THE LITTLE BOOK OF CRYPTO CRIME

Police Service of Northern Ireland

STOP! THINK FRAUD
NATIONAL CAMPAIGN AGAINST FRAUD

THE LITTLE BOOK OF CRYPTO CRIME

On behalf of The Police Service of Northern Ireland (PSNI), I am pleased to bring you 'The Little Book of Crypto Crime', reproduced by kind permission of The Metropolitan Police Service's Crypto Unit.

In recent years, the PSNI, like counterparts across the UK, has seen a rise in crime reports involving crypto assets such as the online theft of cryptocurrency, the use of compromised social media accounts to promote crypto-investment scams or blackmail demands in crypto payments to prevent the release of data.

There are simple security measures you can implement to avoid becoming a victim of crime online, such as adding multi-factor authentication to accounts, and creating strong passwords.

Services, such as Cyber Aware (**cyberaware.gov.uk**) from the National Cyber Security Centre offer a quick and easy-to-follow guide to address issues such as weak passwords, which criminals can all too easily exploit.

This booklet covers a wide variety of crypto asset-related fraud and cybercrimes used to target people and businesses across Northern Ireland, and supports advice available online at **psni.police.uk**

I hope you find this booklet beneficial, and it encourages you to change some of your behaviours online to keep you, your family and your money safe from criminals.

Emma Neill

T/Detective Chief Superintendent

CONTENTS

INTRODUCTION

Police Service of Northern Ireland are supporting the UK Government's National Campaign Against Fraud.

STOP! THINK FRAUD
NATIONAL CAMPAIGN AGAINST FRAUD

Stop! Think Fraud is a new national campaign against fraud and has been developed by the Home Office, National Crime Agency (NCA), National Cyber Security Centre (NCSC) and in consultation with a wide range of other partners and external stakeholders.

It supports the delivery of the Fraud Strategy with a multi-channelled campaign aiming to increase the likelihood that people will take action and adopt behaviours that will prevent them falling victim to fraud.

Fraudsters aren't fussy. They'll pick on anyone.

Nobody is immune from fraud. The criminals behind it target people online and in their homes, often emotionally manipulating their victims before they steal money or personal data.

But there is something we can do. By staying vigilant and always taking a moment to stop, think and check whenever we're approached, we can help to protect ourselves and each other from fraud.

Find out more at **gov.uk/stopthinkfraud**

THE LANGUAGE OF FRAUD

Criminals committing fraud will try to create an emotional response in us through invoking anger, fear, concern, fear of missing out (FOMO), shame, love, helpfulness or curiosity; posing as people we trust, reputable businesses, potential love-interests, experts and charities to get us to act quickly. They add time pressure to make us react to the emotional response instead of stopping to think.

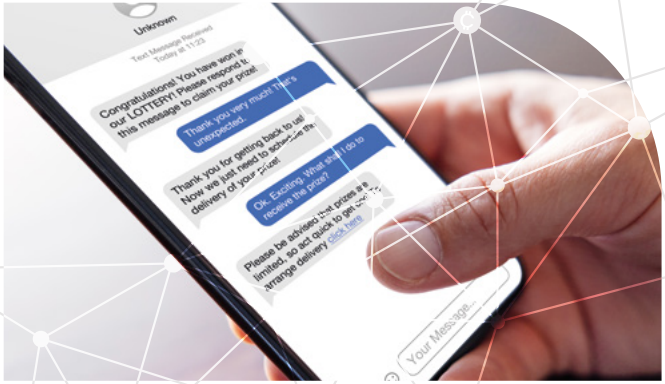
Academic research has found that there are four common linguistic strategies which criminals use to target people, namely;

- Requesting confidentiality or secrecy.
- Appealing for urgency, either explicitly or indirectly.
- Attempting to establish credibility.
- Referencing or implying trust.

Criminals are incredibly persuasive and use techniques to make us feel at ease and disguise any cause for concern. The language used is skilfully designed to abuse vulnerabilities, undermine people's confidence and manipulate decision-making in a similar way to domestic abuse and psychological grooming. It will make requests seem reasonable and expected instead of a cause for concern. Criminals can seek out and isolate individuals, who may not even realise that they are being targeted.

Anyone can be the victim of fraud.

Stop, challenge and protect yourself from crime online.



SOCIAL ENGINEERING

Social engineering is the practice of using deception to manipulate our human psychology into performing actions or divulging sensitive information. Social engineering attacks, where trust is abused to gain information, can happen both online and offline. Some attacks, such as phishing, target large groups of people but others target individuals. In some instances, criminals utilise data leaks and hacks to find out personal information about us, including our historically used usernames or passwords to help build our trust.

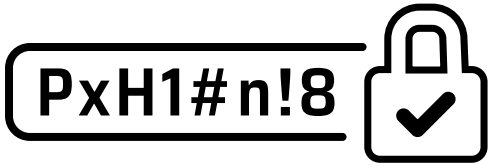
Consider the information you post about yourself online; information you wouldn't tell people on the street. A lot of the information we publish online is **personal identifiable information** (PII) which can be abused by criminals. Major updates on your life are nice to share with loved ones but consider how much of this information is also associated to password security questions, such as significant dates, names of pets or details of schools attended.

Criminals combine social engineering with time pressure to make you act quickly without thinking.

How to protect yourself:

- Open new communication channels through contact details found on websites instead of clicking on links in unsolicited text messages and emails; even if they appear to be from someone you know and trust such as parcel delivery companies or your bank. Some businesses have been targeted by criminals posing as company employees to build trust and make requests for information or transfers of funds seem expected. Report and delete any such texts or emails.
- Keep private information limited to your close social circle and restrict open profiles where PII information is being shared to individuals you know and trust.

- Review the permissions and privacy settings regarding what data you are sharing with companies. Consider whether the information is necessary for the application or website to function and if it isn't, restrict access to your data.
- Check to see if your email address or password has been leaked in a previous data breach on **haveibeenpwned.com**. Ensure passwords are regularly changed.
- Review the full email address including the domain name (after the @ symbol) of a sender. Criminals often include a reputable company name in the email address to make it appear genuine. Be wary of those sent from free email address providers, for example Amazon@gmail.com or domain variations such as Admin@Amazon-Support.com.

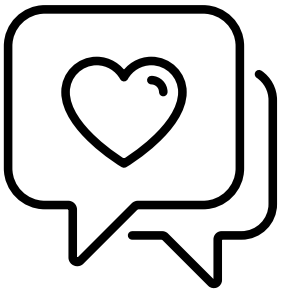


THE POWER OF SOCIAL MEDIA

Influencer marketing is a powerful digital strategy which uses celebrities and social media influencers to sell or promote assets. In recent years, both legitimate companies and criminals alike have recognised the power of social media in promoting their businesses.

Criminals sometimes use convincing-looking fake testimonials accompanied with a picture of a well-known figure to help frauds seem legitimate. These adverts may impersonate celebrities to promote products or encourage investment. Just because a company has a glossy website, celebrity endorsement and good reviews, it doesn't mean it's genuine.

Criminals also engage in fraud through hacks of social media accounts of celebrities and financial-influencers. In some instances, the influencers themselves may have genuinely bought in, either knowingly or unknowingly, that it was a fraud. In other cases, criminals hack people's everyday accounts and impersonate people's friends or family to facilitate fraud.

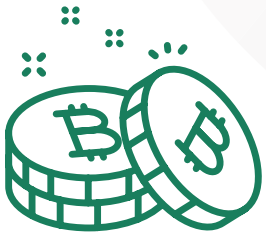


Verified accounts — Social media platforms, including those trading in digital assets, use authentication marks to signify trust. Fraudsters are known to have purchased or falsified 'blue ticks' to appear legitimate.

How to protect yourself:

- Check an independent platform before signing up for promotions to confirm the legitimacy of what is being offered.
- Cross-reference account names, even those with authentication marks, against official sites or independent platforms to make sure that you are viewing genuine accounts instead of near-identical copies.
- Research whether the celebrity or influencer has an ulterior motive for publishing the content and whether they have received any benefits for advertising.

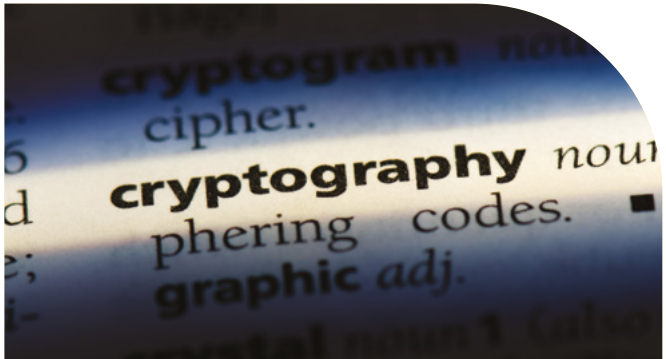
CRYPTO 101



INTRODUCTION — WHAT ARE CRYPTO AND DIGITAL ASSETS?

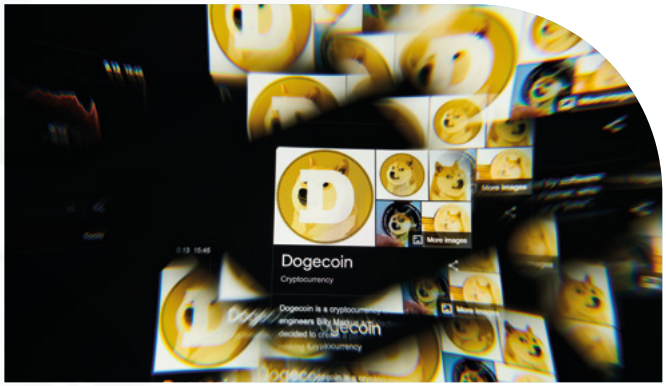
Cryptoassets, also commonly referred to as 'cryptocurrency', 'tokens' or 'coins', are digital representations of value or rights which can be stored, transferred and traded, often using distributed ledger technology. They are so called as they use cryptography to secure communications. There are thousands of coins currently in existence including well-known coins such as Bitcoin, Ethereum and Ripple.

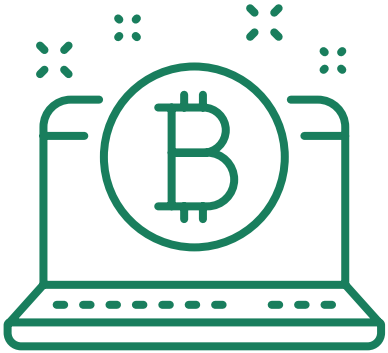
Cryptography is the practice of protecting information through encryption and decryption. Encryption involves transferring information to a code which is secured with a key; a string of characters within an algorithm used to alter data so it appears random. There are public and private elements to keys in a similar way to account numbers and PIN codes for banking. A private key needs to be held for assets to be sent as only someone with the key can decrypt the data.



Distributed ledger technology is a combined schedule of transactions which are processed and recorded collectively by a network of independent computers. This makes it very difficult to censor or tamper with. The ledger is not usually controlled by a central authority such as a bank or a government and no-one can stop or reverse transactions. This allows value transfers directly between individuals, in a similar way to using cash.

The most well-known distributed ledger is the Bitcoin **blockchain** which provides a permanent, public record of all Bitcoin transactions that have taken place since it was first used in 2009. There are many other coins, often called **Altcoins**, so-named as they were originally considered alternatives to Bitcoin.





Cryptoassets differ from each other in the way in which they operate, including scope, value, processing time, transaction fees, functionality and the use of smart contracts. For example, Ethereum uses a different technology to Bitcoin which allows the processing of more transactions and is also a platform on which other applications are built.

Stablecoins are tokens whose value is advertised as being tied to other assets. This includes government currencies such as US dollars or other items like gold.

Stablecoins are popular because their value does not fluctuate as rapidly as other cryptoassets. This is useful in countries with large populations without ready access to bank accounts, those with high inflation or those where it is difficult to save in the local currency without losing value.

Caution must also be taken when purchasing stablecoins as the link, or 'peg', to the underlying asset is not guaranteed and **capital is still at risk**.

Cryptoassets tend to be volatile, speculative and their use comes with a number of risks. Within the UK, although certain laws and regulations apply to them, they are not regulated as strictly as banks or the stock market and losses are unlikely to be covered by the Financial Services Compensation Scheme (FSCS) so you may struggle to obtain reimbursement if your assets are lost, even to fraud.

HOW ARE DIGITAL ASSETS USED IN CRIME?

The benefits of decentralised financial structures (decreasing fees for services, quick transfers of assets, relative anonymity and lack of centralised authorities) are also attractive to criminals for illicit means. For example, criminals utilise the ability to remain **pseudo-anonymous** whilst sending and receiving illicit funds as a way of avoiding detection. **Ransomware** attackers often demand payments in cryptoassets as this eliminates the need to use financial institutions to process transactions and allows the rapid transfer of funds to increase difficulty in retrieving them.

Cryptoassets have been used as a method of payment on **Darknet** marketplaces for a number of years. These marketplaces are commonly used by criminals as a way to promote and sell goods including drugs, weapons, extreme material and even criminal contracts. It is important to use caution, conduct thorough research and to follow legal guidelines while using crypto and digital assets to avoid inadvertently participating in, or supporting, criminal activities including money laundering and terrorist financing.

More recently there has been a rise in the number of street crimes involving digital assets due to a lack of user awareness of phone and wallet application protections, as well as digital security generally.

In addition to crime facilitated by digital assets, there are other growing crime types which are directly linked to them. Many applications and websites are found entirely on the blockchain; crypto-banks, crypto-games, crypto-based social media and more. It is common for hackers to attack and steal funds from such blockchain applications so risks associated to specific applications should be checked prior to depositing assets.

However, whilst there are billions of pounds of illicit crypto transactions each year, this only accounts for a small percentage of all transactions globally.

GOLDEN RULES TO PREVENT DIGITAL ASSET FRAUD

Digital Assets are a volatile market in which prices can rise or fall rapidly. As with other investments, **your capital is at risk**. Criminals utilise the 'high risk, high reward' investment advertising for crypto as an opportunity to facilitate fraud.

1. **Don't be rushed** into decisions and take time to do your research. Seek advice from family and trusted friends, or independent assistance from an advisor accredited by the Financial Conduct Authority with knowledge of cryptoassets. Ensure you understand what it is you're buying and verify the legitimacy of where you're buying it from.
2. **If it sounds too good to be true, it probably is**. There are no guaranteed get-rich-quick schemes. Any taglines or phrases which can 'guarantee returns' or promise 'consistent profit' should be treated with caution. Do your research and check the White Paper which provides the background to the project and what it intends to do.
3. **Be wary of unsolicited contact** which prompts you to act or divulge information; even if you are a customer with the company contacting you or know the person requesting it. Log in to your accounts directly rather than clicking on links in messages, emails or on social media.
4. **Look for subtle differences** in URLs (web addresses), contact numbers and email addresses to identify fraudulent activity. Check receiving wallet addresses before transferring assets and ensure when accepting contract terms that these are facilitating what is advertised.
5. **Don't advertise your holdings**, in much the same way as you wouldn't advertise your wealth; this can make you a target for criminals.

Lots of firms associated to digital assets are in international jurisdictions which makes recovery of assets incredibly difficult. You may not have access to compensation schemes if you lose your assets; even if they are lost as a result of fraud.

If you are the victim of fraud or cybercrime, report it to **Action Fraud**. Reporting through official channels means law enforcement can target offenders and identify patterns. Prompt reporting is key for asset recovery.

WHAT ARE EXCHANGES OR COIN SWAP SERVICES?

A cryptoasset exchange is an online service, accessed through a website or application, through which an individual can buy or sell different cryptoassets and monitor changes in their values.

Centralised exchanges, or CEXes, allow conversions between 'fiat' currencies (those decreed by governments such as pounds, euros or dollars) and cryptoassets as well as between different cryptoassets. They are 'centralised' as they are governed by a single company which has control over customer assets in a similar way to a Bureau de Change. Some exchanges allow users to store their cryptoassets within the exchange itself in custodial wallets.

A number of exchanges are registered with the Financial Conduct Authority to ensure compliance with Anti Money Laundering (AML) and Countering Terrorist Financing (CTF) directives; however not all are.

Decentralised exchanges, also known as DEXes, token swap or coin swap services, are applications running entirely on the blockchain. These can also be used for trading assets but with some important differences;

- DEXes can only be used to trade between different cryptoassets and do not allow conversion to 'fiat' currency.
- DEXes are **non-custodial** which means they never take control of the assets in your crypto wallet. Your assets remain in your wallet and can only be used to trade assets approved by you.
- Unlike CEXes, DEXes do not require users to open accounts or verify their identity, which means that risks of illicit activity and money laundering are higher. Higher commission for trades is also normally charged.

Due to the decentralized nature of cryptoassets, if you have lost digital assets due to a crypto-related crime, there is no central authority which can compensate you. Buying or selling cryptoassets from an unregistered exchange creates an additional level of risk.

Protect yourself

WALLETS

A wallet is a digital tool which allows you to store and interact with your digital assets in a similar way to a bank account. Wallets can be non-custodial or custodial. Non-custodial, or 'self hosted', wallets are those under your control; the digital equivalent of keeping cash in your pocket. Custodial wallets are under the control of a third party who operates it for you; similar to keeping money in your bank account.

Wallets contain both public and private keys needed for transfers. Public keys are visible to the network (like a bank account number and sort code) while a private key is kept secret and is used to authorise transactions, like a password or PIN number.

Wallets come in various forms and can be 'hot' or 'cold'. Hot wallets are continually connected to the internet whereas Cold wallets, or offline wallets, aren't.

Custodial wallets — these can be application or web-based and are provided by exchanges or other third parties. They are easy to use and convenient however rely on the provider following good security practices to avoid hacks or attacks.

Paper wallets — these are printed copies of the keys, often containing a QR code. Although they are safer as they are not connected to the internet, the paper must then be stored securely as if lost or stolen, access to the assets can be lost forever. Malware checks should be run before generating the keys for printing.

Software wallets — these are non-custodial, digital wallets which are available through phone applications or web browser plugins. They are usually free and easy to use but may be more susceptible to hacks because they are always online.

Hardware wallets — while these are more costly to purchase and are less convenient than other wallets, they provide secure storage offline as they are not always connected to the internet. Your keys are stored on a separate device, similar to a USB drive. Although protected by a PIN, consideration should also be given to physically storing them safely. Never buy a wallet second-hand as the recovery seed to rebuild it could be retained by the seller, even if the passwords are provided.

Information on how to keep your wallet safe can be found on page 18.

WHAT IS WEB3?

In its current form, most online data on the 'Web2' internet is controlled by central authorities such as search engines, e-commerce marketplaces and social media platforms. The concept of Web3 is to create an overhauled version of the internet by promoting the distribution of power across a network; recording transactions on a distributed ledger and using coins and tokens as a way of exchanging value. The vision is that all online activities could be controlled collectively by users so that there isn't a dominating company.

It is suggested that this decentralised environment could utilise **Smart Contracts** and **Decentralised applications** (dApps) which are linked with the development of virtual worlds such as the metaverse.

Supporters of Web3 suggest its decentralized nature allows more financial independence, control and ownership however critics fear that Web3 may be difficult to police and each individual could bear all the risks if things were to go wrong. The pseudo-anonymous nature of the system could also create difficulties in users not being confident in who they are dealing with.

WHAT IS DEFI?

DeFi, or **decentralised finance**, is a collection of financial services built on distributed ledger technology. Its enthusiasts believe it has the potential to revolutionise traditional financial systems by allowing users to engage separately from central authorities to provide greater individual control over financial activities. It is intended to replicate banking and financial services but instead have them controlled by users in a similar way to a co-operative, rather than through centralised entities.

WHAT ARE SMART CONTRACTS?

Smart contracts are self-executing transactional agreements which enforce the terms and conditions written in a code and eliminate the need for third parties in carrying out contractual obligations. As an example, with a particular smart contract in place, cryptoassets from a purchaser would not be released to a seller until the goods or service have been delivered. Alternatively, contracts could allow lending governed by a code instead of a bank's assessment about their customer. Their uses are varied but they can be used for decentralised financial transactions or in decentralised applications (DApps) such as decentralized versions of social media platforms.

Smart contracts can also be used or attacked by criminals for illicit means. This can be by exploiting flawed smart contract codes or through using malicious smart contracts designed to allow asset theft by creators of the contract. They can also be used to engineer rug-pulls **(see page 26)**. In other cases, criminals may encourage you to click on links which accept terms or transactions you wouldn't agree to.

The nature of some contracts means that admin keys are needed to allow individuals to update the code however others are designed so that even the creators cannot control or modify it. Trust is still required in the code creators that coding mistakes, design flaws, bugs or hacks will not lead to them being compromised.

How to protect yourself:

- Avoid clicking on links or scanning QR codes without knowing where these lead.
- Check what is being agreed and that you understand the contract before accepting terms. Criminals often use complex or vague terms to appear legitimate.
- Ask if the code has been independently audited. This typically involves a review to identify vulnerabilities or weaknesses affecting performance.
- Research DeFi platforms and protocols before investing to familiarise yourself with the specific risks of DeFi investments. Treat investment pools with caution, particularly those with limited timeframes to join.

PRECAUTIONS & PROTECTION

BE AWARE OF YOUR PHYSICAL SURROUNDINGS

Be aware

Hardware and physical items associated with digital assets such as paper wallets and recovery seeds **(see page 18)** can be targeted for thefts in much the same way as other high value items. Advice on protecting your home from burglary can be found on the Police Service of Northern Ireland website — **psni.police.uk/safety-and-support/keeping-safe/protecting-your-home**

Criminals can also gain access to your personal information by **shoulder surfing**. They target you in crowded areas such as on public transport, bars, shops or cafés, or when at a state of heightened vulnerability such as when intoxicated.

Criminals may watch or film as you input private information such as passwords or security patterns. It is common for mobile phones to then be stolen. Criminals can then quickly change the necessary passwords or security features to move funds from digital wallets or make purchases on applications.

How to protect yourself:

- Be aware of your surroundings when accessing your device, particularly when entering your PIN number or passcodes.
- Use additional biometric data such as a face or fingerprint ID, or enable 2-step verification (2SV), which is also known as two-factor authentication (2FA) or multi-factor authentication (MFA), to secure high-value applications within devices.
- Use different PIN numbers and passwords for your phone to any wallet or banking applications and consider keeping high-value applications on separate devices.
- Don't store passwords or recovery seeds to any digital wallets on your phone.

KEEPING YOUR DEVICES SAFE

Use a strong and separate password for your email

If access to your email address is gained, criminals can find out private information about you including account numbers for other services such as your bank. They can also use your email address to reset passwords for other accounts. In some cases, criminals send emails pretending to be from you to help commit fraud against people you know.

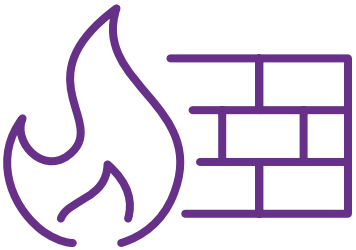
Check to see if your email address or password has been leaked in a previous data breach on **haveibeenpwned.com**

Keep software updated

Not keeping software up-to-date means that any new vulnerabilities found by cyber criminals. Designers are constantly improving it as new vulnerabilities are discovered so older software may be redundant or not have the updated support. This means that any new vulnerabilities found by cyber criminals may not be fixed, leaving the software vulnerable to attack. This is especially true for operating systems.

You can do this by downloading updates or patches from the software developer, and you can turn on automatic updates for your devices and software that offer it. This means you will not have to remember each time.

Some devices and software need to be updated manually. You may get reminders on your phone or computer. Do not ignore these reminders. Updating will help to keep you safe.



STRONG PASSWORDS

Often IT security is breached because a default password on software or hardware has not been changed. It is important that all default passwords are changed as soon as possible.

Consider storing passwords in a password manager; major operating systems typically have these included.

If you're not using a password manager, the National Cyber Security Centre and the Metropolitan Police Service recommend starting with three random words put together such as OrangeWalletJoke. The MPS have created a video to help create a strong password which can be found at **met.police.uk/littlemedia**

There are a number of general rules regarding passwords that will make them even more secure:

- The longer the password, the harder it is to crack. Aim for at least 14 characters.
- Use a combination of uppercase, lowercase, numbers and symbols, for example: OrangeWalletJoke%62
- Consider altering words found in the dictionary to make them harder to guess such as using '0' instead of 'O' or '£' instead of 'E'.
- Avoid personal details such as family names, pet names, date of birth or sports teams.
- Use different passwords for different accounts, especially for your email address.
- Use different passwords on your high value accounts, as well as using biometrics and facial recognition, to keep these accounts or wallets safe.

MULTI-FACTOR VERIFICATION

Multi-factor verification, two step verification, 2SV or 2FA, is a way of granting access to an area or system only after the user has provided two or more pieces of authentication. For example you can't take any money out of an ATM with just a bank card or just a PIN code; you need both.

Most large internet providers such as Google, Amazon, Facebook and LinkedIn as well as financial institution's applications have 2FA available, information on which can be found by searching their webpages.

Basic 2FA usually involves either providing a phone number, so your phone is messaged when someone (including you) tries to log into your account, or an application installed on a smartphone which continually provides a new time sensitive code to allow you to access your account. This means a criminal would need both factors (ie. your password and your phone) to gain access to your accounts or systems.

It is preferable to use a separate device for the authentication process as, if your phone is stolen, criminals may be able to access your authentication applications, emails or text messages to navigate around this security feature. Consider locking your wallet applications when not in use with a separate passcode to that of your phone.

For further information and help on 2FA, go to **ncsc.gov.uk/cyberaware/home**

WALLET SECURITY

Security will vary depending on the type of wallet being used.

How to protect yourself:

- Use reputable providers. Conduct research to ensure the type of wallet is right for your needs and that official applications are used.
- Consider using multisig wallets — these require two or more signatures to authorise transfer of assets. Although these can slow down the process of payment significantly, they require additional validity to authorise transactions.
- Encrypt your wallet on devices with a passcode, multi-factor authentication, biometric data or facial recognition access. Use a password manager, update passphrases regularly and don't share your passphrases with others.
- Check your wallet regularly so suspicious activity can be identified quickly.

RECOVERY SEEDS/ PRIVATE KEYS

A recovery seed, back-up phrase or seed phrase is a list of words which can be used to restore a digital wallet. It allows users to rebuild a wallet in cases of loss, damage or a forgotten passphrase. The recovery seed is made up of a combination of 12 or 24 random words which are generated during the wallet creation process.

It is extremely important to keep this recovery seed safe as, without it, if locked out of your wallet or it's lost or stolen, it becomes impossible to gain access to your assets again. It is also important not to share the recovery seed with others as you risk anyone being able to rebuild your wallet.

The seed should be written down and kept within a safe or lockbox. Ideally, two word-lists should be created, each containing some but not all of the recovery phrase and these should be stored separately so that if the lists are found independently of each other, unauthorised access to the wallet cannot be gained.

Seed phrases should not be stored on mobile phone notes, cloud back-up services or photographs taken of them as if your phone is stolen or the service is hacked, criminals will also be able to access your wallet.

CHECK YOUR PERMISSIONS

When using decentralized applications, you will be connecting to a variety of protocols and granting them various permissions to view and manage your assets. These applications may be able to buy, sell or move assets in your self-hosted wallet, depending on which permissions you grant. It's important to regularly review and remove permissions from any apps and protocols you no longer use or want to have access to your wallet.

For example, if you use a DEX to trade cryptoassets and give it permissions to move certain assets from your wallet, once the trade has been completed you should revoke those permissions as if the DEX is later hacked, the old permissions could be used to remove assets from your wallet.

Use a third-party token allowance checker to determine which sites and apps you have permitted to access funds in your wallet. You should also regularly review the list of devices authorised to access your crypto account and remove any as appropriate.

SECURED CONNECTIONS

Connecting to public Wi-Fi or through insecure networks may also put your wallet's security at risk as rogue access points can be disguised as legitimate Wi-Fi networks. This gives criminals the ability to see your data, including passwords, and grants them access to modify anything that they intercept. Hackers can transfer assets you're sending via these networks to their own wallets.

Only access your wallet via secure network connections and be wary of which networks you are connecting to when in public.

TYPES OF CRIME

INVESTMENT FRAUD

Investing in stocks, shares and commodities can be a successful way of making money however it can also lead to people losing their whole life's savings. Criminals will try to persuade us to invest in schemes which are fake, non-existent or aren't worth the money that was paid. Within the UK, there are an array of investment frauds; both with traditional stocks and shares and also with cryptoassets.

Digital asset markets are incredibly volatile and there is no guarantee of any profit. There are a variety of crypto investment frauds used by criminals who lure in individuals with promises of consistent, high profit returns. It is important to know the risks before investing.

'Crypto experts' may showcase the huge profits they have purportedly made through their investments and offer to teach you to do the same or offer to do this on your behalf. They will often use tactics to make you act quickly; even if you feel that you are in control. Alternatively, they may ask for payments to share their knowledge. Some criminals initially start by providing returns on investments to help build trust. Once enough funds have been extracted, the criminal will then cut all contact.

The Financial Conduct Authority (FCA) does not regulate most crypto activity so the Financial Services Compensation Service cannot protect you if a platform which exchanges or holds digital assets goes out of business. You are also unlikely to have access to the Financial Ombudsman Service and there isn't an easy way to get your assets back if they are stolen.

Profits made from cryptoassets may be subject to tax within the UK; check the HM Revenue and Customers website for further information.

How to protect yourself:

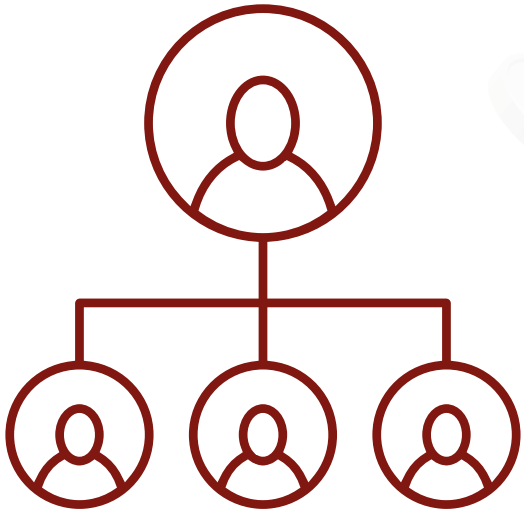
- There are no 'get rich quick' schemes and, as with other investments, investments can go down as well as up. Your capital is at risk and you should avoid investing what you can't afford to lose or borrowing any money to do so.

- Thoroughly research all products and companies that you are investing in and seek advice from a regulated, independent financial advisor with knowledge of cryptoassets. Read reviews and research the individuals who are part of the business to determine whether the team behind the project hold the relevant experience and whether they are backed by credible venture capital or strategic advisors.
- Check the legitimacy of businesses by referring to the FCA's warning list of unauthorised firms and validating the publicised registration number. Verify the company details through multiple sources, not just Companies House. Even registered companies have risks, so ensure you understand these before investing.
- Check the FCA 'ScamSmart' investment and pensions checker to determine whether the opportunity you've been offered is known to be fraudulent.
- Be wary of aggressive, 'hard-selling' marketing approaches, particularly those who make repeated attempts to contact you across various platforms, those where you are incentivised to recruit others to invest or those where there is a minimum purchase level.
- There are now rules on marketing crypto products to ensure that advertising is clear, fair and not misleading. Overseas and unregulated firms may not adhere to these regulations so be wary of anyone who doesn't clearly highlight the risks of investment.
- Take your time — criminals will try to pressure you into making quick decisions; often describing or implying the situation is 'time sensitive' so you do not have the time to research and make an informed decision.

If you lose money as a result of a digital asset crime, be wary of illegitimate firms offering to retrieve any money for you as this may be criminals targeting you again.

PONZI SCHEMES

A Ponzi scheme is a fraudulent investment scheme where new investor's funds repay the investments made by earlier investors; creating an illusion that profit is being made. Criminals will take a cut of this themselves to make money. As the scheme grows and operators struggle to find new investors to sustain the promised returns, the operator may disappear leaving investors with significant financial losses.



Because of the reliance on constant recruitment of new investors, criminals will post messages in online forums or message boards to encourage participation or use existing investors to recruit their family and friends. Organisers will often purport to use the latest technology or products to entice investors as people are less sceptical of investments when assessing something new or innovative. Ponzi schemes have been used for over a century but have recently moved to cryptoassets due to these having less regulatory oversight than other investments.

How to protect yourself:

- Ignore 'Low risk, High Reward' advertising — Every investment carries risk and crypto is an incredibly volatile market. Even genuine investments also go up and down over time so overly consistent return promises should be treated with caution.
- Do not rush — Some criminals will encourage you to make decisions 'right now'. This reduces your time to think rationally and make a well informed decision. Take your time and seek advice before committing.
- Criminals exploit trust derived from membership of a group who share an affinity through national, ethnic or religious affiliation. Respected or prominent members may be enlisted, both knowingly and unknowingly, to advertise 'investments'.

Low risk, High reward

- Do your research — Companies House and the FCA both hold information about registered companies. Secretive or complex strategies can be used to disguise fraudulent schemes so be wary of excuses for why you can't review information about investments in writing. Check the backgrounds of the employees to validate their experience working for credible companies previously and verify how the company is making money. If the only identifiable source of funds is through new investment this may suggest it's a Ponzi scheme.

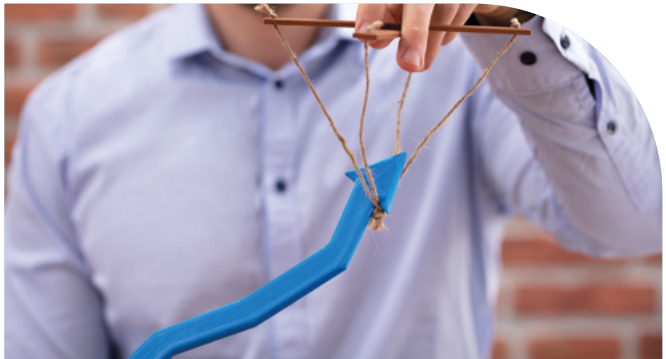
INSIDER DEALING AND MARKET MANIPULATION

Market manipulation is where an individual or group deceive investors by deliberately controlling or affecting the price of financial markets for their benefit. This includes markets containing digital assets.

As an example, a group may make agreements amongst themselves to buy and sell coins at predetermined times in order affect the supply and demand of a particular asset. They may also agree to artificially inflate the price of an asset to deceive other investors; the goal of which is to make as much profit for themselves whilst exposing other investors to a loss.

Whilst this type of fraud does not usually target any one person specifically, it can cause sudden changes of an asset's value without any prior warning.

It is difficult to know as a victim of market manipulation whether the loss of value is by chance or if someone has deliberately acted in a way which has caused a shift in value. Crypto and digital assets are not regulated in the same way as other financial investments so the protections under the Market Abuse Regulation (MAR), which were introduced to increase market integrity and investor protection, may not apply.



It is advised that if you see any person online discussing or planning action with the intention of directly manipulating the market value of any cryptoassets, that you report it to Action Fraud.

How to protect yourself:

- Research the history of an asset to see patterns of movement prior to investing. Sudden, unexplained changes in trading volumes may suggest manipulation as may excessive sales in a short space of time or multiple accounts behaving in a similar way.
- Before acting on a report of information, check where it's come from and verify the information from numerous sources to avoid false claims.

PUMP-AND-DUMP SCHEMES

Pump-and-dump schemes are a type of fraud which involves artificially inflating the price of an asset and then selling it at the inflated price for a profit. The assets then often plummet leaving unsuspecting investors out of pocket.

Fraudsters, either individually or in groups, agree to accumulate assets while the price is low and then rapidly promote the project or coin by spreading misinformation. They use aggressive advertising through 'finfluencers' (financial influencers), social media channels and other means to create hype around an asset to artificially create demand and attract investors.

The information the fraudsters use is usually fictitious and predominantly focussed on unmissable opportunities which drives the 'fear of missing out' (FOMO) or quick desires for profits. These types of schemes generally do not tend to target specific individuals as they want as many people as possible to buy in and increase the demand of the asset.

How to protect yourself:

- Be wary of 'high return, low risk' advertisements and those not adhering to the Financial Conduct Authority's regulations.
- Review the history of an asset's value through a block explorer. Value can fluctuate due to performance or market conditions however sudden swings should be viewed with caution. A small number of token holders can also mean that if assets are sold there can be sudden damage to value.
- Clarify how the company secures their customer's assets and how easily you can remove them from the particular platform.
- Consider the source of any hype and be wary of fake news. Reflect why, if a scheme was so lucrative, someone would be so pushy about advertising it. Fact check information with other sources and be cautious of 'hot tips'.

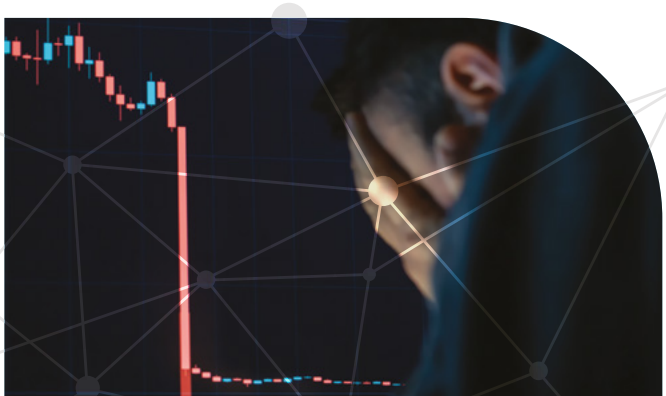
RUG PULLS

A rug pull is a type of fraud where the creator or development team behind a project suddenly disappear; taking with them all of the invested funds. This often involves liquidating or selling off any assets they hold resulting in a value drop and significant loss for investors. These are a type of **exit scam** which are common within decentralized finance (DeFi). The exit often happens quickly, leaving investors with devalued or worthless assets.

Rug pulls happen with coins and NFT frauds. It's important to find out about a project's roadmap prior to investing to see where the project is going.

How to protect yourself:

- Be wary of hype on social media or channels such as Discord, Telegram or Reddit for anyone advertising consistently high returns — if something seems too good to be true, it probably is.
- Research the legitimacy of projects by reviewing the previous projects of the creative team, their community engagement and how transparent they are.
- Check whether there has been a formal audit process of the underlying code. This should be carried out by a reputable, independent third party.
- Check whether the coin is liquidity-locked with time-locked smart contracts through a third-party. Without this, there is nothing stopping the creators liquidating the project. Check the percentage of the liquidity which has been locked as this is only helpful for the pool it secures.
- If unsure, buy a small amount of the asset and then attempt to sell it to check for **Limiting Sell Orders** prior to investing larger amounts. These orders place restrictions on the code and may affect their saleability or value. Sites such as DexTools can be used to search for the token which show whether it has limitations on selling, amongst other information.



ROMANCE FRAUD

Due to Covid-19 and the subsequent lockdown, the manner in which we meet people for relationships has changed. More and more people are using online chatrooms, social media sites and matchmaking applications to find love.

Romance frauds happen when people are socially engineered into false relationships by criminals who aim to steal their identities or money. Criminals are well practised at building trust and manipulating people so that when money is asked for, this doesn't seem unreasonable.

Romance fraud can have a severe financial, social and emotional impact upon individuals and is similar to grooming, domestic abuse and coercive control. This type of crime may be identified by family and friends first as victims may feel they are making decisions which are rational and reasonable. This, and a sense of embarrassment, can have an adverse effect on willingness to report what's happened to law enforcement.

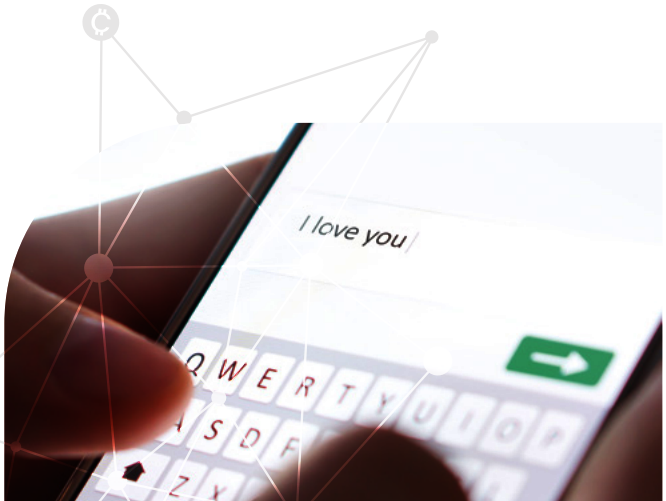
The following are **common tactics** used by romance fraudsters to manipulate you;

- Setting up the relationship in a harmless and expected way by providing information about their life, job, family, aspirations and wishes.
- Verifying their existence by introducing other criminals who pose as family members, friends or professionals to make their story seem convincing.
- Distracting you with promises for the future.
- Disguising requests for money, requesting it in an indirect way or implying that the need for financial support is temporary. This can come from the drip feeding of information so that when asked for, it doesn't raise concern. They may also make you feel it's your idea or initially turn down your offers of financial assistance to build your trust.
- Encouraging secrecy, cutting you off from your support networks and making you feel disloyal for seeking advice or questioning what is being asked. This is made to seem as if it is mutually agreed rather than a cause for alarm.

- Manipulating the sense of power so that you apologise or feel guilty for raising concern, even when this is reasonable, or by the criminal claiming the lack of belief is causing physical or emotional pain.

How to protect yourself:

- Be aware of what personal information you are providing about yourself online and never provide copies of your personal documents to anyone you haven't met.
- Block and report profiles to social media platforms from individuals who create a sense of obligation to respond.
- Keep conversations on the matchmaking service platform. Criminals will often try to move the conversation to an encrypted application. This makes it harder for law enforcement to gather evidence and trace the individual.
- Don't send any money or cryptoassets to people you haven't met, regardless of how long you've been speaking to them or how much you trust them. Avoid transferring money on their behalf, taking out loans for them, sending or receiving parcels for them or allowing them access to your bank accounts.
- Perform a Reverse Image Search for pictures which may have been taken from somewhere else. Examine the metadata of images provided to determine if these are generated by Artificial Intelligence. Be wary of videos where there is a mismatch between sound and motion or distortions in mouth movement.
- If in doubt, ask your friends and family to sense-check the situation. It may be difficult to judge someone if you are too close, and be wary of anyone who is encouraging you to keep information away from your support network.



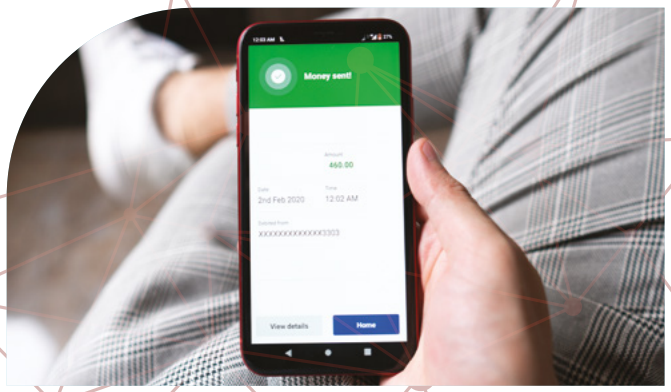
SOCIALLY ENGINEERED INVESTMENT FRAUD

Socially engineered investment fraud, often referred to as **'pig butchering'**, is a specific form of long term fraud whereby a criminal exploits a relationship they have built and encourages investment in what appears to be a seemingly profitable scheme. This can be through any trust-based, false relationship which may be romantic, friendship or through someone posing in a professional capacity. This type of fraud occurs through psychologically manipulating you to send or invest money. It is common for intelligent and tech-savvy individuals to be targeted.

In some circumstances, criminals may pose as a knowledgeable or trustworthy investor, or claim they know someone who is, to give tips, ask you to invest in schemes or to transfer crypto to certain types of wallets. They may show you examples of their supposed wealth and may offer to show you how this was achieved.

To make this scheme seem legitimate and encourage you to keep sending more money, the criminal may send you what is purported to be an initial return on your investment with the promise of greater returns if further assets are sent. Eventually, you will invest a significant sum only for the criminal to cut off all communications and leave with your assets.

There are occasions in which criminals will contact you after the original fraud, pretending to be someone who can 'help' you get your assets back. The criminal may then convince you to pay a further fee, described as a tracking fee or recovery fee, which can result in the return of your assets. Out of desperation, some victims pay this, resulting in further losses.



How to protect yourself:

- Be cautious of unsolicited messages on social media platforms such as Instagram, LinkedIn or dating applications as well as 'wrong number' texts and contact through group chats.
- Criminals may ask you to move communications away from these platforms to encrypted messaging services such as WhatsApp, Telegram or Signal.
- No matter how long you've been speaking to someone online and how much you trust them, never send them any money or allow them access to your bank account or digital wallet. Do not transfer money on their behalf, invest your own money on their advice or take out a loan for them.
- Never provide copies of your personal documents such as passports or driving licences, or provide details of your financial accounts or cryptoassets.
- Be wary of individuals posing as experts who do not also highlight the risks around investments.
- Do your own research before investing in digital assets. The Global Anti-Scam Organization and ScamAdviser websites amongst others maintain a list of fraudulent websites, many of which involve cryptoassets.
- Use a third-party blockchain explorer to independently check addresses of where assets are being sent.

Socially engineered investment frauds are committed through the criminal developing complete trust from you, often over an extended period of time. By the time that money is requested or investment encouraged, you will have been primed to believe this is legitimate so the request may not feel unexpected.

Speak to trusted friends, family or an independent financial advisor to 'sense-check' before making decisions.

IMPERSONATION FRAUD

Impersonation fraud involves criminals masquerading as someone they are not to deceive you to buy into a project, disclose private information or send assets.

These types of criminals are skilled at social engineering and are convincing in their stories. The impersonations range from staff members of crypto services to individuals from technology teams and from government officials to police officers.

In some cases, criminals pretend to be individuals known to you including your relatives. The criminal will often ask for secrecy to prevent this information from being checked.

The criminal may start by unsolicited contact; outlining an issue and needing an urgent response. They may then either ask for personal information from you, payments, security answers, wallet recovery seeds or passwords; providing an excuse linked to their impersonation. In some instances, criminals posing as technical support may ask for remote access to computers.

How to protect yourself:

- Ignore unsolicited calls, messages and emails and do not provide personal information, bank details, wallet addresses or passwords from this contact. Legitimate companies would not ask for this information. Criminals can spoof (imitate) phone numbers to make it seem as though a trusted service is calling you.
- If in doubt, contact the agency directly from a different phone, using details found on an official website or document instead of those given to you to verify anything that is being asked.
- Never give remote access to your computer or install any software on direction of an alleged support agent.

SEXTORTION

Sextortion is a form of blackmail which involves threatening to publish sexual information, photographs or videos to extort money or to get you to do something against your will. Photos or recordings are often made without you realising or consenting. Criminals will sometimes demand a payment in cryptoassets for these videos not to be released.

These types of crimes are also sometimes committed by individuals who do not hold any such videos of you. They can be committed as part of a phishing attack to numerous people or directed towards specific individuals. The communications from the criminal may also include a password or username from one of your online accounts which has been taken from a data-breach to attempt to appear more credible.

How to protect yourself:

- Always be careful about the information and pictures you share and post online. Consider who you are sending intimate content to, if they are who they say they are and if you can trust them.
- Keep your devices protected with antivirus software.
- Review your privacy settings.

If targeted:

- Do not panic — non-judgemental help is available.
- Don't pay the money which is being requested. Many victims who pay continue to get demands for higher amounts of money. In some cases, even when demands are met, the criminals will still post the videos online.
- Save the evidence — take screenshots, save messages and images. Collect URL links and report it to social media companies.
- Report the matter to Police using our online reporting tools or by calling **101**.

INITIAL COIN OFFERINGS (ICOS) FRAUD

Initial Coin Offerings (ICOs) are fundraising methods used by cryptoasset projects to raise capital by issuing and selling their own digital coins or tokens to investors. The tokens may have some utility related to the product or represent a stake in the project and a share of its profits. Many legitimate projects have successfully used ICOs to raise funds however they are less regulated than stock market Initial Public Offerings (IPOs) and have often been used to defraud investors in a variety of ways including;

- Fake projects — Presenting the ICO as a genuine investment opportunity but for a project which doesn't exist or lacks any substance.
- Misleading information — Offering the investors a promise of quick returns or guaranteed profits, advertising little or no risk, promoting false partnerships with genuine companies, inflating the market potential or through using celebrities or influencers to endorse the products to generate trust.
- Pump and Dump schemes **(see page 25)**.
- Phishing and Hacking **(see page 38)**.

Following initial investment, criminals may then disappear with investors' money as part of a rug-pull **(see page 26)**.

How to protect yourself:

- Know what you are buying into and conduct due diligence research. Look for clear and transparent information about the project, its team and the technology. Check the White Paper which provides the background to the project and what it hopes to achieve.
- Scam coins may copy White Papers of legitimate companies to appear genuine so you need to validate the company as part of your research.
- Be wary of red flags such as unrealistic promises, a lack of a prototype or a lack of community engagement.
- Seek advice from a registered financial advisor or investment professional who has knowledge and experience of cryptoassets.

FAKE WALLET APPLICATIONS

A large number of individuals access their digital asset wallet via an application on their phone. There are a number of different applications and, whilst the majority are legitimate, some are not. Fraudulent wallets vary in levels of quality and some can be incredibly convincing. These applications are designed to deceive you into thinking that you are sending your cryptoassets to a secure location but in fact divert them to criminals. These fake applications can also be used to steal seed phrases.

Fraudulent applications can sometimes appear in adverts on webpages with what appears to be a link to an App store. Some are promoted by online influencers who may or may not be aware that the product they are advertising is fraudulent.

There are certain ways to identify potential fraudulent wallet applications; one of which is misspelt words within the application URL. This could be words omitting a letter or swapping two letters within a word, such as 'invetsment' or 'crytocurrency'. A lack of social media presence, or lack of information on the owner or company, can also be indicators of fraudulent activity.

How to protect yourself:

- Double-check the spelling — It's easy to miss small details like a letter being missed or added in a URL.
- Make sure the application you are downloading is the correct version. Just because one application is the most downloaded, it doesn't mean it's genuine. Check official websites to be sure of the name.
- Most wallet providers will have some form of social media presence or information about them online. Verify reports before downloading applications.
- Add the legitimate website address to your browser's favourites list instead of searching for it on a search engine for faster access.

DIGITAL ASSET THEFT

Digital asset theft is the taking of an individual's assets through illegitimate means. This can be committed by hacking your wallet, tricking you into disclosing your private key or recovery seed, fraudulent play-to-earn games or manipulating you into transactions. Funds can also be stolen indirectly through the hacking of exchanges, lending platforms or decentralised applications.

Hacked wallets/accounts need to be identified promptly to avoid further losses. Log-in details should be changed and the hosting service should be notified. Ensure ties are cut off to other accounts including bank accounts and ensure a scan for malware is completed.

Fake giveaways are a common method of convincing individuals to send assets to criminals. Advertisements may be published by malicious groups; often in public spaces or on social media claiming to give away crypto if a transaction fee is paid. Sometimes these advertisements may divert to an illegitimate page. Details of wallets are also requested purportedly to send assets to which are then emptied by criminals.

Fake gaming applications are also used to steal cryptoassets through advertisement as 'play-to-earn' games where rewards are earned in exchange for an activity. Criminals incentivise this further by encouraging the storage of additional funds in the game's wallet to earn extra rewards. Fake rewards are accumulated and then either cannot be withdrawn or payment is requested for withdrawal.

If something sounds too good to be true, it probably is.

How to protect yourself:

- Be wary of publicising ownership of digital assets as this can make you a target. Ensure you store wallet details securely and don't keep all of your holdings in one place.
- Use a new email address and secure password for setting up wallet accounts to avoid compromises from your email and create a unique wallet for crypto-gaming.
- Use a third-party blockchain explorer to independently check balances of the addresses in your gaming wallets.
- Avoid clicking on links if you can't verify the destination path as these may divert to malicious websites.
- Keep your devices up to date with the latest security software and ensure all manufacturer's updates are completed.

CRYPTOJACKING

Cryptojacking is the unlawful hijacking of a computer to mine crypto without permission. The mining process is incredibly expensive because of the hardware needed and the large electricity costs to power it. Criminals cryptojack to save money.

Cryptojacking software is easier to use and harder to detect than traditional hacking software so is becoming more popular. Cryptojacking is carried out through downloading malware, hijacking IT infrastructure and accessing cloud services.

Criminals usually initiate their hacks via phishing whereby after the malicious link is followed, the program embeds itself within the device's hardware. This can infect computers, mobiles and servers as the scripts can move to other devices. Cryptojacking can also be carried out by infecting websites with a JavaScript code which auto-executes once loaded in the browser.

Cryptojacking can be detected by noticing decreased performance, hardware overheating, reduced battery life and an increase in Central Processing Unit (CPU) usage.

How to protect yourself:

- Monitor processing usage by the computer and if this is significantly higher than anticipated, run additional checks for cryptojacking software.
- Disable JavaScript when browsing online.
- Ensure all web browsers have the most recent updates installed and use an in-date ad blocker so the latest version of malware protection is used. Run regular malware scans and check for file changes.
- Be aware of and follow advice for protection against phishing **(see page 38)**.

PHISHING, SMISHING AND QUISHING

Phishing is a type of online crime where an individual is socially engineered into sharing personal information or data by a criminal pretending to be from a trustworthy source.

This type of crime is commonly committed via emails (phishing), text messages (smishing) or QR codes (quishing) containing links to fraudulent sites or applications which are designed to look legitimate. These often purport to be services that everyone uses such as banks or delivery companies so that they have common appeal. Phishing attacks are normally high-volume, mass communications which are sent to lots of people. Phishing attacks may or may not involve cryptoassets.

Spear-phishing is a sub-type of phishing where a criminal will target a specific person. Often the sender pretends to be a person the receiver knows such as a colleague or the company's IT department. They often pose as someone who you would trust with financial transactions or security. Criminals may research your social media profiles to find out information about you or may have obtained information from data-leaks to help them create trust or credibility.

If you receive a phishing email, forward it to **report@phishing.gov.uk** or if you receive a smishing text, forward it to **7726**. 7726 was chosen as it spells 'spam' on an alphanumeric phone keyboard. Sending texts to this number alerts your mobile phone provider to investigate the number and potentially block it if it's found to be a nuisance.

Advice on how to forward these messages from various devices can be found on the Ofcom website titled 'How to report scam texts and mobile calls to 7726'.

How to protect yourself:

- Don't respond to communications which you suspect may be phishing and report these to your provider or via the details provided on **page 38**.
- Check email addresses and phone numbers of the sender. It is relatively easy for criminals to purchase or spoof (imitate) numbers which appear as if they are from a trusted provider such as your bank, service provider or government agency. They may also set up email addresses which appear similar to official or corporate email addresses. Business emails which are not sent from an official domain, and instead come from free email providers such as Yahoo or Gmail instead, should be treated with caution.
- Check the spelling and grammar — fraudulent communications and websites sometimes include anomalies, for example using a zero instead of an 'o'.
- Be wary of unsolicited contact — consider whether you had contacted the individual or whether they've contacted you before verifying your details. A bank will never ask for your PIN numbers and they will already hold your customer records.
- Use a search engine to see if anyone has flagged the email address, website or phone number as malicious.
- Be wary of emails or messages which offer generic greetings such as 'Dear Customer'. Most companies will refer to you by your name and will often include your account number in communications. Fake 'unsubscribe' emails are often a common phishing tactic which are used by criminals. These divert to malicious websites to engineer you into inputting personal information.
- Ensure you use antivirus software and keep your browser up to date.

If you're a business, advice on how to protect your company against phishing attacks, including restricting administrator privileges, educating staff and checking your digital footprint, can be found on the National Cyber Security Centre website.

SPOOFING

Spoofing is the process of criminals disguising themselves to appear as though they're a known or trusted source. This technique is often used for emails, phone calls, websites or IP addresses to help convince you that the contact originates from somewhere it doesn't.

Some criminals will use phishing attacks to get through spam filters by putting malicious content in attachments. HTML or EXE attachments may install malware on your device so avoid clicking on unknown attachments.

DNS spoofing diverts victims from one website to another by changing the associated IP address. These secondary sites are often fraudulent and are used to obtain information or to inject malware into devices.

Caller ID and SMS spoofing services are designed to appear as though calls or text messages are coming from a trusted provider or geographic region. These often include links to malicious websites where personal information is obtained.

How to protect yourself:

- Check the validity of communications by logging into your accounts via official contact routes and not the ones supplied in the message or emails.
- Be wary of typosquatting which takes advantage of common typos people make while using the internet. Make sure you type in the correct address to avoid being diverted to malicious websites. Some criminals also attempt to make their sites appear genuine by using subtle differences in URLs, such as replacing the case of letters or using a different domain extension. This is purposefully not obvious to avoid detection.
- Hover your cursor over links before clicking them to verify the URL of the site and ensure after clicking that this is the site you were attempting to access.

MALWARE

The term malware refers to malicious software. This is designed to gain unauthorised access to computers or other connected devices and disrupt their normal operation or gather information from them. Malware pre-dates the use of digital assets but can also be used for stealing private key information or recovery seeds.

Malware can infect a computer or network from a number of sources including:

- Contaminated email attachments.
- Infected websites.
- Malicious files stored on external devices such as memory sticks.

Types of Malware:

Spyware

Spyware is designed to steal information about your activity on a computer or other device. Spyware can record screenshots, log keystrokes or even watch you through your webcam. This enables criminals to harvest inputted data, such as your wallet passphrases, and use it themselves.

Remote Access Trojans (RATs) are a type of spyware which allows a cyber criminal to remotely connect to infected devices and control them as if they were the authorised user. If individuals auto-save their passwords onto their browser, criminals would have instant access.

Virus/Worm

Viruses and worms infiltrate systems and then spread to infect others. Once on a system, they create copies of themselves and can then spread onto any other connected device.

Worms and viruses can also carry additional 'payloads' designed to perform harmful activity. This type of malware can rapidly cause widespread damage. Worms can enable attackers to create a network of hijacked machines (sometimes referred to as a botnet) which can be used in a distributed denial of services attack (DDoS). This can lead to individuals not being able to access services which include cryptoasset services such as wallets or exchanges.

Ransomware

Ransomware is a dangerous form of malware which enables cyber criminals to remotely lock-down files on a computer or device. This prevents the operator from accessing the files; making them unusable. Once the files have been locked, the criminal will make contact with you and offer to unlock them if you pay a ransom. Ransomware also pre-dates digital assets however it is becoming more common for demands of payment to be made in cryptoassets.

There is also a 'double extortion' method, where the criminal will, in addition to encrypting the data, also steal the data to provide additional leverage for the ransomware payment. If the ransom is not paid, the criminals will sell the stolen data or publish it online.

It is recommended that you do not pay ransomware demands. There is no guarantee that if ransoms are paid that you will get access to your data or that it won't be disseminated. Paying ransoms may also increase your changes of being targeted again.

How to protect yourself:

- **Use antivirus software.**

  Ensure antivirus software is installed on all of your applicable devices. This includes most smartphones, computers and servers. It will monitor for malware within the device's memory, processes and storage and alert you if any is found. Most antivirus software can remove malicious software it has detected and repair damage it may have caused.

- **Back up your data regularly.**

  Make regular backups of important work and data to a separate device such as a portable hard drive and check that backups have been successful. If possible, backups should be stored offline and in a safe place such as a fire-proof safe. If your computer is infected by malware such as ransomware, it can then be restored using the backup and any locked or lost data can be restored. Ideally, you should backup data to two separate locations, only one of which should be in the cloud.

- **Encrypt your data.**
  Make sure that your data, especially business critical, or data that has Personally Identifiable Information (PII) is encrypted at all times, especially when you're not using it. This way, if someone does manage to exfiltrate (steal) your data, they won't be able to read it or publish it as part of a ransomware attack.
- **Implement device control.**
  Prevent malware from infecting computers by restricting what devices can be connected to them such as USB drives and smartphones. These can carry malware which can transfer to the host computer when they are plugged in. Don't connect any unknown or untrusted device to your systems.

Device control

- **Don't follow links or open attachments in emails unless from a trusted source.**
  Opening links and attachments in emails may allow malicious software to be downloaded onto your system or device. Malware can be concealed in email attachments or downloaded from a malicious webpage. If you receive an email from an unknown source, or it's a trusted source but the email isn't like their usual email, don't click on any link without checking first. This also applies to messages on social media accounts such as Twitter or Instagram. There are occasions where personal accounts are hacked and used to deceive friends and colleagues by masquerading as the individual who owns the account. They can also further spread their control via contaminated links.

FINANCIAL EXPLOITATION

Money mules are individuals who move money on behalf of someone else; usually through their bank account or crypto wallet. Criminals need money mules to launder the profits of their crimes and this can also be through digital assets.

Criminals target individuals with advertisements detailing opportunities for easy ways to make money; often aiming this towards students who are looking for quick cash or those looking to work from home, flexibly or part-time.

Individuals are told to complete tasks including setting up new bank or crypto accounts, withdrawing cash or transferring money on behalf of others. The individual is ordinarily able to keep a certain amount of the assets for their help. Transferring criminal money is a crime which could result in a criminal conviction.

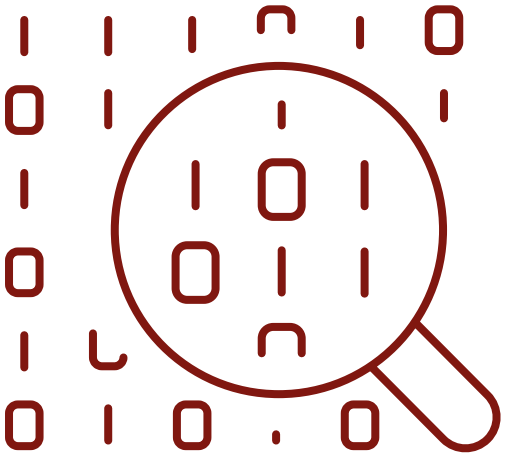
In order to avoid assisting criminals in hiding their illicit funds, you should be cautious when accepting online proposals to move money or assets for others, especially if you have not met them personally.

A legitimate business would almost always use a business email address rather than a personal one, so check who has contacted you and how they have got your details.

How to protect yourself:

- If an offer sounds too good to be true, it probably is.
- Be aware of unsolicited offers for easy money and of job offers where all of the interactions will be done online and you don't meet the employer in person.
- Treat job adverts with caution if they are written in poor English with spelling and grammatical errors.
- Watch out for offers of work which are made through social networking sites or encrypted messaging services.
- Research the wider company and make sure they are genuine. Legitimate business details can be found on Companies House or on official websites.
- Only provide your bank account or public key details to people you know and trust.

You can report financial exploitation to the Police on **101** or **999** in an emergency. You can also report it anonymously to Crimestoppers online or by calling **0800555111**.



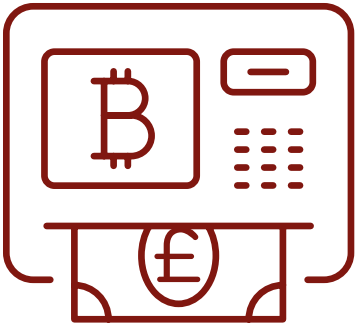
MONEY LAUNDERING — BITCOIN ATMS

Crypto-ATMs are stand-alone electronic kiosks which allow people to buy or convert fiat currency into cryptoassets. Not all of the Crypto-ATMs allow coins to be sold and some are limited to purchase only. The machines themselves charge high fees for use as commission.

If you have been offered a job opportunity requiring you to send assets or cash via an ATM, you may be the subject of financial exploitation.

Criminals also advertise cheap deals on online marketplaces and ask that you pay in crypto via an ATM. After the transaction has been made, the seller then disappears leaving you without remittance or the promised item. There is no central authority governing crypto payments, and the transactions are not reversible.

In the UK, Crypto-ATMs require registration with the Financial Conduct Authority to be able to operate legally. Those which begin operating before being registered are in breach of anti-money laundering regulations. Check with the FCA whether the machine is registered prior to making transactions.



NFTS

A NFT (Non Fungible Token) is a form of digital asset which represents ownership of an item. Unlike other crypto tokens or coins which are interchangeable and have the same value, each NFT is original. They are similar to having a digital collectible which can be bought, sold or traded. NFTs use distributed-ledger technology, typically on platforms like Ethereum, to confirm ownership and track the history of transactions.

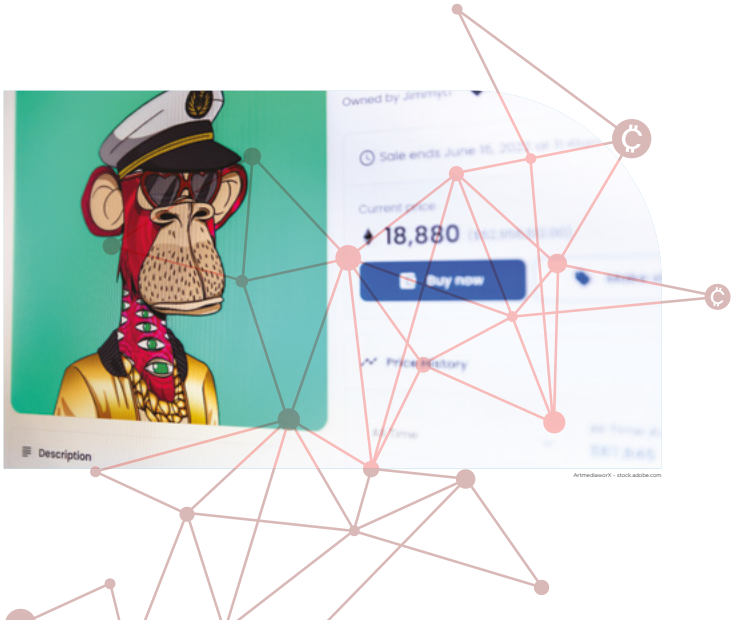
NFTs can be used in a variety of ways including:

- Digital Artwork.
- Profile pictures (PFPs).
- Gaming coins/currency.
- Music and videos.
- Ticketing.

NFTs were popularized in 2021 with the growth in collections such as CryptoPunks and Bored Ape Yacht Club. NFTs are represented on the blockchain by a smart contract and are secured through digital wallets in the same way as other cryptoassets. The wallet holds the cryptographic keys which prove ownership, allow transfer of the NFTs and facilitate the showcasing of a collection using compatible applications or platforms.

Video games have begun using NFTs as a method of in-game currency for players to purchase cosmetic items as well as in-game advantages. This is extremely popular amongst young people who play the games.

There is potential for NFTs to be used in fraud, money laundering and other financial crimes, in similar ways to other cryptoassets. Publicly displaying high-value or rare NFTs can make you susceptible to being targeted by criminals so take additional precautions if doing so, such as using secure crypto wallets and trading through reputable marketplaces.



TYPES OF NFT CRIME

Duplicates or website fraud — Criminals copy the original artwork and then create NFTs which aren't supported by the original artist. They can also create fraudulent websites which replicate original marketplaces.

How to protect yourself:

- Research the seller on a variety of platforms before purchasing and buy NFTs from verified sellers as even tokens listed on genuine sites can be fraudulent.
- Be wary of incorrect spellings within URLs or public usernames used on social media accounts for those trying to impersonate legitimate accounts or marketplaces. The URL of the site should have a valid certificate. You can check the validity of the certificate by viewing the site information from within the URL bar.

Rug Pulls, Pump and Dump and Wash Trading — As with crypto tokens, promoters try to create hype around an NFT collection to encourage investment; over-inflating the prices. After a number of people have invested, they withdraw and disappear which causes a rapid fall in the value of the NFT. This can also happen through the developers modifying the original code preventing resale.

How to protect yourself:

- Trust your instincts and question anything which sounds too good to be true.
- Watch out for sudden price surges and examine the number of trades in the transaction history.
- If fewer people are involved in the transactions, this could suggest the same people are buying and selling the assets to drive the price increase.
- Check the official website for a clear project roadmap of the NFT and research the past collections to see how they have performed so far. Influencer endorsement does not necessarily correlate with authenticity.
- 'Take Five' and consider if you feel pressured from hype to act quickly.

Giveaway or airdrop scams — Criminals may post details of giveaways on social media with website links. After clicking on the link, the user will often be asked to connect their wallet to claim the prize. The information entered can then be used to access the wallet and transfer the NFT to criminals.

How to protect yourself:

- Avoid clicking on links in pop-ups or emails where the legitimacy of the website can't be verified.
- Don't input details of your wallet or any passwords without verifying the legitimacy of the offer.
- Typically, you will be able to verify the details of large, trusted platforms on other sites. Be wary of sites which have detailed instructions on how to connect a wallet but have limited information on the roadmap or project. A large following does not necessarily make a site legitimate.
- Social media users often 'call out' what they believe to be a fraud. If others are hesitant to call the deal genuine, then it may be best to avoid it altogether.

Customer Support fraud — Criminals will purport to be technical staff on NFT marketplaces and will offer to resolve problems; asking for sensitive information in the process.

How to protect yourself:

- Customer services or technical support teams are unlikely to contact users via social media. Check who you're speaking to and contact the original platform if you're unsure.
- Never give out any personal information, especially wallet details, passwords, recovery seeds or security question information following unsolicited contact.
- Algorithms and Cookies may also make you susceptible to fraud as the more you are involved in looking at particular content, the more it is recommended for you.
- Watch out for those purporting to be customer support on closed Discord channels which target individuals interested in NFT content.

NFT Swap Scam — Some services allow individuals to trade NFTs. Often fraudsters will present themselves as legitimate traders to propose deals. The criminal will often suggest not to trade on the listing site but instead move to a different site. These secondary sites will often be fraudulent and assist in the criminal stealing the NFT or personal details after information has been input.

How to protect yourself:

- Be aware of trading on platforms which you were not previously aware of.
- Always check the URL for spelling to ensure the legitimacy of the website.
- Always be sceptical of NFT trades which the other party does not have in their wallet. Verify the transaction history of holdings prior to transfer.

Sleep-minting fraud — In Sleep-minting, criminals use another creator's wallet to create a fake NFT. They then transfer ownership of the NFT to themselves before listing it for sale. This gives the illusion that the original developer created the NFT.

Some criminals have also found ways to bypass the verification checks to present copied NFTs as genuine and can embed the verification mark to pass the automated checking process.

How to protect yourself:

- Examine the NFT metadata and read the transaction history.
- Consider messaging the creator about authenticity if you're suspicious and follow creators on social media for details about official drops.

Phishing — For NFTs, phishing attacks often involve fake representatives of wallet providers attempting to engineer you to verify your wallet's private key or passphrase.

How to protect yourself:

- Avoid clicking on unfamiliar attachments or following links after unsolicited contact. For large transactions, verify the legitimacy of transfers through a separate communication channel to make sure this has been confirmed.
- Never give out your wallet's private key and be wary about who you are providing personal information to.

REPORTING & FURTHER ADVICE

REPORTING FRAUD, CRYPTO AND CYBER CRIME

If you think you have uncovered a crime, have been targeted or have become a victim, there are many authorities you can contact for advice or to make a report.

This isn't your fault — criminals are skilled at targeting us.

In the first instance, you should contact your bank immediately on a number you know to be correct such as the one listed on your statement, their website or on the back of your debit or credit card.

Report cybercrime and fraud in the UK to Action Fraud, either online at **actionfraud.police.uk** or by telephone on **0300 123 2040**. If you are deaf or hard of hearing you can use textphone **0300 123 2050**.

If you are in Scotland, please report to Police Scotland directly by calling **101** or Advice Direct Scotland on **0808 164 6400**.

Every report assists police investigations, provides intelligence, informs national alerts that protect all communities, disrupts criminals and reduces harm.

In the UK you can forward smishing text messages to OFCOM on **7726** (free of charge) and forward suspicious emails to **report@phishing.gov.uk**

Don't forget to share your experience with friends and family to make them more aware.

FURTHER ADVICE

Below is a list of websites that you may find useful for further support and advice:

Action Fraud

Action Fraud is the UK's national reporting centre for fraud and cyber crime. If you have been the victim of these types of crime, you should report the incident directly to Action Fraud by telephone or via their website. The Action Fraud website also has up to date information on numerous types of fraud and cyber crime and details of how to protect yourself when online — **actionfraud.police.uk**

Cifas

UK fraud prevention service Cifas offers Protective Registration to people who have fallen victim to, or are at risk of, identity theft. This service flags your personal file so that when Cifas member companies receive an application in your name, they'll conduct extra checks to ensure the application is genuine — **cifas.org.uk**

Cyber Aware

Cyber Aware (formerly Cyber Streetwise) provides cyber security advice for small businesses and individuals, such as using strong passwords made up of 'three random words' and always downloading the latest software and app updates, which can help you protect your devices from cyber criminals. It's guidance is based on expert advice from the National Cyber Security Centre, a part of GCHQ — **cyberaware.gov.uk**

Cyber Choices

The Cyber Choices network was created to help people make informed choices and to use their cyber skills in a legal way. The programme is a national initiative co-ordinated by the National Crime Agency and delivered by Cyber Choices teams within Regional Organised Crime Units and Local Police Force Cyber Teams — **cyberchoices.co.uk**

Cyber Helpline

The Cyber Helpline provides free advice and support to individuals in the UK aged 13 or over, and sole traders, on how to recover from cyber security attacks. They provide chatbot and volunteer services as well as a number of guides — **thecyberhelpline.com**

Financial Conduct Authority

The Financial Conduct Authority's aim is to make financial markets work well so that consumers get a fair deal. They regulate the conduct of thousands of companies within the financial sector including some of those related to digital assets. They also operate an investment and pensions fraud warnings list of companies to avoid and a reporting tool for unauthorised firms. They can be contacted via their website; **fca.org.uk** or by calling **0800 111 6768**. Their ScamSmart tool can be accessed at **fca.org.uk/scamsmart**

Financial Ombudsman Service

The Financial Ombudsman Service is a free and easy-to-use service that settles complaints between consumers and businesses who provide financial services. They resolve disputes fairly and impartially including frauds and investments — **financial-ombudsman.org.uk**

Financial Service Compensation Scheme (FSCS)

The FSCS protects the customers of financial services firms which have failed. They provide free compensation claims advice through an online claims service to individuals who are eligible under the FSCS compensation rules. These are set by the UK services regulators; the Financial Conduct Authority and the Prudential Regulation Authority — **fscs.org.uk**

Get Safe Online

Get Safe Online is a leading internet safety website which provides easy-to-understand information about online safety. Their website is a unique resource providing practical advice on how to protect yourself and your business against common types of cyber crime, guidance on performing backups and data protection as well as a number of articles on crypto — **getsafeonline.org**

Have I Been Pwned?

"Have I Been Pwned?" (an online gamer term) is a free website for businesses and individuals to check to see if an email address has been involved in any data breaches. By typing in an email address, you can see if and when it was involved in any data breach, and where that breach occurred. This can help people see if their email or password has been made public, and to ensure passwords are changed — **haveibeenpwned.com**

National Crime Agency (NCA)

The NCA leads the UK law enforcements' fight to cut serious and organised crime. Their website contains information regarding current crime threats and online safety guidance for businesses — **nationalcrimeagency.gov.uk**

National Cyber Security Centre (NCSC)

The NCSC is part of GCHQ and is the UK's lead authority on cyber security. The NCSC's main purpose is to increase cyber security and cyber resilience. It works with UK organisations, businesses and individuals to provide authoritative and coherent cyber security advice and cyber incident management, underpinned by world class research and innovation. NCSC also provides incident response to minimise harm to the UK, help with recovery and learn lessons for the future — **ncsc.gov.uk**

No More Ransom

The "No More Ransom" website is an initiative by the National High Tech Crime Unit of the Netherlands Police, Europol's European Cyber Crime Centre and private cyber security companies. Its goal is helping victims of ransomware retrieve their encrypted data, without having to pay the criminals. Since it's much easier to avoid the threat than to fight against it once the system is affected, the project also aims to educate users about how ransomware works and what countermeasures can be taken to effectively prevent infection. It can be accessed via **nomoreransom.org**

NI Trading Standards Service

The Trading Standards Service is responsible for enforcing legislation covering a wide breadth of sectors and practices including: scams and e-crime, doorstep crime & home improvement services and false or misleading descriptions of good and services. To report a matter to the Trading Standards Service contact Consumerline on **0300 123 6262** or visit **nidirect.gov.uk/consumerline**

Northern Ireland Cyber Security Centre (NICSC)

The NICSC work to make Northern Ireland cyber safe, secure and resilient. NICSC work with public, private, third sector organisations and citizens to improve their ability to defend against cyber attacks, increase their knowledge of cyber threats, and become more cyber resilient — **nicybersecuritycentre.gov.uk**

UK Finance

UK Finance is the trade association representing the banking and finance industry operating in the UK. It represents more than 250 firms in the UK providing credit, banking, markets and payment related services. Their website contains a wealth of information on how you can protect yourself and your business from fraud and cyber crime.

Part of UK Finance's campaign is Take Five to Stop Fraud which urges people to stop and consider whether the situation is genuine and think if what they're being told really makes sense. They can be contacted via **ukfinance.org.uk** or through the campaign website **takefive-stopfraud.org.uk**

Victim Support NI

Victim Support NI is the leading independent charity supporting victims of all crime types in Northern Ireland. They offer practical and emotional support to help victims recover from the impact of crime. They also support victims and witnesses at court through their Witness Service. Their services are free and confidential and are available throughout Northern Ireland. Contact Victim Support NI through their Belfast or Foyle Hubs on **028 9024 3133** or **028 7137 0086** or via email **info@victimsupportni.org.uk**. More information can be found at **victimsupportni.com**

CONTACT US — POLICE SERVICE OF NORTHERN IRELAND

In an emergency, always dial **999** and to report non-emergency incidents to the police call **101**. Further information about reporting crime can be found on our website **psni.police.uk/report**

The Police Service of Northern Ireland provide services free of charge to help protect organisations and businesses from cyber crime — **psni.police.uk/cyber-protect**

The fraud pages of the Police Service of Northern Ireland website also provide information to assist in combating fraud and other economic crime — **psni.police.uk/scams-and-fraud**

The Little Media Series is a repository of all the booklets, leaflets and videos created by the Metropolitan Police to help raise awareness around fraud and cyber crime — **met.police.uk/littlemedia**

Police Service of Northern Ireland

STOP! THINK FRAUD
NATIONAL CAMPAIGN AGAINST FRAUD