current account
from your credit union

Protecting you and your Current Account & Debit Card from Fraud

For more information visit
www.currentaccount.ie

V2 2024

Protecting Yourself from Financial Fraud

It is not uncommon to hear about financial transaction fraud in the news, and with fraudsters becoming more and more sophisticated, it is increasingly important to take measures to safeguard yourselves.

While most financial fraud still happens via phone, texts and emails, fraudsters are also utilising technology and publicly available information to deceive people.

As a valued member of our Credit Union, we are providing you with this guide to help you become more aware of these types of fraud threats.

If you have any questions about this document, please do not hesitate to contact your Credit Union or or call our 24 hour Credit Union Card Services Team, IMMEDIATELY on +353 1 693 3333.

PROTECTING YOUR PASSWORDS

NEVER EVER write your password down or share it with anyone else. Change it immediately if you believe it has been compromised.

Use the security settings on your device - You should turn them on and set them to the highest level possible.

Only YOU should know your PINS, PASSWORDS or ONE TIME PASSCODES (OTP) for your bank cards and online access.

Your Credit Union will NEVER ask you to confirm PINs or Passwords over the phone or by SMS.

Always use a strong password with alpha-numeric characters and at least 8 characters in length.

Dont use personal information or easily recognisable words for passwords.

If you follow these simple steps, it will help to keep your Current Account & Debit Card Safe and Secure.

SHOPPING ONLINE

Don't use unsecured public Wi-Fi networks or hotspots to make a card purchase or access your online account. Use your home or mobile data internet connection instead.

Ensure that when you are shopping or making a payment online, that your internet access is secure and you have the most up to date antivirus software to protect your device.

The beginning of a website address should change from 'http' to 'https' before a purchase is made. This indicates that you are using a secure connection.

This should be combined with other checks as fraudsters can copy or buy these padlocks, so it isn't a guarantee the website is safe.

REMEMBER if its too good to be true, trust your instincts - it's likely to be a scam!

SHOPPING ONLINE

SCAM ALERT

Criminals can use fake advertising and websites to lure you into providing your debit card information.

Once you have either,

- Entered your debit card details to authenticate a purchase or
- Provided a One Time Passcode (OTP) to complete the payment.

The fraudster or fake website now has stolen your card details and can spend your hard-earned money!!

This is known as Tokenised Fraud, using the **'Smishing'** method.

- Never divulge personal information including account details, Debit Card Number one time passcode (OTP) or PIN, online information over the phone or by SMS.
- Don't be Fooled by ads on Social Media with 'incredible' offers.
- Do not respond to requests to purchase gift cards and then provide the code as a form of payment.

If you think you have responded to a request of this nature or provided your card details to an unknown 3rd party, contact your Credit Union or call our 24 hour Credit Union Card Services Team, IMMEDIATELY on +353 1 693 3333.

SHOPPING ONLINE

Review the website in detail before you make a purchase.

Look for a 'padlock' symbol in the address bar or browser.
This normally indicates the site is encrypted so your activity can't be intercepted.

- Are there any grammar or typo errors?
- Check the website address is spelled correctly e.g.; www.storeie.ie
- Have they a registered business address / a good returns policy?
- Are there positive Google reviews?
- Are there genuine Social Media followers / posts?

If anything looks unusual,
DO NOT
make a purchase from them!

PROTECTING YOUR DEBIT CARD PIN

Be aware of others around you especially people offering help.
If a stranger offers to help you at a cash machine, put your card away and leave. This is most likely a scam to try and see your PIN and steal your card.

Be Aware of any damage or obvious fixtures to the ATM that look out of the ordinary. If in doubt, use another ATM.

Protect your PIN and NEVER EVER SHARE your Debit Card PIN details with anyone.

Shield your PIN & check there is no one near you before using an ATM.

Never write your PIN down or share it with anyone.

Check your receipts against your Credit Union statements regularly.

Never let your Debit Card out of your sight when you are making payments.

If you find a transaction that you don't recognise, contact your Credit Union or call our 24 hour Credit Union Card Services Team, IMMEDIATELY on +353 1 693 3333.

SCAM CALLERS - PHISHING

EMAIL SCAM

It's important to be aware that fraudsters may contact you by phone, pretending to be from your Credit Union, the Gardai, or other well-known companies.

These scam calls can sound professional and convincing, and are often accompanied by the caller already having some information about you.

Fraudsters attempt to trick you into handing over personal information such as your credit union details, usernames, or passwords via phone or email, by pretending to be from a trustworthy source such as your Credit Union.

The information they gain can then be used to access your Current Account or debit cards.

current account
from your credit union

REMEMBER if its too good to be true, trust your instincts - it's likely to be a scam!

SCAM CALLERS - VISHING

VOICE & PHISHING SCAM

Phone scam where fraudsters target you by phone and try to trick you into divulging personal, financial or security information or into making a financial transfer to them.

A fraudster can phone you, claiming to be from a bank, Credit Union, the Gardaí/Police or a service provider such as a telephone company, internet provider or computer company. The number they are calling from maybe from the legitimate company number.

This is better known as 'Spoofing'.

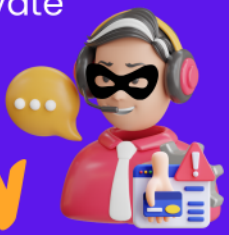
The fraudsters trick you into believing they are a legitimate representative of the organisation and that it is in your interest to give the information they ask for.

Fraudsters can then try to extract information from you such as debit card details, PIN number, online banking details, password, and personal details such as name, address and date of birth.

SCAM CALLERS - SMISHING

TEXT MESSAGE SCAM

SMS from a reputable organisation asking you to click on a link to a fake website or to call a phone number to "verify", "update" or to "reactivate" your account.



The message will typically ask you to click on a link to a website or to call a phone number in order to "verify", "update" or to "reactivate" your account

The website link leads to a bogus website and the phone number leads to a fraudster pretending to be the legitimate company

The criminal attempts to get you to disclose personal, financial or security information, which will then be used to steal your money.

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

If you find a transaction that you don't recognise, inform your Credit Union or call our 24 hour Credit Union Card Services Team, IMMEDIATELY on +353 1 693 3333.

SCAM CALLERS KEY ADVICE

NEVER EVER click on a link in an email or text message asking you for your personal security information.

ALWAYS check the legitimacy of a request even if the message comes from a person or business, you are familiar with.

STOP! → THINK! → CHECK!

DO NOT be pressured into sharing information or a request to make an urgent payment.

ALWAYS confirm the legitimacy of a request to send money or add a new payee to your online banking - even if it's a family member!

Your Credit Union will NEVER EVER ask you for any PINs or Passwords to your App or Online Banking or request you withdraw money to hand over to them or transfer money to another account, even if they say it is in your name.

ROMANCE SCAM

Romance fraud occurs when you think you've met the perfect partner online, but they are using a fake profile to form a relationship with you.

They gain your trust over several weeks or months and have you believe you are in a loving and caring relationship.

A romance scammer may ask you to send money for things like: Travel expenses, a plane ticket Visa or Medical expenses like surgeries.

Sometimes, the extent of the scam is not fully known because many of the victims are too embarrassed to report the fraud to Gardaí, so ensure you provide as much information as possible for the investigation of the scam.

If you believe you have been a victim of a scam, contact your local Garda Station, Credit Union or call our 24 hour Credit Union Card Services Team, IMMEDIATELY on +353 1 693 3333.

DEAR 'MUM' DEAR 'DAD' MESSAGE SCAM

This scam involves fraudsters posing as family members to manipulate victims into transferring money

Typically, the conversation on WhatsApp, or via text message, is then started by an automated bot, and then forwarded to a human who can communicate with the victim if they engage.

Parents are targeted by criminals pretending to be one of their children, saying they are texting from a new number as their phone has been lost or damaged.

They typically begin the conversation with "Hello Mum" or "Hello Dad" and then ask for their parents to transfer money urgently as they need to buy a new phone or pay a bill.

If you find a transaction that you don't recognise, contact your Credit Union or call our 24 hour Credit Union Card Services Team, IMMEDIATELY on +353 1 693 3333.

KEY ADVICE

Be WARY of any number that is not already in your contacts, and try calling the original phone number of the person who is apparently making contact.

If in doubt, **DO NOT** proceed with the transaction.

If you complete the transaction and have concerns, you can temporarily SUSPEND your Current Account debit card in your mobile App, by contacting your Credit Union or our 24 hour Credit Union Card Services team.

IMMEDIATELY contact your Credit Union or our 24 hour Credit Union Card Services Team on +353 1 693 3333 if you think you have provided your bank details to an unknown third party.

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

REMEMBER if its too good to be true, trust your instincts - it's likely to be a scam!

MONEY MULING

Money Muling is a type of Money Laundering

A money mule is someone who transfers or moves illegally acquired money on behalf of someone else.

Criminals recruit money mules to help launder proceeds derived from online scams and frauds or crimes like human and drug trafficking.

The majority incidents involving current accounts belonging to those aged between **18 & 24**.

Money mules are typically recruited though social media in what appears to be a friendly approach by the criminal offering 'easy' money.

MONEY MULING WARNING SIGNS

- Beware if you receive an unsolicited e-mail or social media message that promises easy money for little or no effort.
- Never agree to open a new current account in your own name or use your own account in order receive a transfer/inbound payments on behalf of anyone.
- Money mule advertisements or offers might replicate a legitimate company's website and use a similar web address to create the impression of authenticity for the scam.
- Fake Job Offers - The role includes transferring money or goods/job duties are not specified with no education or experience requirements.

current account
from your credit union

If you suspect you have been the victim of fraud or have noticed unusual activity on your Current Account or Debit Card contact your Credit Union or Credit Union Card Services **IMMEDIATELY** and also report to your local Garda Station.

Fraudsters move fast; the quicker you contact your Credit Union to safeguard your accounts the better!

Our Credit Union Card Services Team are available anytime on +353 1 693 3333.

For more information visit
www.currentaccount.ie