prize to be released
- A work colleague requesting that you urgently purchase twenty £50 Amazon vouchers and send them the codes so that they can sweeten and close a deal



Treat any request for money with deep suspicion, particularly if there is some urgency attached to the request

Do not be fooled by the imposter appearing to know details which seem highly personal; these could easily have been picked up from social media accounts

And be suspicious of anyone claiming to be a close friend or relative who requests money via text messages; they might not be who they say

Always contact the person or company independently yourself, ideally by phone, to check that the request is really genuine



Top Scams To Look Out For

THE PARCEL SCAM

You receive a text message or email from a parcel delivery company like Royal Mail, DPD or Hermes; the message states that you need to pay a small excess payment – maybe just one or two pounds - in order for the parcel to be delivered. If you click on the link, you'll be taken to a site which looks real and which asks you to provide your contact and bank details.

Later, someone claiming to be from your bank calls and explains that they have detected fraudulent activity on your account linked, they believe, to a 'fake parcel delivery scam'.

Did you respond to such a message?

OK, you might think, I've been foolish; but then you feel relieved that your bank appears to have been so vigilant and that it is looking out for you.

The BANK 'spokesman' then explains that all the money in your account is at risk and that you urgently need to transfer it into a temporary 'safe' account until the danger has passed.

But if you do this, you will never see your money again since the whole thing is an elaborate scam.

Your bank would never contact you in this way.

And they would certainly never suggest that you transfer any cash into a new account.



PROPERTY FRAUD

When the Reverend Mike Hall was working away from his home in Luton, his neighbour happened to mention the building work which was taking place on his property. This came as a surprise as he hadn't asked for any work to be done.

Hurrying back home, he found his key no longer worked and the door was opened by a man he did not recognise.

Pushing him aside, he was astonished to find his house had been stripped bare...furniture, possessions, carpets, curtains, all gone.

It turned out that the new occupant of the house was equally shocked, having just paid a considerable sum for the property. What neither realised at the time was that a fraudster had stolen the Reverend Hall's identity and had sold the property without his knowledge, pocketing all the proceeds for himself.

Shocked, he contacted the police...and was even more shocked when they declined to take any action, claiming that it was a 'civil matter', not a 'criminal case, and that he should seek redress through his solicitor.

Subsequent investigations found a duplicate driving licence issued by DVLA in Hall's name, details of a bank account set up, also in his name, to receive the proceeds of the sale; and phone recordings of the house being 'stolen.'

The Law Society of England and Wales says property fraud usually involves the criminals pretending to be the victim's lawyer to trick them into diverting their payment to an account the crooks control, something known as 'conveyancing theft'. "These frauds can involve huge sums of money and have a devastating lifelong impact on the home buyer and their personal finances."

Friday Afternoon' fraud

'Conveyancing fraud' is also known as 'Friday afternoon fraud' since most property completions take place just before the weekend.



THE TAX SCAM

As the deadline for completing your tax return nears, you might notice messages purporting to be from HMRC which claim that you owe a sum of money and which you need to immediately pay in order to avoid further penalties or arrest. Or the message might claim that you are owed a tax refund and invite you to submit your bank details by completing the form, which appears when you click a link. This is almost certainly a scam; contact HMRC first before making any payment and only do so through the methods prescribed on their site.



THE FAKE CHARITY

Sometimes a scammer might pretend to be from a genuine charity and send a message asking for you to contribute to a worthy cause. They might even select a charity to which, from information gathered from your social media, they think you are most likely to donate; for example, they might pretend to be contacting you from the World Wildlife Fund (WWF) if you have expressed an interest in animal welfare.



Alternatively, the scammer might invent a totally new charity altogether, one that you have never heard about before. Either way, though, you should not use any bank details provided to make a payment.

If you do wish to make a donation, visit the charity's official website and use the details provided there. And if it is a charity that is new to you, make sure it is real by checking the charity register at the link you can find [here](#).



THE JOB SCAM

You should be aware that some criminals use fake job postings on well known sites to lure you into providing detailed personal information which they can then use to steal your identity.

Some of them additionally ask you to pay an 'admin fee', possibly followed by a 'processing fee' if you get that far. Naomi explains...

The following two cases were recorded by Cifas (names have been changed to protect anonymity):

#1: Fraudulent DBS check; Finchley Jackson, 52, London

"I signed up to receive new job notifications from Indeed and one day I received an alert for a job as a

Warehouse Operative for Renault Logistics. I filled out the application form which involved just a few questions.

"A few hours later I got a call asking if I wanted to take the job, even though I had only completed a short application. I thought it was a great opportunity so said yes, and next day received an email asking when I would be available for an induction.

"The company confirmed that I would need to do an induction the following Tuesday, and that I would need my National Insurance number, passport, birth certificate, have a CBS (DBS) check and provide a job reference. The company sent across a link to apply for the CBS, flagging that they would pay for the administration fees and I would only have to pay £19 for the check.

#2: Requests for money as part of a scam; Naomi

"When searching for a job online, I came across a role on an online job board. As part of my application, I provided my full name, date of birth and address.



"I also provided documents such as a scanned copy of my passport, proof of address, a National Insurance letter, and a DBS certificate.

"The company asked me for money as part of the job application, but when I refused, they stopped replying to my emails. When I attempted to call them on the phone number provided in the job advert, the number was invalid and I was unable to get in contact with anyone. The experience made me feel very anxious and panicked, and discouraged me from looking for further jobs online. I've been left worried that the fraudsters will use my details in illegal ways."

ROMANCE FRAUD

This type of fraud can be particularly upsetting since the victim can lose a considerable amount of their money as well as being left feeling embarrassed, betrayed and bereft. Romance scams involve people being tricked into sending money to scammers who go to great lengths to gain their trust and convince them that they are in a genuine relationship.

Scammers often borrow profiles from genuine individuals which they have lifted from genuine sites. You can check whether the images have been used elsewhere before by conducting a 'reverse image search', details [here](#).



The following signs may suggest that a friend or relative are involved in a romance scam:

- They may be very secretive about their relationship or provide excuses for why they are often online
- They may become angry or hostile if you ask them for information about the person with whom they are corresponding
- They are sending money to someone they have never met in person



I've been hacked – what should I do?

Whether it's your email, social media or some other type of online service, many things can alert you to the fact that someone else is accessing your account.



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 logins or attempted logins from unknown locations or at unusual times. Changes to your security settings and messages sent from your account that you don't recognise are also give-aways.

Update your device

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 anti-virus software. This isn't usually necessary for phones and tablets.

Contact your provider

If you can't 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. If you can't find what you need on the service's website, try a search engine like Google or Bing. For example, "facebook account hacked." Follow links to the service's own advice.

If your email account was hacked: once you've 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 should be found on your provider's help pages.

Change passwords

Once you have confirmed there are no unwanted email forwarding rules in place, change the passwords on all accounts with 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. (see section on passwords above). (see section on 2 factor authentication above).

Set up 2 factor authentication

This provides an extra layer of protection against your account being hacked in the future

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. You should contact the people you know regardless of whether you managed to restore your account or not.

If you can't recover your account

You may choose to create a new one. Once you've done this, it's 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.



PENSION & INVESTMENT SCAMS

Pension scams can be incredibly convincing and even the most sophisticated investors can be tricked.

Scammers can appear highly credible and knowledgeable, with seemingly impeccable references, testimonials, websites and promotional materials, all of which can make it almost impossible to distinguish it from the real thing.

They might even claim to be endorsed by well known personalities or celebrities, even though no such endorsement has been given.

Sometimes the promised returns look too good to be true (because they are), but other times they appear reasonably modest in order to make the scam look even more convincing.



How the scams work

Scammers usually contact people out of the blue via phone, email or text, or through online adverts on web browsers like Google or Bing.

Alternatively, you might be introduced by an unwitting friend or relative who is unaware they too are being scammed.

Sometimes scammers glean information from social media accounts (see 'Data Leakage, page 14) and might infer you have been recommended as an astute investor by someone at your golf/ tennis/ social club, whilst maintaining that professional confidentiality prohibits them from naming exactly who.

Often, their promotional material and website will claim they are authorised by the FCA, or they might instead claim that they are not required to have such authorisation because they are providing the advice themselves.

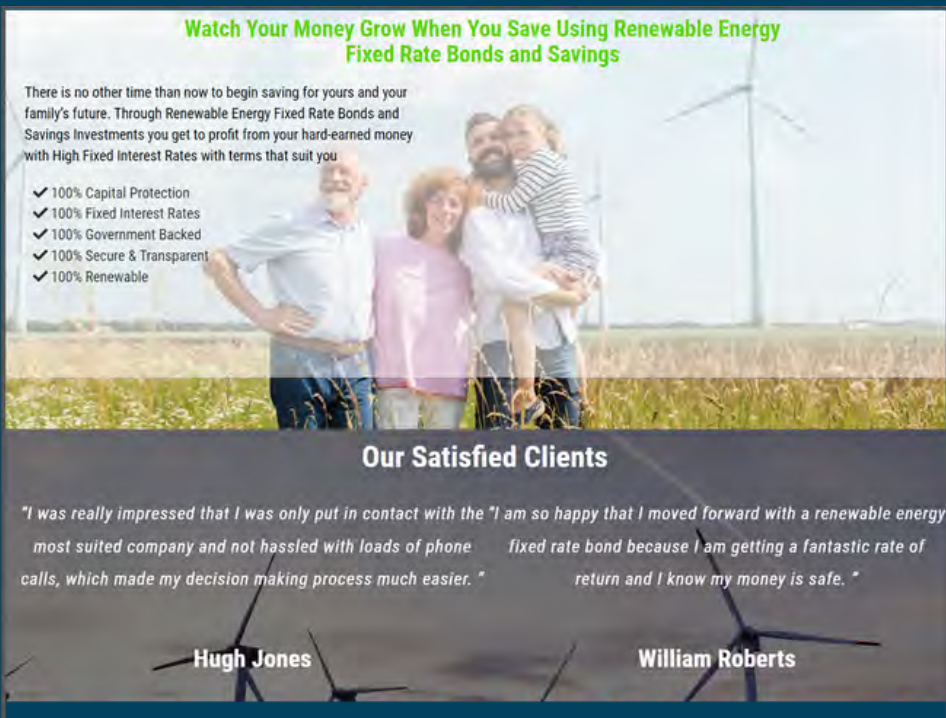
Their intention is always to persuade you to transfer your pension pot to them, or at the very least, to release some of its funds, something you are now allowed to do from the age of fifty five.

The large sums of money involved make this a very lucrative market for the scammers, which is why they are prepared to go to such lengths to appear so convincing.



The following areas have been identified as those most popular with pension and investment scammers:

- Unusual and high-risk investments like crypto currencies, overseas property, forestry, renewable energy bonds and storage units. Investments like this tend to be unregulated and illiquid, meaning it might be hard to get your money back (assuming, that is, that any of your money was invested at all)
- More conventional products but within an unnecessarily complex structure which hides multiple fees (often to overseas parties) and high charges; sometimes the investment might be presented as a long-term opportunity, meaning it might be several years before you realise something is wrong
- Scams where your money is simply stolen outright



Watch Your Money Grow When You Save Using Renewable Energy Fixed Rate Bonds and Savings

There is no other time than now to begin saving for yours and your family's future. Through Renewable Energy Fixed Rate Bonds and Savings Investments you get to profit from your hard-earned money with High Fixed Interest Rates with terms that suit you

- ✓ 100% Capital Protection
- ✓ 100% Fixed Interest Rates
- ✓ 100% Government Backed
- ✓ 100% Secure & Transparent
- ✓ 100% Renewable

Our Satisfied Clients

"I was really impressed that I was only put in contact with the most suited company and not hassled with loads of phone calls, which made my decision making process much easier."

"I am so happy that I moved forward with a renewable energy fixed rate bond because I am getting a fantastic rate of return and I know my money is safe."

Hugh Jones **William Roberts**

An example of a company highlighted by the UK Financial Conduct Authority (FCA) as offering investment opportunities in the UK without authorisation to do so

Frequently, the scam begins with an offer to conduct a 'free' pensions review to check whether your pension is performing adequately. Proper professional advice is never free and so you should immediately smell a rat and ignore their invitation, without disclosing any details about yourself or your circumstances.



Another popular technique is for the scammers to offer to help you release money from your pension, even though you are under the age of fifty five; this is not authorised and is a definite sign of a scam.

Three simple ways to protect yourself from pension scams

1 Reject unexpected offers

If you're contacted out-of-the-blue about an investment or pension opportunity, it's highly likely to be a scam and you should simply hang up or ignore the text. Contacting you uninvited in this way is illegal and you should never engage, even if they say a friend or relative referred them

2 Check who you're dealing with

Make sure the firm you are dealing with is not a clone; scammers often pretend to be a genuine FCA-authorized firm by mimicking their website and name

3 Do not be rushed

Do not allow yourself to feel pressurised into making a quick decision, even if it means risking losing out on an "amazing" opportunity.



A Final Word

We hope you have found the information in this guide useful and informative and that it will help keep you and your family safe from online scams and fraud.

The volume of fraud is expanding exponentially, and so there will always be new and ever more sophisticated scams since it is a highly profitable business.

Whilst this means that you need to be constantly vigilant and alert to the many dangers, it certainly doesn't mean you need to compromise your cyber life or restrict your online activities.

What we recommend

As well as the measures outlined in the initial chapters here, we strongly recommend you subscribe to the following tools:

- Anti-virus software
- A VPN (Virtual Private Network) if you use public WiFi
- Automatic dark-web monitoring to alert you as soon as your details appear for sale on the dark web
- A Technical Support Service which can assist you with any issues you face. These might include optimising device settings, ensuring they receive recommended software updates, installing anti-virus software and checking for malware. In addition, such a service might also be able to general advice and tips, such as how to use an app like Zoom or Skype or how to manage or synchronise cloud storage



In addition, we recommend that you consider subscribing to an **Identity Theft Resolution service** which can help restore your identity and repair the damage should you be a victim.

Getting your identity back can be a long and frustrating task and it is very useful to have a trained fraud investigator work on your behalf to liaise with all the relevant parties – including banks, lenders, credit card

providers, HMRC, Department of Work and Pensions, DVLA, credit rating agencies, insurance providers, The Passport Office and any affected suppliers.

These tools and services are relatively inexpensive – particularly when compared to the potential damage and losses they can prevent – and should be viewed in the same way as household insurance: essential if you have anything worth protecting and for peace of mind.



GLOSSARY

3G/ 4G/ 5G

The way in which your mobile phone receives mobile data (without being connected to your home internet connection). 'G' stands for 'generation' and each new generation provides progressively faster connection and data speeds. '3G' was launched in the UK in 2003 and something which might have taken an hour to download back then could now be downloaded on '5G' in less than twenty seconds

A

Anti-Malware Software

Software which is designed to find and neutralise malicious malware which could cause harm or damage; also known as anti- Virus Software ([learn more](#))

Anti-Virus Software

See Anti Malware Software above

Apple

A brand of phone, computer or tablet, known as iphones or ipads and using the iOS operating system; if your device is not made by Apple, it will be an 'Android; device (see above)

Authentication

Confirming the identify of a person trying to connect to a computer system or site



B

Back Door	An unofficial method by which a system or application can be accessed. Hackers may try to identify and use back doors to side-step formal security measures
Bandwidth	The amount of data which can be transferred through your internet connection; a 'low bandwidth' means you will struggle to watch TV or movies via a streaming service such as Netflix or BBC iplayer
Backup	A safely stored copy of all or part of the data held on a device (or system) which can be used should the original data be lost or compromised (<i>learn more</i>)
Biometric	A characteristic of your body which can be used to identify you; for example, your fingerprint or irises
Brute Force Attack	A method used by hackers to identify passwords; the hackers use a program which tries as many attempts as possible, advised by any extra supporting information they might have found (see Data Leakage)
Bits per second (bps)	A measure of data delivery speed via the internet. 'Bit' is short for 'Binary Digit' and is the smallest unit of data on a computer. Back in the 1980's, an internet speed of 1,100 Bps was common but these days speed is measured in megabits per second (mbps), with one megabit equivalent to 1 million bits. Not to be confused with 'bytes' which commonly refers to a group of 8 'bits' working together
Bluetooth	A type of wireless technology which allows one device to connect to another, so long as it is within range (usually no more than several meters)
Broadband	A generic term for access to the internet and which, in the home, requires subscribing to a broadband service provider such as BT or Virgin
Browser	The program which allows enables you to view the internet, such as Google Chrome, Safari or Microsoft Edge. Browsers have a search facility so that you can search for sites

C

Cloud	Refers to how your data is uploaded to and stored on remote servers. This means your data can be recovered should your device fail or go missing and also relieves the pressure on your device's memory because it does not need to store all your emails, photos, music and films (learn more).
Cookie	A token embedded into web pages which allows the site's owner to track your progress, remember who you're logged in as and (if you give permission) allow advertisers to target you with profiled adverts

D

Dark Web	The portion of the internet which is only accessible via a specialised browser such as TOR (see below) and cannot be accessed by browsers such as Google, Microsoft Edge or Chrome. The dark web is unregulated and is used by criminals to promote illegal activities (learn more).
Dark Web Monitoring	An App or subscription service (such as DynaRisk) which automatically alerts the individual (or company) should any of their confidential data be offered for sale to criminals on the dark web (learn more)
Data Leakage	Information which you might inadvertently disclose via social media but which hackers can use against you (for example, your date of birth, address, maiden name). Hackers use such information to create a 'fullz', see below (learn more)
Data Allowance	The amount of data you are allowed to download on your mobile device before incurring additional charges. Your allowance is specified by the mobile phone contract to which you have agreed, with higher allowances costing more. If you are unclear about how much data you require, your mobile provider will be able to analyse your past usage and recommend a plan based upon this. Some contracts specify unlimited data usage (see 'Bytes/ Megabytes/ Gigabytes' for more information)
Denial of Service	An attack which bombards a system with connections to keep it so busy that it is unable to accept legitimate connections. Similar to Distributed Denial of Service, below
Distributed Denial of Service (DDoS)	A security attack where the attacker employs an army of third-party devices (such as devices owned by hacked individuals) around the world to launch simultaneous attacks against a single organisation to overwhelm their systems (learn more)

E

eLearning

Education or training delivered remotely over the internet rather than in person; links to videos and information resources can enhance the capabilities

F

Firewall

Where traffic is filtered between networks to ensure that only the desired connections can happen

Firmware

The low-level software in a computer or network device that drives the core operation

Fullz

A full set of personal information compiled by a hacker and which is then offered for sale to criminals so that they can impersonate the individual or steal their identity ([learn more](#)).

H

Hacker

An individual who attempts to break into computer systems

Hyperlink

See 'Link', below



I

Identity Theft	Where a cyber criminal hijacks an individual's identity in order to directly benefit from credit card applications, loans and spending (learn more)
Identity Theft Resolution Service	A subscription service which provides access to a trained fraud investigator should an incidence of identity theft occur; the fraud investigator will contact all necessary parties (banks, lenders, government agencies, etc.) to successfully resolve the situation (learn more)
Imposter Scam	Where a criminal impersonates a bank, credit card provider or service provider in order to trick an individual into disclosing confidential information or transferring money (learn more)
Internet of Things (IoT)	Everyday household devices such as doorbells, light switches, cameras, thermostats and baby monitors which are connected to the internet. Because individuals rarely change the factory-set passwords, they can easily be hacked (particularly dangerous if the device contains a camera or microphone). Hackers might recruit an army of such devices worldwide to launch a Distributed Denial of Service (DDoS) attack, see above (learn more)
Internet Protocol (IP)	A set of standards used to identify and route data on the internet
iOS	This refers to the operating system used by any device made by Apple (such as iphones, ipads etc)

K

Key Logger	Malware which monitors what a user types on a keyboard and which then sends this information to the hacker (learn more)
------------	---



L

Link

A link (or 'hyperlink') is a shortcut to an internet page and is useful when you wish to direct someone to a particular site. To send a link, copy the browser address (when highlighted, press the 'ctrl' key and 'c' key simultaneously) and then paste into your email or message (to paste, press the 'ctrl' key and 'v' key at the same time). You can also embed a link into text or a picture by highlighting the word or photo required and selecting 'insert', then 'link' and then pasting the link into the space provided

Local Area Network (LAN)

A group of connected computers and devices which are all located together in the same place

M

Malware

A piece of damaging software that causes a security problem ([learn more](#)).

Man-in-the-middle (MitM) Attack

Where a hacker positions themselves (via a piece of malware or hardware) between a user and an application so that they can eavesdrop or impersonate one of the parties; this type of attack is made particularly easy when an individual uses a public WiFi network (see below) ([learn more](#)).

Mobile data

Mobile data enables your phone to get online without connecting to your WiFi. Most mobile phone contracts specify the amount of mobile data you are allowed to use each month before incurring extra charges. This is usually expressed in megabytes (Mb) and Gigabytes (Gb). Using mobile data to stream or download movies can consume a considerable amount of an allowance and so you should consider connecting your phone to your WiFi when doing this. (See 'Bytes/ megabytes / Gigabytes' above for an example of common usage)

Mobile hotspot

This is when you use your mobile phone to create your own secure WiFi network, enabling you to connect your tablet or computer to the internet in a secure manner. This is a safer alternative to using public WiFi which is not secure and where your data and personal information can be copied or compromised. Having turned on your phone's mobile hotspot function (via 'settings') you will see your phone listed on your computer or tablet as an available network; once selected, simply enter the password shown on your phone. Be aware, however, that you are now eating into your 'Data Allowance' ([see above](#))

N

NCSC	The National Cyber Security Council, the UK government-funded agency responsible for combatting cyber crime
------	---

P

Patch	An update for an operating system or software application, to correct a functional problem or security vulnerability (learn more).
-------	--

Personal Firewall	Security software installed on an individual's computer
-------------------	---

Phishing	Where a hacker pretends to be someone else and sends fake emails to trick an individual into doing something they shouldn't (like sending money) (learn more).
----------	--

Pop-ups	Pop-ups are new small windows which open on your computer and which obscure the page you were previously viewing. Often used for alerts or by advertisers, you can normally close the pop-up by clicking on the 'x' symbol normally located at its top left or right
---------	--

Portal	A web site
--------	------------

Public Domain Software	Software where the source code is released to the public free-of-charge so that anyone can use it
------------------------	---

Public WiFi Networks	Free-to-use WiFi which can be found in popular venues such as cafes, shopping centres, restaurants, airports and bars. Because the network is not secure, hackers can easily intercept communications (see man-in-the-middle attacks above) as well as infect devices with malware. Subscribing to a VPN (see below) can prevent this (learn more).
----------------------	---

R

Ransomware	Where a hacker uses malware to compromise or prevent access to a computer or system and demands a payment to prevent files being deleted or compromised (learn more).
------------	---

S

Skype	A type of video-calling software which you can install on your phone, tablet or computer. A paid version makes it possible to call mobile phones abroad at considerably less cost than would normally be the case
Smishing	Similar to Phishing but using SMS text messages instead of email (learn more)
SMS	Short Messaging Service, also known as text messaging
Spam	Unsolicited bulk messages usually sent by email. Spam filters can help weed out the most obvious examples
Spear Phishing	Similar to Phishing (where a hacker impersonates someone else) but using a more targeted approach by pretending to be a someone actually known to the individual, such as a work colleague, relation or friend (learn more)
Spoofing	Faking the identity or address of a message in order to hide the attacker's real identity
Spyware	Malware inserted into a device or system without the owner's knowledge and which transmits confidential information, including passwords and messages, to a third party



T

Tabs	Tabs are like pages on your internet browser; you can open a new page or tab by clicking the '+' symbol so that you can view or search for a new site without closing the site you are currently viewing
Tablet	A cross between a mobile phone and a computer; the large screen makes it easier to browse the internet than via a phone
Technical Support	A subscription service which provides expert technical assistance should an individual need help. Issues might include security, device performance, synchronisation of calendars or accounts or general advice on Apps and programs. Some providers only cover individual devices whereas others cover all devices used within the family household, including any connected devices such as TVs and consoles (learn more)
Tor	The Onion Router: one of the most popular browsers used to access the dark web (learn more).
Trojan Horse	A malicious program hidden inside what appears to be something innocent
Two Factor Authentication (2FA)	A way to improve security by making the user identify themselves by two methods instead of one; often this involves quoting the code sent via a text message to the user's registered mobile phone (learn more).

U

URL	A website address (the term actually stands for 'Uniform Resource Locator' but no one ever calls it that anymore)
-----	---

V

Virtual Private Network (VPN)	An application which uses encryption to turn a public WiFi network (see above) into a secure private network (learn more)
Virus	A common alternative term for Malware

W

Worm

A piece of malware which spreads to other connected devices by exploiting vulnerabilities and sending copies of itself

Z

Zero Day Attack

An attack which takes place when hackers exploit a flaw before developers have a chance to address it; sometimes written as 0-day

Zoom

A type of video-calling software which you can use from your smart phone, tablet or computer; you can easily switch the camera off if you prefer and the free version means you pay nothing to make calls, even to other countries around the world



Written, designed and published by
One Brightly Cyber Inc.
© Copyright 2023

For further information, see OneBrightlyCyber.com