Be Aware
Beat Fraud

A Guide To Fraud Prevention

Banking & Payments Federation Ireland

An Garda Síochána

Police Service Northern Ireland

Identity fraud

Some key warning signs in recognising identity fraud include:

- You receive letters from solicitors or debt collectors for debts that aren't yours.
- You receive bills or invoices for goods or services you haven't ordered.
- You are refused a financial service (such as a credit card or a loan) despite having a good credit history.
- You are billed for a mobile phone contract (or similar) set up in your name without your knowledge.

Always remember:

- Lock all valuable documents in a secure place.
- Shred unwanted documents and anything containing your personal or banking details.(e.g. old utility bills, credit card receipts etc)
- Inform all service providers promptly when moving address
- Protect mail left in communal areas of residential properties
- Set up a mail forwarding arrangement with An Post/ the Post Office.
- Never give you PIN number to anyone.
  Check your credit report with a credit reference service.

Bank and Credit Card Statements

Often times it is the early detection or notification of fraud that will assist or prevent further fraud.

- Regularly check your bank and credit card statements and bank transactions for evidence of fraudulent activity. Chase up any statements not delivered when expected.
- Report any suspicious or fraudulent activity to your bank immediately.
- Don't throw out old statements and/or receipts with your household rubbish. Dispose of it carefully, i.e. shred or burn it.

Phishing

'Phishing' is a form of online fraud where fake emails or websites, supposedly from a legitimate company, seek to obtain your confidential account details. This is done with a view to conducting illegal transactions on your account.

If you think you may be a victim of a 'phishing' attack:

1. Notify the relevant financial institution.
2. Change your passwords.
3. Contact An Garda Síochána/Police.

Always remember:

- Your bank will never send you an email requesting your bank security details.
- You will only need your security details when logging into your bank's Internet banking service.
- Do not share your password with anyone.
- Do not open email attachments from people you don't know.
- Be wary of clicking on links, they can lead to false sites.
- Review credit card and bank statements regularly to reveal any problems and inconsistencies.

Online security

'Spyware' is software that is downloaded onto your computer, without your knowledge. Once there, it can steal a user's information or corrupt the user's system files and may transmit it to a third party.

Always remember:

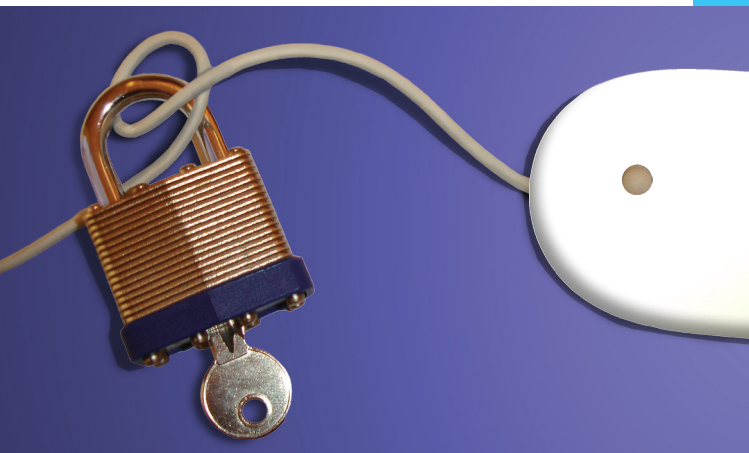
- Install a reliable anti-spyware application.
- Ensure the application is kept up to date.
- Activate a firewall.
- Be security conscious when surfing and downloading.
- Only download from sites you trust.
- Read security information before you download software.
- Any unsolicited request for bank account information you receive through pop-up windows should be considered fraudulent and reported immediately.

Internet – Buying/selling online

When selling high-value goods and services over the internet be wary of cheques/drafts received for a sum in excess of the agreed amount. Fraudsters may claim that this extra money is to pay a handling agent or to cover shipping costs. Do not transfer funds from your own account in order to refund the 'surplus' money. Do not release high-value cash or goods until you are quite certain that the cheque or draft received by you has been paid. Bring such cheques or drafts to the attention of your bank before lodging. Report any fraudulent activity to your local Garda/Police station.

Advance fee fraud

The advance fee fraud occurs where people are persuaded to advance sums of money in the hope of gaining a much larger sum. Recent variations have seen claims by alleged members of staff of a bank who seek assistance to steal substantial sums of monies from dormant accounts. The information contained in the email is totally bogus; the sender is attempting to defraud the recipient. Do not respond to these emails. Avoid and report phishing emails and websites (e.g. support.google.com or satety.yahoo.com etc) to An Garda Síochána/Police.



Security Tips for your smartphone and tablet

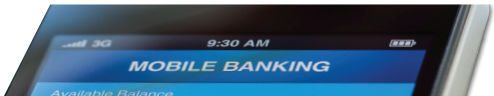
Security Tips for your smartphone and tablet:

- Lock – set your smartphone and tablet to automatically lock. A password protects your device so that no-one else can use or view your information. Store your device in a secure location.
- Contact your bank if you lose your smartphone or tablet – Call your bank immediately to report the loss and provide your new mobile number especially if your bank uses an SMS message to authenticate transactions.
- Clear your mobile device of text messages from banks especially before sharing, discarding or selling your device.
- Be careful what you send via text – never use text messages to disclose any personal information, such as account numbers or passwords which could be used to steal your identity.
- Use only official apps – make sure to only use apps supplied by your financial institution and only download them from official app stores. Install apps from reputable app stores.
- Protect your tablet and smartphone – install and keep up-to-date anti-virus and firewall software purchased from trusted suppliers. It is important to update the software regularly to ensure that you are protected against new viruses.
- Protect your passwords – ensure you keep confidential your PIN and Internet banking logons and passwords. Avoid using the same login passwords for multiple websites, especially when it enables access to websites that include sensitive personal information. Set a pass code for your device and a PIN for your SIM. If your banking app allows login with a PIN, make sure it is different to the one used to unlock your mobile device. Make sure your password or code is something that's hard for others to guess but easy for you to remember.
- Read privacy policies – before you provide personal information to any website, understand how your information will be used and how long it will be retained.
- Be wary of free downloads, programs, software or screensavers – sometimes malware and spyware can

be hidden in files offered free-of-charge.

- Beware hoax e-mails – be alert to offers that are 'too good to be true' or are designed to elicit an emotional response and triggers the thought of sending money. Always question messages that come out of the blue and verify the authenticity through trusted channels. Do not respond using information or links provided in the original message. No bank will ever send customers an e-mail with a link to online banking or ask for confidential information, so treat with suspicion any unsolicited e-mail that appears to be from your bank.
- Never reply to unsolicited texts - simply delete them.
- Check your bank account statements – contact your bank immediately if you find any unusual or suspicious transactions. Your bank will then take action to protect your account. Bank staff may call you before your statement has arrived to advise you of unusual activity on your account.
- Don't store your banking PINs or passwords in your smartphone or tablet – this makes your account vulnerable if the device is lost or stolen.
- Regularly clear your browser's cache – some mobile devices store copies of web pages that may contain your banking information.
- Always log out of Internet banking sessions once you've finished.
- Be aware – when using Internet banking in busy, public areas, check for people looking over your shoulder.
- Wi-Fi - don't conduct internet banking using unsecured public Wi-Fi networks or hotspots. Use a 3G or 4G data connection instead.

Device Security - Do not jailbreak your device and do not use jailbroken or rooted devices for internet banking. jailbroken or rooted device is any electronic device not designed or authorised by phone manufacturers and network operators. Jail breaking your own device can significantly weaken its security.



Card fraud

Chip and PIN has changed the way we pay for goods and services. It is easy and secure:

- Using your PIN to verify transactions will make card fraud considerably more difficult.
- Take care when entering your PIN – always keep it safe, cover the keypad when entering the PIN, never tell anyone what it is and never write it down or record it on any device.
- When paying for goods and services prevent cloning by insisting on being present when your card is being processed.
- You should never provide your PIN when carrying out telephone and Internet transactions, or purchase by mail order.

Card fraud – holiday travel

When on holidays you will be more relaxed and perhaps less vigilant so here are a few tips:

- When paying for anything with your credit or debit card don't let the card out of your sight. You can always accompany the staff member to the payment terminal or ask if the terminal device can be brought to you.
- Consider whether it is necessary to carry all your cards with you when you go out. Leave unused cards safely locked away.
- Have details of who to contact (in your card issuing bank) in the event that you lose your card or it is stolen.
- Have your card number(s) and account number(s) details available in the event that you should lose or have your card stolen.
- Always keep your card(s) and data in a safe place.
- Be careful with your PIN, never divulge it to anyone for any reason.

Golden rules to reduce ATM Crime

Always remember:

- Be aware of your physical surroundings.
- Check that other people in the queue are at a reasonable distance.
- Shield your PIN number with your hand to prevent hidden cameras or person from capturing your information. Never reveal your PIN to anyone.
- Use ATM machines which are in clear view and well lit. Be careful of machines in dark areas or places that don't appear to be well monitored. If suspicious, walk away.

Observe the ATM

- Pay attention to the front of the machine: – If the front of the machine looks different from others in the area (for example, it has an extra mirror on the face), has sticky residue on it (potentially from a device attached to it) or extra signage, use a different machine and notify bank management with your concerns.
- Pay close attention to the slot were you insert your card, if you're visiting an unfamiliar ATM machine, examine it carefully for hidden devices. Even if you are familiar with an ATM machine, pay attention to any differences or unusual characteristics of the card reader.
- If the ATM appears to have anything stuck onto the card slot or keypad, do not use it. Cancel the transaction walk away and immediately notify your local Garda/Police station.
- Never try to remove suspicious devices.

Counterfeit notes - Euro

Is your Euro note genuine or counterfeit? Here are some things you can check:

- Feel – you can feel the raised intaglio printing on all genuine notes and also the tactile marks on the €200 and €500 banknotes.
- Look – hold the note against a bright light source, the denomination (e.g. €5, €10, etc.) in the top left hand corner should be fully visible and perfectly formed.
- Tilt – look at the colour shifting ink on the reverse side of the high value notes (i.e. €50, €100, etc.). The value numeral looks purple when viewed straight on, but appears olive green or even brown when viewed at an angle. On the reverse of low-value notes (i.e. €5, €10 & €20) look for the iridescent stripe that shines against bright light.
- Check – you can see a security thread embedded in the genuine note. If you hold the banknote against a bright light source you can see the watermark and the security thread on the note. The watermark is visible from front and back of the note. The watermark comprises the main architectural motif and the value numeral of the note.

Counterfeit notes - Sterling

If you discover a possible fake note check the following:

- Feel – Most notes are embossed, usually the writing or the logo. The note should feel crisp not limp, waxy or shiny. Security paper and special printing processes give banknotes a unique feel.
- Look – Print lines should be sharp and well defined with no blurred edges. The colours should be clear and distinct with no hazy fringes.
- Tilt – Check for the watermark image and security thread. The watermark should be hardly apparent until the note is held against a bright light source. Check for hologram features on some of the notes.
- UV Light – Under ultraviolet (UV) light, barcodes are visible.
- Compare – Compare both sides of the notes to one you know is genuine.
- Detector Pen – Don't rely totally on the pen – use it as a guide. Be careful not to use the pen on ordinary paper as this will lower its effectiveness and may lead to a genuine note being marked as fake.
- For all bank notes, do not rely on just one feature to assess whether a note is genuine, check a few. If in doubt, refer the item to your local financial institution.

Investment fraud (Boiler room fraud)

Overseas companies (usually unauthorised) make unsolicited contact and offer to sell shares which are about to 'go through the roof', or they may invite you to invest further monies to capitalise on 'inside' information.

Always remember:

- Check if the company is authorised (by a financial regulator) to deal in such investments.
- Get independent advice froma qualified financial advisor before investing.
- Report any unsolicited approaches to An Garda Síochána/Police.
- Reject cold calls. If you have been cold called about an investment opportunity, it is very likely that it is a high risk investment or a scam.
- Do not respond to high pressure tactics.
- When investing with a regulated firm, always make your cheque payable to the named financial institutions

Fraud against the elderly

Elderly customers can be particular at risk from bogus traders/callers who set out to gain their confidence before taking financial advantage of them.

Typically these people call door-to-door and offer to carry out works such as replacing roof tiles, mending guttering, decorating or they 'convince' the victim that repairs are necessary. Some of these people carry out a little work and charge exorbitant amounts of money for their services.
In many cases the work is unnecessary. On completing the work in a very short time, they then demand substantial payment often using threatening and intimidating tactics. In some instances, they offer to drive the victim to the bank to withdraw the cash.

Always remember:

- You should never leave strangers, even bona fide workers, unsupervised in your home.
- Never engage a person who insists on cash payments for services offered. Most reputable traders will not

ask for money up front. Always use a method of payment which is traceable.
- Never sign a blank form for any reason - it could cost you dearly.

Cheques and drafts fraud

Always remember:
- Control who has access to your cheque books.
- Do not sign cheques in advance.
- Ensure all issued cheques and unused cheque numbers are accounted for. Review regularly to ensure no cheques are missing.
- Cross all cheques "a/c payee only"

Money Mules (Job Vacancies)

Money Mules are people recruited by criminals to help transfer fraudulently obtained money from bank accounts. Fraudsters contact prospective victims with "job vacancy" adverts on the Internet, on job search websites or in newspapers. These jobs are usually advertised as 'Financial Manager' or 'Payments Clerk' withno other requirement than having a bank account. The mule accepts the "job" and in so doing becomes involved in criminal activity. Once recruited a Money Mule receives stolen funds into their account, followed by a request to forward the funds, minus their commission, usually overseas, using a money/wire transfer service.

Always remember:
- Thoroughly research any work-from-home offer and do not get involved unless you are sure the business is legitimate.
- If a job sounds too good to be true, then it probably is.

Lottery fraud

Another scam currently being carried out by various groups of international fraudseters involves victims being contacted by email in which they are advised that

they have won the lottery. No ticket purchase was necessary - according to the scammers. The victim is encouraged to pay a fee before the 'winning' lottery cheque is handed over. This scheme is a fraud and you should not become involved or communicate with them in any way as these winnings do not exit.

Principal Organisations

Banking and Payments Federation Ireland	www.bpfi.ie
An Garda Síochána	www.garda.ie
PSNI	www.psni.police.uk

Participating Financial Institutions:

AIB	www.aib.ie
An Post	www.anpost.ie
Bank of Ireland	www.bankofireland.ie
Bank of Ireland UK	www.bankofireland.co.uk
Danske Bank	www.danskebank.ie
Danske Bank	www.danskebank.co.uk
EBS Limited	www.ebs.ie
First Trust Bank	www.firsttrustbank.co.uk
KBC Bank Ireland	www.kbc.ie
Permanent TSB	www.permanenttsb.ie
Rabodirect	www.rabodirect.ie
Ulster Bank	www.ulsterbank.ie
	www.ulsterbank.co.uk

Useful Websites:

www.makeitsecure.ie	www.fsa.gov.uk
www.cyberaware.gov.uk	www.getsafeonline.org
www.bpfi.ie/news/fraud-alerts/	www.centralbank.ie
www.takefive-stopfraud.org.uk	www.actionfraud.police.uk
www.financialfraudaction.org.uk	

Disclaimer Note:

09.05.2017