

Be Aware Beat Fraud

A Guide To Fraud Prevention



**IRISH
BANKING
FEDERATION**



Protect Your Identity	1
Stay Secure Online	2-3
Guard Your Cards	4-5
Know Your Money	6-7
Spot Fraudsters	8-9

Garda Commissioner - Fachtna Murphy (An Garda Síochána)

Everyday fraudsters by their dishonest actions ruin people's self respect and lives by deceiving them through the activities this leaflet describes. We must all, the individual, the Garda Síochána and the financial industry, play a role in preventing fraud by acting on the excellent advice this guide offers us.

CEO - Pat Farrell (Irish Banking Federation)

This straightforward guide will enable you to safeguard against fraud arising in the financial services that you use. Through a better understanding of the different types of fraud and by following the simple, practical advice provided in this guide, you can be more vigilant in protecting your interests.

CEO - Pat McLoughlin (Irish Payment Services Organisation Limited)

IPSO works hard to ensure that payments are made as safely and as securely as possible. However payment fraud is a growing concern. Knowing what the issues are is the first step toward prevention and helps strengthen our defences.

Chief Constable - Matt Baggott (Police Service of Northern Ireland)

Fraud can take many forms and is often perceived to be a victimless crime. This is not the case. While it can mean a significant financial loss for companies and organisations, it can also have an impact on you, your family and friends.

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 (e.g. old utility bills, credit card receipts etc.).
- Inform all service providers promptly when moving address.
- Set up a mail forwarding arrangement with An Post/ the Post Office.
- Never give your PIN number to anyone.
- Check your credit report with a credit reference service.

Bank and Credit Card Statements

Oftentimes 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.
- 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 collect information from your system and may transmit it to a third party.

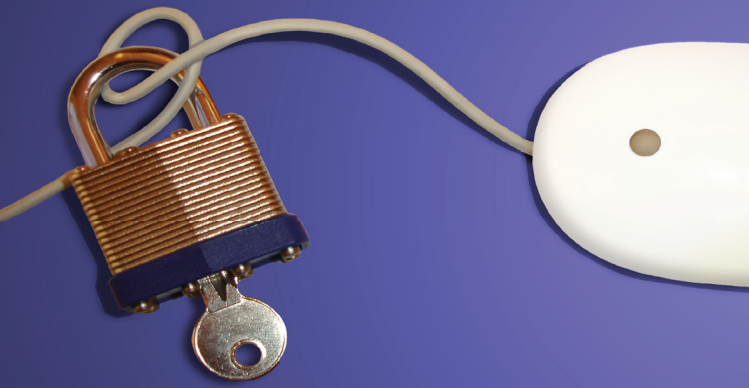
Always remember:

- 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.

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. Forward them to the relevant internet service provider (e.g. abuse@hotmail.com or abuse@yahoo.co.uk, etc) and notify An Garda Síochána/Police.



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 where 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.



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 from a qualified financial advisor before investing.
- Report any unsolicited approaches to An Garda Síochána/Police.
- Do not respond to high pressure tactics.
- When investing with a regulated firm, always make your cheque payable to the named financial institution.

Fraud against the elderly

Elderly customers can be particularly 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 service. 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' with no 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 fraudsters 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 exist.

Principal Organisations

Irish Banking Federation	www.ibf.ie
IPSO	www.ipso.ie
An Garda Síochána	www.garda.ie
PSNI	www.psnipolice.uk

Participating Financial Institutions:

AIB	www.aib.ie
An Post	www.anpost.ie
Anglo Irish Bank	www.angloirishbank.ie
Bank of Ireland	www.boi.ie
	www.bankofireland.co.uk
EBS Building Society	www.ebs.ie
First Trust Bank	www.firsttrustbank.co.uk
First Active	www.firstactive.ie
Halifax	www.halifax.ie
Irish Nationwide Building Society	www.irish-nationwide.com
National Irish Bank	www.nationalirishbank.ie
Northern Bank	www.northernbank.co.uk
Permanent TSB	www.permanenttsb.ie
Postbank	www.postbank.ie
Ulster Bank	www.ulsterbank.ie

Useful Websites:

www.financialregulator.ie	www.fsa.gov.uk
www.makeitsecure.org	www.banksafeonline.org.uk
www.cardwatch.org.uk	www.safecard.ie
www.identitytheft.org.uk	
www.financialfraudaction.org.uk	

Disclaimer Note:

The contents of this booklet/brochure are provided as an information guide only and are intended to enhance awareness regarding fraud issues. While every effort has been made to ensure the accuracy of the material in this publication, no responsibility is accepted by, nor liability assumed by or on behalf of the participating organisations.