Fraud SMART

Protect Yourself from **Financial Fraud**

www.FraudSMART.ie

Banking & Payment Federation Ireland

supported by

Led by Banking & Payments Federation Ireland, FraudSMART is a joint initiative developed by the banking sector. Sign up on www.FraudSMART.ie for alerts on current fraud trends that may impact your business.

Contents

Top tips to Prevent Fraud 5

Phone Scams 6

SMS/Text Message Fraud - Smishing 10

Email Scams 12

Online Fraud 14

Online Shopping Fraud 16

Social Media Scams 18

Social Media – Social Engineering – Your Data 20

Safe Online & Mobile Banking 22

Identity Theft 24

Card Fraud 26

Distraction Fraud 28

Cheque Fraud 30

Money Mules 31

Fake Advertising and Other Scams 32

What to do if you are a victim of fraud? 34

FraudSMART

Most people would believe that they are fraud savvy however fraudsters are more sophisticated than ever, and we need to do more to protect ourselves from becoming victims of fraud.

While most financial frauds still use phone, texts and emails to commit the crime, the frauds themselves are increasingly clever using technology and publicly available information to trick you. You are likely to get an email or a phone call from somebody you "know" and "trust" or shop on a website that looks legitimate.

FraudSMART is a fraud prevention initiative which aims to raise consumer and business awareness of the latest financial fraud activity and provide simple advice on how best you can protect yourself and your money. Consumers can log onto www.FraudSMART.ie for a wide range of information and advice on the latest frauds and how to avoid being scammed.

Led by Banking & Payments Federation Ireland, FraudSMART is a joint initiative developed by the banking sector. Sign up on www.FraudSMART.ie for alerts on current fraud trends.

www.FraudSMART.ie
@FraudSMART
@FraudSMART

Top Tips to Prevent Fraud

Be Informed

- Stay in control, don't be rushed and make a decision you will regret.
- Don't assume you can trust caller ID. Phone numbers can be spoofed so it looks like your bank is calling.
- Fraudsters may already have basic information about you in their possession (e.g. name, address, date of birth) do not assume a caller is genuine because they have these details.

Be Alert

- To unexpected/unsolicited emails, telephone calls or texts. Always independently check the person is who they say they are.
- Always check your statements, and if you notice any unusual transactions, report them to your bank immediately.

Be Secure

- Take your time to do the relevant checks and independently verify any requests.
- Never give your security details such a full banking password, code/login details or PIN to anyone.
- Never use public Wi-Fi to make an online payment or access your online banking, use your 3G/4G connection instead.

Phone Scams

Vishing

Vishing (Voice and Phishing) is a phone scam where fraudsters target you by calling and claiming to be your bank or service provider e.g. computer support looking to "upgrade your system" or fix a problem.

Fraudsters trick you into divulging personal, financial or security information or into making a financial transfer to them. Information they look for includes debit or credit card details, PIN number, online banking details, password and personal details - name, address and date of birth. This information can be used to access your bank account or carry out transactions with your card.

Phone scam techniques

It has been reported that fraudsters may encourage you to check their identity or to make a report to the Gardaí/Police. When you hang up your landline, the fraudster holds the line open (by not hanging up). You then pick up the phone again to ring the genuine company or the Gardaí/Police but you are still talking to the fraudster.

Persuasion
even if you are tech savvy fraudsters are smooth talkers

Urgency
vishers utilise fear tactics pressuring you into thinking you must act quickly as your money is in danger

Personal Info
can be bought from hacked company data or found on your social media/ website

Phone Spoofing
Phone numbers/IDs can be faked to hide the origin of the call

Environment
criminals can play sound effects to make it sound like they are in a call centre

Types of Phone Scams:

Money Transfer Scam

- The fraudster calls you unexpectedly posing as your bank. They tell you that there is a problem such as irregular activity or fraud on your account.
- They advise you to transfer money out of your account to a so-called "safe account", indicating that once the problem is resolved the money will be transferred back.
- They give account details and tell you to transfer money, usually via a money transfer or wire which involves going to the premises of a Money Transfer Agent e.g. Post Office, Western Union or Money Gram. They use rush tactics, saying it needs to be done immediately, often targeting older individuals.

Technical Support Scam

- The fraudster calls you unexpectedly posing as computer/ broadband support. They tell you that there is a problem with your computer, modem or internet connection e.g. virus or software update.
- To "fix this" they say they need to gain access to your computer and talk you through steps that will fix the problem.
- They use this opportunity to download malicious software (malware) on to your computer that will track your online activity and pass personal, financial or security information to the fraudster.
- Fraudsters use familiar names such as "Microsoft", "Windows" or "Apple" to make them sound more credible and even piggy-back on known technical problems that have gained media attention.

Be Informed

- Never give personal information unless you have validated that the caller is a genuine representative of where they claim to represent:
  - Advise the caller you will call them back once you validate their identity.
  - Hang-up and look up the number independently using the phone book or website, NEVER use a number given to you by the caller.
  - Make sure you hear a dial tone before you dial.
  - If the caller is genuine they will understand your need to validate them.

Be Alert

- Be wary of unsolicited calls especially from your bank.
- Remember it takes two people to terminate a landline phone call; you can use a different phone line to check the caller's identity.
- Fraudsters may already have basic information about you in their possession (e.g. name, address, account details), do not assume a caller is genuine because they have these details.

Be Secure

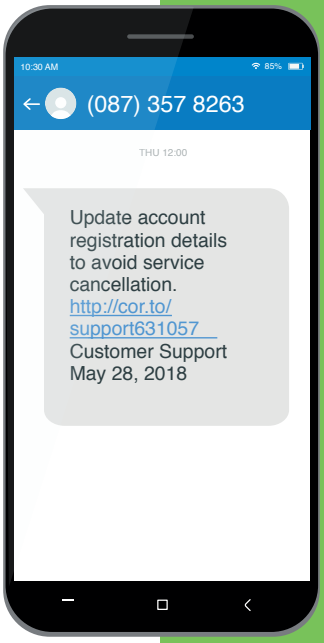
- Don't assume you can trust caller ID. Fraudsters can spoof their numbers so it looks like they are calling from a particular company or bank, even when they're not.
- Your bank or the Gardaí/Police will never ask you for your credit or debit card PIN number or full online banking password.
- Your bank will never ask you to transfer money to another account, even if they say it is for safekeeping.
- Don't allow yourself to be rushed. Take your time and do the relevant checks. The caller may try make you feel foolish or negligent if you don't follow their instructions.

SMS/Text Message Fraud – Smishing

Smishing is where fraudsters send text messages claiming to come from a reputable organisation such as a bank, Revenue or a service provider e.g. a mobile phone company.

The message will typically ask you to click on a link to a website or to call a phone number to "verify", "update" or to "reactivate" your account. The website is a fake one and the phone number leads to a fraudster pretending to be the company. They then attempt to get you to disclose personal, financial or security information, which will be used to steal your money.

The messages often attempt to alarm you, claiming that urgent action is needed, or it will have negative consequences.



65% of people said they could have prevented fraud by checking the legitimacy of unexpected emails/texts before clicking on links within them

Be Informed

- A text from your bank will not ask you for any personal information, only ever respond Y or N to bank text messages.
- Never respond to a text message that requests your 4-digit card PIN or your online banking details or any other password.
- Do not respond to unsolicited text/SMS messages before independently validating the text is from who it says it's from by:
    - Looking up the organisation's phone number using the phone book or their website and making direct contact with them.
    - Do not use the phone number in the text as it could be a fake number.

Be Alert

- Don't be rushed. Take your time and make the appropriate checks before responding.

Be Secure

- Do not click on a link, attachment or image that you receive in an unsolicited text without first verifying the text and understanding what you are clicking on.
- If you think you have responded to a Smishing text message, contact your bank immediately.

Email Scams

Fraudsters target potential victims by sending fake emails that look like they are from a reputable company or your bank. These emails are 'phishing' for information such as your bank details, usernames, or passwords. They will urge you to click on a link and enter your personal and financial details into a fake website that will look like a genuine website.

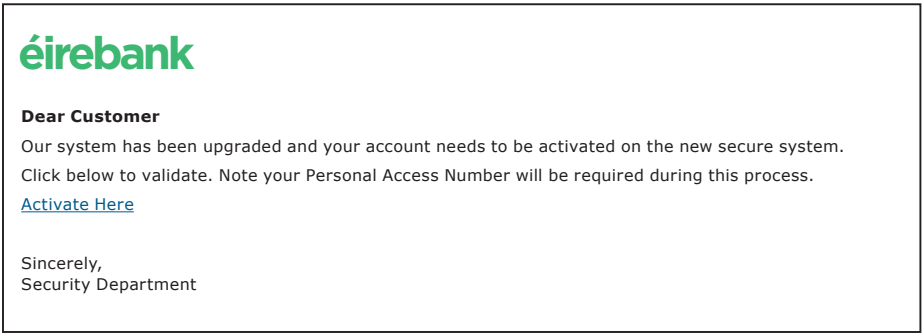
52% of people said they could have prevented fraud by not opening email attachments until they independently verified the email was from the company that sent it

Phishing emails characteristics

- Convey a sense of urgency asking you to "verify", "update" or "reactivate" your account.
- May indicate that something is wrong and if you don't act immediately it will have negative consequences e.g. that money will be lost or that there is fraud on your account. The fraudsters don't want to give you time to investigate if the email is legitimate.
- Promise money – asking you to submit your details for a refund, eg. a credit for an unexpected revenue refund.
- Include a link or attachment that when clicked, downloads malicious software on to your PC or device which is used to track your online activity and record your financial, personal or security information.
- Contain a link that brings you to a fake website where you are asked to input your financial or security information. The website will look almost identical to the real thing including logos and branding.
- Tend to have generic greetings such as "Dear Customer" or "Account Holder".
- The fraudster might have some details about you (often found on social media) such as your name or your birthday.

Be Informed

- Never respond to any unsolicited emails/click on links until you have verified the source.
- Do not do this using the contact information in the email. Look up this information yourself.
- Never give away personal information or security details such as your PIN or full online banking password to anyone.
- Don't allow yourself to be rushed. Take your time and do the relevant checks.



éirebank

Dear Customer

Our system has been upgraded and your account needs to be activated on the new secure system.

Click below to validate. Note your Personal Access Number will be required during this process.

Activate Here

Sincerely,
Security Department

Be Alert

- Be wary of payment requests that are unexpected or irregular, whatever the amount involved. If in any doubt, do not make the payment, however urgent it may seem or whatever the suggested outcome(s).
- Fraudsters can change an email address to make it look like it has come from a legitimate source. Look out for different contact numbers and/or a slight change in the email address e.g. '.com' instead of '.ie'
- Be wary of emails that don't use your name and use generic greetings like 'Dear Customer' or 'Dear Sir/Madam'.

Be Secure

- Do not open or forward emails that you think may be spam. Take heed of any messages that appear in your browser alerting you to a possible attack or suspect website.
- Limit or restrict personal information you share across all social media platforms.
- Remember card issuers and banks will never ask for PIN, full security credentials or account information.

Online Fraud

The internet is part of our daily lives for shopping, banking and connecting socially but it also allows fraudsters to defraud and take financial advantage of you from a distance reducing their chances of being caught. They do this by accessing your online banking or by enticing you to transfer money with false offers and using your card details.

Be Informed

- When shopping or making a payment online, make sure your internet access is secured – the beginning of the website should be 'https' indicating a secure connection.

- Look for the padlock – when you click on the security icon (padlock or unbroken key symbol) the link should describe the type of security and encryption being used.
- Never use unsecured public wi-fi networks or hotspots to make a payment or access your online banking. Use a 3G or 4G internet connection.

Be Alert

- Be cautious of emails with special offers. Generally, if it sounds too good to be true then it probably is.
- Heed your own instincts – if you have any doubts about giving out your card details, end the transaction and purchase your goods elsewhere.
- Do not click on pop ups or adverts that state that you have won a prize or adverts on social media.

Be Secure

- Install reliable and trusted antivirus and browser security software. Regularly install updates and ensure there is a regular malware scan.
- Remember your information is valuable to a fraudster. Use appropriate privacy settings on your social media profiles.
- Be password savvy – use a different password to your network or computer logon to the one that is used for online orders or retailer accounts. Avoid using your address, date of birth or phone number. The best passwords are alpha-numeric (using letters and numbers) and at least eight characters in length.

Online Shopping Fraud

Online shopping is easy and convenient, can offer you greater choice and help you find the very best deals.

75% of all card fraud occurs online. Know how to shop safely online and be secure.

Be Informed

- Do your research. Find out as much as you can about the retailer before you purchase. Use websites that your friends and colleagues have used before or that you have heard about through trusted sources.
- Keep a record of your purchase, print or save a copy of your order.
- Read the Terms and Conditions. Make sure there are no commitments such as a series of recurring payments.
- Pay attention to free trials that ask for your credit/debit card, paid subscriptions can kick in automatically at the end of the free trial.

Be Alert

- Use a secure website. The website address should be 'https' before the purchase is made. The 's' indicates a secure connection.
- Look for the padlock – the security symbol should be a padlock/ unbroken key. Clicking on it will describe the security and encryption.
- Be cautious about emails claiming outrageous offers or online adverts. Generally, if it sounds too good to be true, it probably is.

Be Secure

- Install reliable and trusted antivirus and browser security software. Regularly install updates and ensure there is a regular malware scan.
- Check that the highest level of security notification and monitoring is activated on your computer, these are not always default.
- Be password savvy – the best passwords are alpha-numeric and at least eight characters.
- 3D Secure – this is available for MasterCard and Visa cardholders to protect against unauthorised online transactions. It enables you to verify that you are the cardholder using a password like using a PIN at a point of sale. Contact your bank/card issuer to find out about registering for 3D Secure.

Social Media Scams

Social media is great for sharing information, searching topics and products and connecting with people. However, it also provides criminals with an opportunity to blend in with the crowd and entice unsuspecting individuals to interact with them with the goal of stealing their personal, financial or security information.

- **Twishing** – is a form of phishing in which a message is sent to you on Twitter to obtain your personal or security information by directing you to a bogus website.
- **Fake comments on popular posts** – fraudsters post fake comments on popular posts that include interesting looking links which in fact direct you to phishing websites.
- **'Help, I'm in Trouble' messages from genuine friends** – beware of posts or emails from friends saying they are in trouble and need you to send money. It is very likely that their social media or email accounts have been hacked.
- **Miracle Products** – beware miracle beauty or health products that offer a free trial but involve giving your credit or debit card details up front. If the product is genuine, you are often tied unknowingly into a fixed period contract. Read the terms and conditions carefully.

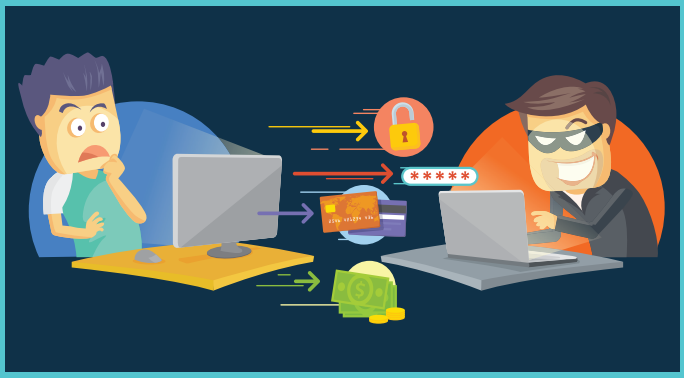
31% of Irish consumers have experienced online scams including profile hacking and fake links.

- **Job/Work from Home Scams** – some of these opportunities involve payment up front for training, products etc. so always independently check out the credentials of any company offering you a job or work from home opportunity. Never give your account or card details until you are confident this is a legitimate offer.

- **Romance Scams** – fake online profiles and persona are designed to lure you in and, after "wooing you", they will find some compelling reason to ask for money, gifts or your card details. They may use a fictional name or falsely take on the identities of real, trusted people such as military personnel, aid workers or professionals working abroad.

Social Media - Social Engineering Your Data

Fraudsters use social media to build up your profile and potentially steal your identity or use it as part of a phishing or vishing scam to make you believe they are who they are pretending to be e.g. calling pretending to be your bank, using your name and other information they have gathered online to build your trust convincing you to divulge other personal and financial information. This is known as Social Engineering.



Be very cautious about what information you post on social media. Think of security questions e.g. mother's maiden name, where you work, where you went to school, birthday messages = date of birth. The fraudster can build up a profile through various social media channels to build a picture of your identity.

Be Informed

- Do not give out personal information in response to a posting e.g. by taking quizzes or signing up for offers that ask for your personal details.
- Never give your card details or make a payment on a special offer on social media unless you have verified it is legitimate.
- Be mindful of information you share on social media e.g. your birthday posts, your family members, your workplace – individually they mean nothing but altogether they start to build your profile.

Be Alert

- Do not 'friend' or link with someone you don't know.
- If you get a request from a friend that seems unusual, e.g. a request for money or a friend request from somebody you're already friends with contact them by another independent method.
- Fake Friend Requests – Only accept friend requests from people you know or have reason to want to connect with you. Criminals often use fake friend requests to gather you and your friends' data.

Be Secure

- Use appropriate privacy settings on your social media profiles – your information is valuable to fraudsters who use it to build up your profile.
- If a link appears on your social media page and you don't recognize it or want anything to do with it, delete it immediately.
- Change your password regularly.

Safe Online & Mobile Banking

Internet and mobile banking are a very convenient and efficient way to conduct your banking needs. With an increasing number of attempts by fraudsters to gain access to customers' money, it is important that you protect yourself against online threats

Be Informed

- Never disclose your security details, PIN, full online banking or personal information in response to an email, phone call or letter claiming to be from your bank or other financial institution. Your bank would never ask you to disclose these.
- Your bank will never send you an email with a link to a page that asks you to enter your online banking details.
- Only ever visit your bank's website by entering the address into your browser or using a bookmark you have created using the correct address.

Be Alert

- Be aware of 'shoulder surfers' viewing your screen.
- Always check your statements, and if you notice any unusual transactions, report them immediately.
- Always log out of internet banking sessions once you have finished.

Be Secure

- Never use public Wi-Fi for online banking. Use a 3G/4G connection.
- Look for 'https' at the beginning of the address and the padlock symbol in the browser frame.
- Ensure you have effective and updated antivirus/antispyware software and firewall running before you log in to your bank account.
- Regularly clear your browser's cache – some mobile devices store copies of web pages that may contain banking information.
- Only download banking apps from official App stores.

Identity Theft

Identity theft occurs when your personal details such as your PPS number, driving licence and banking details are compromised or stolen allowing fraudsters to pose as you.

This allows fraudsters to use your information to obtain credit or to purchase goods or services in your name, take over your bank account or to make applications in your name for new bank accounts, cards or loans.

One of the biggest problems with identity theft is that the crimes committed by the fraudster can often be attributed to you. If this happens, you may have difficulty applying for loans, cards or a mortgage until the matter is sorted out. You should carefully guard any personal information that might allow a thief to impersonate you.

Always

- Keep important personal documents such as your passport, birth certificate, payment cards and cheque books in a safe and secure place.
- Limit/restrict how much personal information you share or divulge on social networking sites.
- Shred or destroy any documents containing personal information before disposing of them.
- Regularly check your bank and credit card statements, report any unfamiliar or unusual transactions to your bank immediately.
- Report lost and stolen cards or suspected fraudulent use of your account to your bank or financial institution immediately.

Never

- Never give your credit card or online account details or copies of personal documents to anyone you don't know or trust.
- Never disclose your card PIN or your full online banking password to anyone.

Card Fraud

While credit and debit cards are a very safe way to pay for goods or services or to withdraw cash, it is important to take the necessary precautions to ensure that your card details are kept safe.

Most Irish and European issued payment cards now use "Chip and PIN" technology that helps prevent the physical card being counterfeited and used fraudulently. However, some countries have not yet introduced "Chip and PIN" which means that Irish cards can still be counterfeited and used to make fraudulent ATM withdrawals or pay for goods and services in some countries outside Europe.

Also, card data such as card number, expiry date, CVV and 3D Secure information is a valuable commodity to criminals and can be bought by and sold to other criminals. This data is used to make fraudulent online purchases, often for highly re-saleable goods that can quickly be turned into cash.

Counterfeit Fraud

Counterfeit fraud occurs when a fraudster skims or copies the data held on the magnetic stripe of a legitimate credit or debit card and uses this data to create a fake plastic card, which contains the real cards details. This card is then used to purchase goods or services or to withdraw cash at ATMs in countries that have not yet implemented "Chip and PIN" technology.

Card Skimming

Card skimming can occur by means of a small handheld skimming device when the cardholder is paying for goods and services. It can also happen at ATMs if a criminal attaches a skimming device to the ATM machine. For skimmed card data to be of greatest use to the criminal, they also need to know the PIN number for the card.

Distraction Fraud

Distraction fraud is a method fraudsters use to steal your credit/debit card after viewing your PIN number. It generally involves two fraudsters and can take place at an ATM or after you have entered your PIN at a point of sale e.g. in a supermarket.

Supermarket

While paying in a supermarket the person behind you watches you put your PIN into the machine. Outside in the carpark while you put your shopping away another person, the fraudster's accomplice, stops you and asks you for directions and while you are distracted your bag/wallet is stolen. The fraudsters now have your PIN and your card.

Card Swap

This is when a customer is at the ATM, the person behind them watches them enter their PIN number. Then as the victim goes to take the money the fraudster distracts them, and another person swaps the card for a fake card. The victim takes the card and then their cash not realising it is a fake card and now the fraudsters have the real card and the PIN.

Nightclub/Bar Distraction Fraud

Similar to the supermarket distraction, a fraudster watches you enter your PIN while paying for drinks. Your bag/wallet gets stolen at a point in time after this and they now have your card and your PIN.

ATM/Branch Distraction Fraud

The fraudster or an accomplice watch you keying in your PIN at an ATM and then distract you before the transaction is finished for example by saying you have dropped money. When you look around they grab your card from the machine and in the confusion you may think you have taken it back yourself. They now have your card and PIN.

Be wary of being distracted shortly after you have made an ATM transaction/card payment. If you are, check for your card immediately and if missing contact your bank straight away.

Be Alert

- Check your account regularly and report any suspicious or unrecognised transactions immediately.
- If you do not protect your payment card or PIN, or if you give them to someone else, you may be held liable for any unauthorised transactions.
- Be cautious about emails claiming outrageous offers or online adverts. Generally, if it sounds too good to be true, it probably is.

Be Informed

- If you are expecting a card or PIN in the post and it does not arrive, notify your card issuer immediately.
- Sign any new cards as soon as they arrive from your bank or card issuer. Cut up old cards as soon as the new one becomes valid.
- To prevent new cards or PINs being intercepted in the post be mindful of leaving post sitting in a mailbox especially if you live in an apartment block where other people may have access to the boxes or if you are away for a period of time.

Be Secure

- Keep your card in sight when paying. Go with the staff member to the point of sale.
- Your PIN is the most valuable piece of information to a fraudster, it is vital to shield it when you are paying for goods and services. This includes at ATMs, Point of Sales and carpark machines. Watch out for 'shoulder surfers' and being distracted during and after the transaction.
- Keep your card safe and report to your bank immediately if its lost or stolen.

Cheque Fraud

Although cheque usage in Ireland has declined significantly, fraudsters continue to use cheques as a means to make money and defraud customers.

Be Informed

- When sending cheques in the post, send securely and avoid using window envelopes.
- Cross all cheques 'a/c payee' only'.

Be Alert

- Ensure all issued cheques and unused cheque numbers are accounted for. Check this when you get a new cheque book and review regularly to ensure no cheques are missing.

Be Secure

- Keep cheques in a secure place.
- Control who has access to your cheque book.
- Do not sign cheques in advance.

Money Mules

Money Mules are people recruited by fraudsters to help transfer stolen or fraudulently obtained money from bank accounts. Money Mules can also be known as 'money transfer agents'. Fraudsters recruit Money Mules in many ways:

- Targeting students in schools and colleges offering money in return for lodging cash/cheque into their account, often using the excuse that they cannot open an account themselves.
- Posing as employers with job vacancies advertised online or in local newspapers. Often the only requirement is to have a bank account. The mule accepts the 'job' and in doing so becomes involved in money laundering, which is a criminal activity.

Once recruited, a Money Mule receives stolen funds into their account, this is followed by a request to transfer/forward the funds, minus their commission, usually overseas using a money/wire transfer service. The money the mule is transferring is stolen, and what they are doing is called money laundering. Those who become involved in money muling are involved in criminal activity and can be prosecuted.

Be Informed

- Research any work-from-home opportunities to ensure it is a legitimate business.
- Verify any company that makes you a job offer, check their contact details (address, landline phone number, email address and website) – try calling the landline.
- Never accept payment for use of your bank account.

Be Alert

- Be wary of unsolicited offers or opportunities to make easy money.
- Be particularly cautious of offers from people or companies overseas as it is difficult to verify their legitimacy.

Be Secure

- Never give your bank account details to anyone unless you know and trust them.
- Never allow your bank account to be used by someone else.

Fake Advertising & Other Scams

There are different ways of tricking individuals into transferring money or getting access to personal data. Criminals will often pose as sellers of highly desirable products or services such as event tickets, mobile phones or designer sportswear. These adverts/ scams can pop up while you are browsing online, show on your social media news feed, be sent to you in an email or post or even be in a newspaper or public place. Here are some of the most common scams to be aware of.

Career Opportunity Scams

The fraudster contacts you directly or through social media claiming to be an employer or recruitment agency who is considering you for a position, which is usually abroad. You fill in an application form and may even be given a phone interview. A job offer is then made and the fraudster suggests organising travel arrangements, accommodation, visa etc. on your behalf. To progress with this, you need to pay an upfront fee. Needless to say, no arrangements are made and there is no job.

Work-from-home Scams

Always be wary of any unexpected opportunities that offer you easy money e.g. lots of money for doing easy part-time work from your own home, especially if you must give money up front in order to avail of the opportunity. Work-from-home scams often ask you to pay an advance fee up front for insurance, training or products, which you never receive or are worthless. Independently check out any potential employer or job opportunity.

Rental Fraud

A potential tenant is tricked into paying a deposit for a property. In reality, the property does not exist or if it does, has already been rented, often to multiple people. This fraud usually targets people who are trying to rent in another country or those trying to rent in Ireland from abroad. Students can be a target at certain times of the year when properties are scarce and in desperation people place a deposit on a property before seeing it.

Ticket Scams

Criminals often take advantage of ticketed events, especially if sold out, such as concerts, festivals, sporting events and live comedy. You buy your ticket online from a private seller or from what looks like a website or agent for the event. You pay your money but either the tickets never arrive, or they turn out to be fake.

Miracle Products

Adverts selling miracle health or beauty products are common particularly on social media and through online advertising. They claim miraculous benefits and they offer you a free trial. All you have to do is to pay for post and packaging or for insurance, but once they have your card details you could end up paying for a lot more. In some cases you will receive nothing in return, in others you'll receive a product but it doesn't do what you expected and you find that you have inadvertently signed up to an ongoing contract that is difficult to get out of.

Fake Antivirus

There is a growing trend whereby criminals pose as companies offering antivirus or anti-spyware software. You may find an alert popping up on your computer or device saying that it is infected with malware and that you can download this software to fix the problem. In reality the software that is downloaded is the virus or spyware.

Mobile Phone Fraud

Beware of people selling highly attractive products especially if the prices are too good to be true. Criminals tempt you to part with your money by posing as sellers of highly desirable goods. Having parted with your money you receive no product or at best a sub-standard one.

What to do if you are a victim of fraud?

If you suspect you have been the victim of fraud or have noticed unusual activity on your bank account, contact your bank immediately and also report to your local Garda Station. Fraudsters move fast; the quicker you contact your bank to safeguard your accounts the better.

AIB	**Internet Banking Transactions:** From Outside ROI **AIB Debit/Credit Card Transactions:** **iBusiness Banking Transactions:** From Outside ROI Opening Hours: Mon-Fri 08.30 – 17.30	0818 724 724 +353 1 771 2424 01 668 5500 0818 720 000 +353 1 641 4889
Avant Money	**Customer Service*** Avant Money Credit Cards Outside of Ireland Fraud Notifications **Customer Service*** An Post Money Credit Card Outside of Ireland Fraud Notifications **Customer Service Opening Hours** 8am to 8pm Monday to Friday and 8am to 2pm on Saturday, excluding Bank Holidays.	0818 409 511 +353719594040 1800 286 262 0818 205 410 +353719594094 1800 800 780
Citi	Citi Contact number	+353 1 622 2000
ICLU	Locate your nearest Credit Union using the locator on the website	Credit Union Locator - Find Your Credit Union - The Irish League of Credit Unions

Bank of Ireland	**365 Online:** From Outside ROI Forward suspicious emails to: **Lost/Stolen Cards 24 Hr** From Outside ROI: **Business On Line:** Opening hours: Mon-Fri 08.00-18.00 Closed Saturday, Sunday, Bank Holidays	0818 365 365 +353 1 4044000 365security@boi.com 1890 706 706 +353 56 775 7007 1890 818 265
PTSB	Card related issues From Outside ROI Alternatively the Fraud Dept. All other fraud queries Your local branch is also available to deal with any suspected fraud queries	1890 500 121 +353 1 2124101 +353 1 6695851 1890 500 121
Barclays Private Bank	Fraud Notifications	+353 1 920 3330
An Post	**Customer Service** **From Outside ROI**	01 705 8000 +353 1 705 8000
Revolut	To report a suspected fraudulent transaction, please **tap on the transaction within the app**, scroll down to **'Get help'**, and select **'Report this transfer as fraud'**. Alternatively, customers can speak to a member of our award-winning support team directly via the **secure in-app chat**, available 24/7. Additional customer support is available via our **online Help Centre**.	help.revolut.com/en-IE/help

You should also report suspected fraud incidents to An Garda Siochana via your local Garda Station. https://www.garda.ie/en/Contact-Us/Station-Directory/

FraudSMART

Informed. Alert. Secure.

FraudSMART was created by

Banking & Payments Federation Ireland

Banking & Payments Federation Ireland
Floor 3, One Molesworth Street,
Dublin 2, D02 RF29

Email info@fraudsmart.ie
Web www.FraudSMART.ie