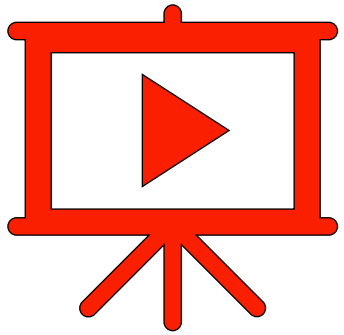
Fraud Awareness for Members

current account
from your credit union

Agenda



1. Spoofing
   - Key Advice
2. Phishing
   - Key Advice
3. Vishing
   - Key Advice
4. Smishing
   - Key Advice

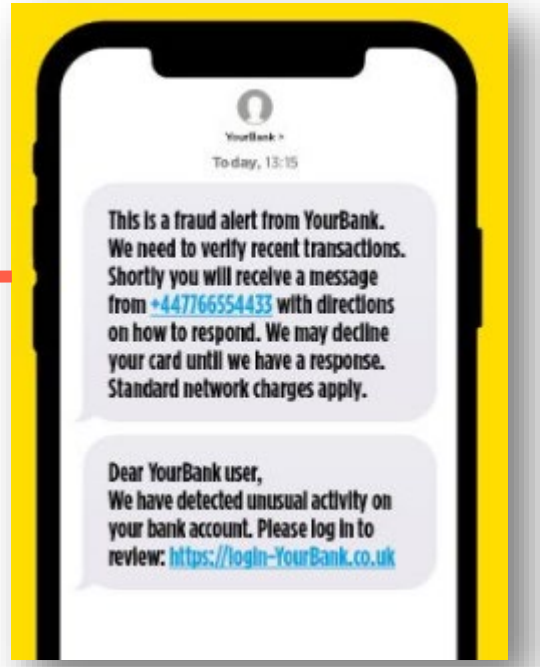
Spoofing

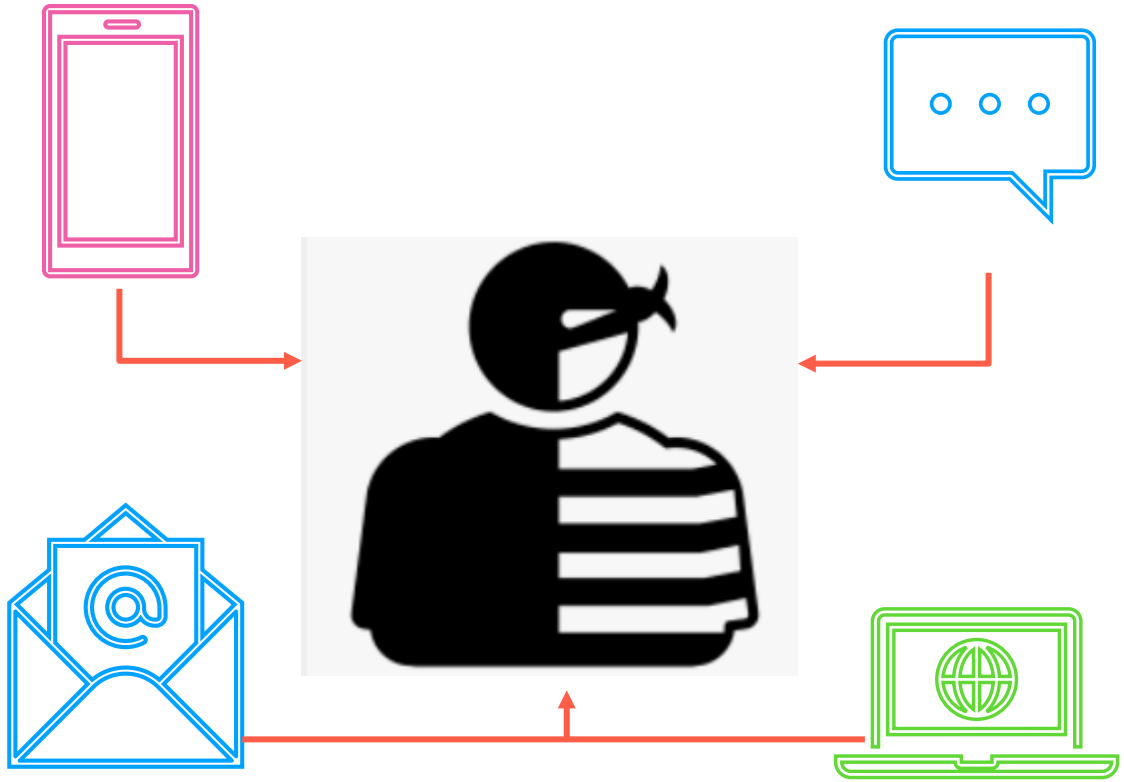
Criminals use a technique called ‘spoofing’ to make it look like you are being contacted by trusted organisation.

These scam calls or texts can often appear in genuine message threads making them difficult to spot.

Spoofing is a type of scam in which a criminal disguises an **email address, display name, phone number, text message, or website URL** to convince a target that they are interacting with a known, trusted source.

SMS Spoofing Example





Spoofing – Key Advice

Know the Signs

Spelling errors, broken links, suspicious contact us information, missing social media badges can all be indicators that the website has been spoofed.

Website addresses containing the name of the spoofed domain are not the official domain

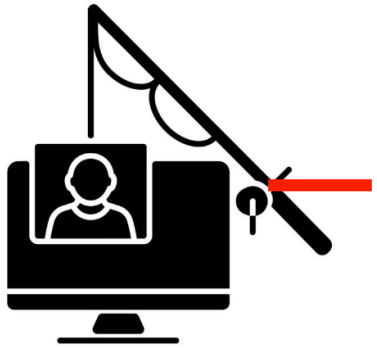
STOP -

Don't be rushed into making a payment of disclosing your personal information

CHALLENGE – Question the source of the call. How the caller got your details and the nature of your query

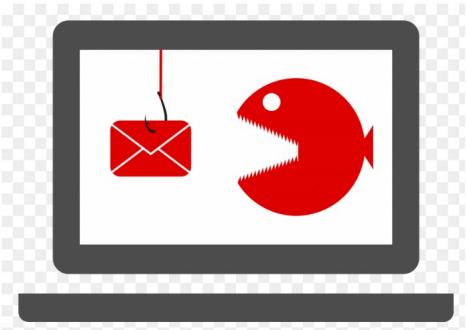
PROTECT – End the call and source the organisations contact details yourself

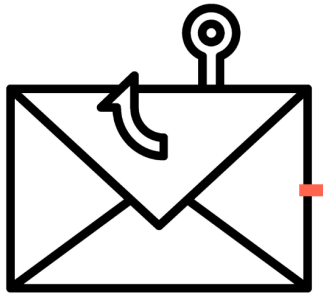
Phishing



Phishing is the attempt by fraudsters to trick you into handing over personal information such as your credit union details, usernames, or passwords via **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.

The criminal typically sends thousands of generic emails out (like bait when fishing – hence the name phishing) to people whose email addresses have been obtained from an unknown source, in the hope of getting a “bite”.





These emails tend to have generic greetings such as “Dear Customer” or “Account Holder”. However, in some cases, a tactic called “spear phishing” is used. In these cases, the fraudster has some detail about you (frequently sourced through social media) and may use your name or some other specific detail about you in the email.

Phishing

The emails try to trick you into clicking on a link in the email by claiming that you need to “verify”, “update” or “reactivate” your account or that you can claim a refund. The link brings you to a bogus website where you are asked to key in your financial or security information. The website will look almost identical to the real thing.

To make phishing emails look like they are genuinely from a well-known company, they include logos and other identifying information taken directly from that company’s website such as your bank, online payment services, or Revenue Commissioners.

The email often imparts a sense of urgency, threatening that your account will be blocked, closed, deactivated or that you will suffer some other negative consequence, if you do not act immediately

Phishing – Key Advice

- Never respond to any unsolicited emails that request personal or sensitive information without first independently verifying the legitimacy of the email.
- Never give away security details, such as your PIN or full online banking password to anyone.
- Never click on a link or attachment in an email until you have verified it is from the source it says it is from.
- Limit or restrict how much personal information you share on social network sites.
- Don’t allow yourself to be rushed; take your time to make the relevant checks.
- Anti-phishing toolbars are included in most web browsers. Ensure that you are using the most up-to-date version of your web browser.

Phishing – Key Advice

- Ensure that your antivirus software is kept up to date
- Be wary of emails that do not use your name and use generic greetings such as “Dear Customer” or “Dear Sir / Madam”.
- 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
- Check your credit union current account and statements regularly and report any unusual account activity to your credit union.
- If you think you have been a target of phishing or have visited a phishing site and provided your details, contact your Credit Union immediately..

Vishing - a combination of the words **Voice** and **Phishing**

current account
from your credit union

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. They 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 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. This information is then used to access your bank account or carry out transactions with your card

Vishing – Variations

Fraud on your Account

- The criminal tells you that there has been fraud on your account and in order to protect the rest of your money you need to move it to a “safe account”.
- They provide you with account details and get you to transfer money out of your account to a fake account (which belongs to the criminals) either via an electronic transfer or via a money transfer service such as Western Union or Money Gram

Technical/ Phone Scam

- You receive a call from a company saying that there is a problem with your PC, laptop or modem (internet / broad band)that urgently needs to be fixed. For more details click here

Courier fraud

- The fraudster makes contact with you by phone, advising you that something is wrong with your card and asking for personal information in relation to the card.
- They then advise you that they will send a courier to collect the card.

Number Spoofing

- The criminal makes contact with you by phone.
- They hide the number they are really calling from and make it look like they are calling from the phone number of the genuine company.

Identify Theft

- Fraudster encourages the victim to check the validity of their identity or to make an immediate report to the Gardaí/Police.
- When the individual hangs up their landline, the fraudster holds the line open (by not hanging up). When the individual picks up the phone again to ring the genuine company or the Gardaí /Police they do not realise that they are still talking to the fraudster

Vishing – Key Advice

Be very wary of any unsolicited phone calls.

Never divulge personal information until you have validated that the caller is a genuine representative of the organisation they claim to represent. You can do this by following a number of steps:

- Advise the caller that you will call them back once you have validated their identity.
- Look up the organisation's phone number (by using the phone book or their website) and make contact directly with them to validate.
- Do not validate the caller using the phone number they have given you (this could be a fake number).
- If the caller is genuine, they will understand and welcome your need to validate them.

Fraudsters may already have basic information about you in their possession (e.g., name, address, dob, account details), do not assume a caller is genuine because they have these details.

Remember that it takes two people to terminate a landline phone call, you can use a different phone line to independently check the caller's identity.

Your Credit Union or the Gardaí /Police will never ask for the following:

- Your credit or debit card PIN number or full online banking password.
- Request you withdraw money to hand over to them or transfer money to another account, even if they say it is in your name.
- To come to your home to collect your cash, payment card or cheque book

Smishing - a combination of the words SMS (text message) and Phishi

Scam where fraudsters send text messages to random mobile phones - the text messages claim to come from a reputable organisation such as a bank, credit union 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 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.

Smishing – Key Advice

Do not respond to unsolicited text/SMS messages before independently validating that it is from the company it says it is from. You can do this by:

Do not validate the texter using a phone number they have given you in the text (this could be a fake number)

Looking up the organisation's phone number (by using the phone book or their website) and make contact directly with them to validate.

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

Do not click on a link, attachment or image that you receive in an unsolicited text without first verifying that the text is legitimate and that you understand what you are clicking on.

Never respond to a text message that requests your 4-digit card PIN or your online banking password or any other password.

If you think you might have responded to a smishing text message and provided your bank details, contact your bank immediately