FINGLAS CREDIT UNION

FRAUD AWARENESS GUIDE

FINGLAS
CREDIT UNION
IRELAND

WELCOME TO OUR FRAUD AWARENESS GUIDE

Fraud and scams are becoming increasingly common, with criminals using more sophisticated methods to target individuals and businesses. From suspicious phone calls and text messages to fake websites and online scams, it is more important than ever to stay informed and aware of the risks.

At Finglas Credit Union, protecting our members' money and personal information is a top priority. This Fraud Awareness Guide has been created to help you recognise common types of scams, understand how fraudsters operate and learn simple steps you can take to protect yourself and your finances. By understanding these risks and knowing what warning signs to look out for, you can reduce the chances of becoming a victim.

Remember: If you ever suspect suspicious activity or receive a message that doesn't seem right, contact Finglas Credit Union directly using official contact details. Our team is always here to help and support you. Staying informed is one of the best ways to stay protected.

TABLE OF CONTENTS:

PAGES 3-4
Information About Phishing, Smishing and Vishing Scams

PAGE 5
Protecting Your Passwords & Debit/Credit Cards

PAGE 6
Online Shopping Safety and Protecting Your Devices

PAGE 7
Social Media Safety & Ticket Scams

PAGE 8
Investment Scams & Frauds

PAGE 9
Money Muling & Ways to Report a Scam

PAGE 10
7 Useful Tips to Remember

PAGE 11
Examples of Scams & Useful Links

HOW PHISHING, SMISHING AND VISHING WORKS

Fraudsters use various manipulative tactics to deceive individuals into revealing sensitive information. Below are three common examples of fraud using email, SMS and phone calls.

PHISHING EMAILS:

Phishing emails are fraudulent messages designed to trick you into sharing personal or financial information. These emails often appear to come from legitimate organisations such as your credit union, bank, utility provider, delivery company or government agency. They may use official-looking logos and urgent language to make the message seem genuine.

Example: You may receive an email claiming there has been suspicious activity on your account, urging you to click a link to “secure your account” or “verify your details.” The link may bring you to a fake website that looks real but is designed to steal your login details, passwords or card information.

What to watch for:

- Urgent messages asking you to act quickly
- Links requesting you to log in or confirm details
- Spelling or grammar mistakes
- Email addresses that look slightly different from official ones

SMISHING TEXTS (SMS FRAUD)

Smishing is a form of phishing carried out through text messages (SMS). These fraudulent texts aim to trick you into clicking a link or sharing sensitive information. They often appear to come from trusted organisations such as your credit union, bank, delivery company or government department.

Example: You may receive a text saying, “Your debit card has been blocked. Click the link to reactivate it.” Clicking the link may direct you to a fake website or download harmful software, putting your personal and financial information at risk.

What to watch for:

- Unexpected texts with links
- Messages creating panic or urgency
- Requests for personal or banking details
- Messages from unknown or unusual numbers

VISHING CALLS (PHONE SCAMS)

Vishing, or voice phishing, involves scammers calling you and pretending to represent a trusted organisation. They may sound convincing and professional and often use fear tactics to pressure you into sharing confidential information.

Example: A scammer may call claiming there is suspicious activity on your account and ask you to provide your PIN, passwords or online banking details to "resolve the issue." In some cases, they may ask you to transfer money to a "safe account," which is actually controlled by the fraudster.

What to watch for:

- Calls asking for passwords, PINs or One-Time Passcodes (OTPs)
- Requests to move money urgently
- Callers creating panic or insisting you act immediately
- Calls claiming to be from your bank or credit union without prior contact

HOW THESE TYPES OF SCAMS TYPICALLY OPERATE

Impersonating Trusted Entities: Scammers pose as legitimate organisations, such as your bank, credit union, government agencies or well-known companies, to gain your trust. In phishing emails, smishing texts or vishing calls, they often mimic official logos, language and tone to appear authentic. This impersonation is designed to make you believe that the communication is genuine, increasing the likelihood of compliance.

Urgency and Fear Tactics: A key strategy of these scams is to create a sense of urgency or fear. Messages might warn you about suspicious account activity, claim your account will be locked or allege you owe money. They pressure you into acting immediately, leaving little time for critical thinking. This emotional manipulation is aimed at making you respond without verifying the legitimacy of the request.

Fake Links and Attachments: Phishing emails and smishing texts often contain links that lead to fake websites designed to look like legitimate login or payment portals. These fraudulent sites collect your personal or financial details. Similarly, attachments in phishing emails may contain malware that, once opened, can compromise your device and give fraudsters access to sensitive data.

PROTECTING YOUR PASSWORDS

Passwords play a vital role in keeping your accounts safe from unauthorised access. Creating strong passwords and managing them securely is one of the most effective ways to protect your personal information. Here are some tips to keep your passwords secure:

Create Strong and Unique Passwords: Use passwords that are at least 12 characters long, including a mix of letters, numbers and special characters. Avoid reusing the same password across multiple accounts and update your passwords regularly.

Avoid Easy-to-Guess Details: Do not use obvious information such as birthdays, family names or common words that could be easily guessed.

Use Two-Factor Authentication (2FA): Where available, enable two-factor authentication. This adds an extra level of protection, making it much harder for fraudsters to access your accounts even if they obtain your password.

Avoid Storing Passwords in Browsers: Instead of saving passwords in your browser, consider using a trusted password manager to store them securely.

PROTECTING YOUR DEBIT/CREDIT CARD PIN

Your debit & credit card PIN is confidential and should always be treated with care to prevent unauthorised use of your card. Here are 3 useful tips to keep in mind.

Keep Your PIN Confidential: Never share your PIN with anyone and avoid writing it down where it could be discovered.

Stay Alert at ATMs: When using an ATM, always cover the keypad while entering your PIN and stay aware of your surroundings.

Choose a PIN That Is Hard to Guess: Avoid using obvious numbers such as birth dates, phone numbers or repeating digits. A unique PIN makes it more difficult for fraudsters to guess.

ONLINE SHOPPING SAFETY

Online shopping is convenient and popular, but it is important to take precautions to reduce the risk of fraud. If an offer is too good to be true, it usually is! Here's some tips:

Use Trusted Websites: Shop only on reputable websites and check for security features such as a padlock symbol and "https" in the address bar.

Choose Secure Payment Options: Whenever possible, use debit or credit cards rather than direct bank transfers, which may be harder to recover if something goes wrong. Do not store your card details on unfamiliar or unsecured websites.

Be Wary of Unrealistic Deals: If an offer seems unusually cheap or too good to be true, it may be a scam designed to attract attention.

Access Websites Safely: Type the website address directly into your browser or use a trusted search engine such as Google or Bing. Avoid clicking on links in emails or unfamiliar websites.

Check Retailer Reputation: Always purchase from well-known retailers or those recommended by trusted sources. If you are unsure about a website, research independent reviews rather than relying solely on testimonials shown on the site.

PROTECT YOUR DEVICES

Keeping your devices secure and up-to-date helps prevent fraudsters from gaining access to your personal and financial information.

Install Updates Promptly: Regularly update your devices and applications to ensure you have the latest security protections against potential threats.

Use Reliable Antivirus Software: Install and maintain antivirus software to help guard against viruses, malware and other harmful programs.

Secure Your Internet Connection: Protect your home Wi-Fi with a strong password and avoid carrying out sensitive transactions when connected to public Wi-Fi networks.

SOCIAL MEDIA AWARENESS

Social media is a great way to keep in touch with friends and family, but it is also a common place where scammers look for opportunities to gather personal information.

TIPS FOR STAYING SAFE ON SOCIAL MEDIA

Think Before You Share: Be mindful of the personal details you post online. Information such as your birthday, address, school names, or even pet names can be used by scammers to guess passwords or security answers.

Be Alert to Fake Profiles and Messages: Watch out for suspicious friend requests or unexpected messages offering prizes, discounts or urgent requests for help. These are often signs of scam activity.

Avoid Suspicious Links or Downloads: Do not click on unfamiliar links or download files sent through social media, especially from unknown contacts or newly created accounts.

Review Your Privacy Settings Regularly: Check your privacy settings to ensure your profile information and posts are visible only to people you trust.

CONCERT, FESTIVAL AND TICKET SCAMS

With concerts and festivals often selling out quickly, scammers take advantage of fans who are eager to secure tickets. Being cautious when buying tickets online can help you avoid losing money. Here are some Do's and Don't to remember when buying tickets.

DO's

- Purchase tickets only from official websites or authorised sellers.
- Use secure payment methods such as credit cards or trusted payment platforms like PayPal.
- Set up ticket alerts so you know exactly when official sales begin.

DON'Ts

- Buy tickets from social media posts, unverified sellers or classified advertisements.
- Trust deals that seem unusually cheap or available after tickets have sold out.
- Pay by bank transfer or share personal details with unknown sellers.
- Click on suspicious links or rush into purchases due to pressure tactics.

INVESTMENT SCAMS & FRAUDS

Investment scams are designed to persuade people to hand over money by promising high returns with little or no risk. These scams often look professional, using convincing websites, testimonials or even pretending to represent well-known companies. Unfortunately, once money is sent, it can be very difficult to recover.

HOW INVESTMENT SCAMS TYPICALLY WORK

Scammers often attract victims by advertising quick profits & guaranteed returns:

- Claim to offer "exclusive" or limited-time investment opportunities.
- Pretend to be financial advisers or representatives of genuine companies.
- Use pressure tactics to push you into making fast decisions.
- Provide fake paperwork or references to appear legitimate.

COMMON TYPES OF INVESTMENT SCAMS

These scams can take many forms, including:

- Ponzi schemes
- Pyramid schemes
- Fake cryptocurrency investments
- "Get-rich-quick" opportunities
- Forex and binary options scams
- Celebrity & fake endorsement scams

HOW TO PROTECT YOURSELF FROM INVESTMENT SCAMS

Be Wary of Unrealistic Promises: If an investment guarantees high returns with little or no risk, it is very likely to be a scam.

Research Before Investing: Always check the company's background and credentials using independent sources. Confirm whether the company is registered with a regulatory body such as the Central Bank of Ireland.

Take Your Time: Legitimate investment opportunities will allow you time to consider your options. Avoid making rushed decisions.

Be Cautious of Unsolicited Contact: Treat unexpected phone calls, emails or messages promoting investments with caution. Scammers may use fake websites or email addresses that closely resemble real ones. Always confirm details through official contact channels before proceeding.

WHAT IS MONEY MULING?

Money muling is a growing type of financial crime that affects people of all ages but is more common among men aged between 18-34 years and newcomers to the country, often without them realising the serious consequences involved. A money mule is someone who transfers or moves illegally obtained money on behalf of criminals, usually through their own bank account. This may involve receiving funds into an account, withdrawing the money, and sending it on to another account, often overseas and in return for a payment or "commission.

HOW ARE MONEY MULES RECRUITED?

Fraudsters use a variety of methods to recruit money mules, often making their offers look like genuine job opportunities:

- Job advertisements for roles such as "money transfer agent" or "local representatives"
- Posts on social media platforms or closed online groups
- Direct contact through emails or messaging apps such as WhatsApp
- Online advertisements that appear professional and legitimate
- Messages promising easy money for little work

It is important to understand that becoming involved in money muling, even unknowingly can have serious legal and financial consequences. If caught, a person may face criminal charges, fines, community service, or even imprisonment. In addition, having a record linked to financial crime can make it extremely difficult to open a bank account, obtain credit, or secure a mortgage in the future.

REPORT THE SCAM!

If you believe you may have encountered a scam, take these steps to protect yourself.

Stop Communication Immediately: If you suspect that someone contacting you may be a scammer, end all communication straight away.

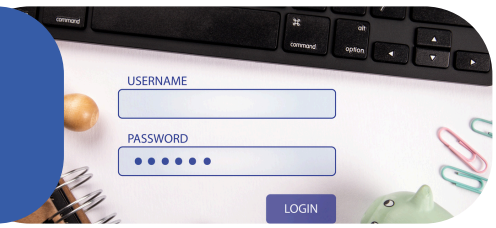
Do Not Send Money or Share Details: Never transfer funds or provide additional personal or financial information once you suspect fraudulent activity.

Report the Incident: Notify the appropriate authorities, such as your credit union or the Central Bank of Ireland, so they can help investigate and prevent further scams.

7 USEFUL TIPS TO REMEMBER

1. Be Cautious with Links: Never click on links in unexpected emails or text messages. If you're unsure, go directly to the organisation's official website instead.

2. Do Not Share Personal Details: Never share your PIN, passwords, One-Time Passcodes (OTPs), or full card details by phone, text or email.



3. Check the Sender Carefully: Look closely at email addresses and phone numbers. Fraudsters often use addresses that look similar to legitimate ones.

4. Verify Before You Trust: If you receive a suspicious call, text or email claiming to be from your credit union contact them directly using their official phone number.

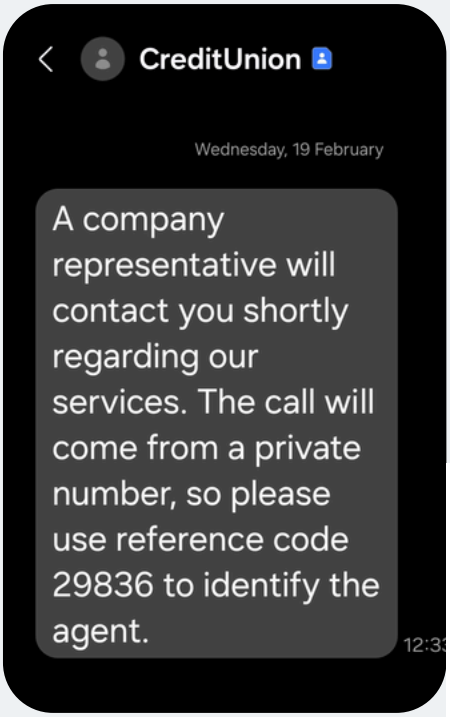
5. Watch for Urgent or Threatening Messages: Scammers often try to create panic by saying your account has been blocked or there is suspicious activity. Think before acting.

6. Delete Suspicious Messages: If something doesn't feel right, delete the message and avoid responding or clicking any links.

7. Keep Your Devices Secure: Make sure your phone, tablet and computer have up-to-date security software and install updates when prompted.

EXAMPLES OF WHAT SCAMS CAN LOOK LIKE

Below are some examples of real scam texts that have been received by Credit Union members across Ireland. It is important to stay alert and be aware of what these messages can look like, as scammers often make them appear genuine. If you receive a suspicious text message, do not click on any links and delete it immediately. If you are ever unsure, contact your credit union directly using official contact details.



Credit union: A new payee Peter Brady IE**********26818/ AIBKIE2DXXX was created online. Please contact us on (01) 578 5614 if you did not create this payee.

CREDIT UNION: A new Payee (JAMIE SMITH) has been added to your account. Contact us immediately on 015134884 if this wasn't you.

Credit Union: 3 failed login attempts. Please reset your password. If this wasn't you, contact support at +353834200992. Ref: 7367F

Credit Union: You could qualify for a 30% electricity reduction if you've saved with your Credit Union. Apply here: https://union-credit.irish

Credit Union: Your credit union account has been placed on hold please review your account: https://mycuireland.im/
Reference: 389210

USEFUL LINKS:

Visit the following websites for more Information about ways to avoid scams and to stay up-to-date with the latest scams & frauds in circulation.

- **FraudSmart:** Link
- **Central Bank of Ireland - Consumer Hub:** Link
- **National Cyber Security Centre:** Link

Banc Ceannais na hÉireann
Central Bank of Ireland
Eurosystem

Opening Hours:

Monday	Closed
Tuesday	10.00am - 4.00pm
Wednesday	10.00am - 4.00pm
Thursday	10.00am - 6.00pm
Friday	10.00am - 6.00pm
Saturday	10.00am - 1.00pm

www.finglascu.ie

01 834 3193

info@finglascu.ie

Seamus Ennis Road, Finglas
Dublin 11

FINGLAS
CREDIT UNION
IRELAND