CYBERSAFETY

EMPOWERING A CYBER-SAFE SOCIETY

Staying Safe Online:

How to Avoid Scams, Stay Informed, and Maintain Privacy.

MTU Ollscoil Teicneolaíochta na Mumhan Munster Technological University
NATIONAL CHALLENGE FUND *From Ingenuity to Research and Solutions*
Rialtas na hÉireann Government of Ireland
Taighde Éireann Research Ireland
Maoinithe ag an Aontas Eorpach Funded by the European Union NextGenerationEU
CYBER EXPLORE
NCSC

© Cyber Safety, 2025. All rights reserved.

TABLE OF CONTENTS

© Cyber Safety, 2025. All rights reserved.

Introduction

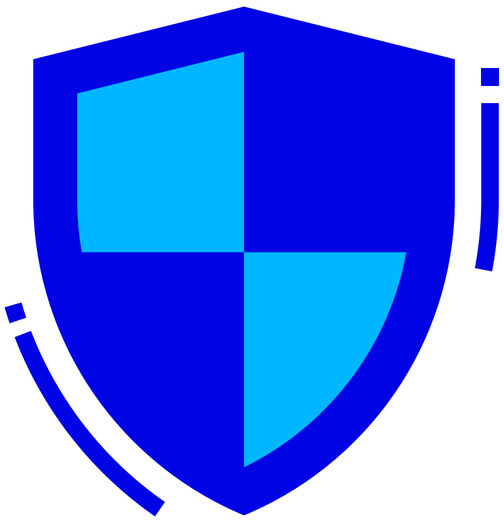
Welcome to the Cyber Safety *"Staying Safe Online"* guide.

Technology has become an invaluable tool for communicating, online shopping and banking, and staying connected with current events.
However, as scams and online fraud rates rise in Ireland, learning how to protect yourself online is becoming more important than ever.

Cyber Safety is a Research Ireland-funded project that develops educational resources to help people of all tech levels stay safe online. Led by cybersecurity experts and informed by human-centred research conducted across Ireland, this guide focuses on answering the concerns we have received from the general public regarding online safety.

In the following sections, you'll find **simple, practical tips** on:

- Identifying scam messages and websites.
- Creating and changing passwords.
- Safe internet usage and how to protect your personal details.
- How to recover if you experience a cyberattack.



Introduction

Firstly, what do we mean by cyber safety, cyber attacks, and cyber hygiene?

Cyber safety means taking measures to navigate the internet and technology safely, in order to protect against scams, fraud, and other forms of **cyberattacks -** these are when someone tries to access your device or personal details to **steal information or cause harm.**

A crucial part of cyber safety involves practising **good cyber hygiene** by:

- Securing your personal devices and accounts with strong passwords.
- Being mindful of what websites you visit, and what personal details you provide them with.
- Ensuring banking details are protected when shopping online.
- Avoiding posting sensitive personal details online.

Let's get started!

Online Privacy Settings

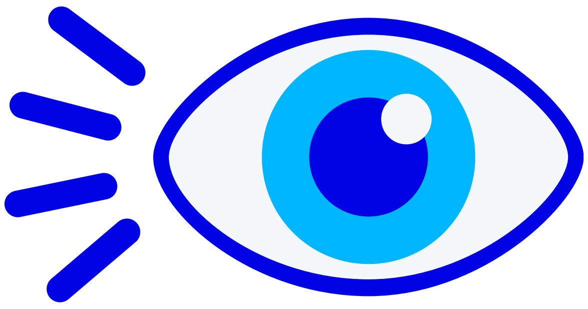
It is important to avoid sharing personal information on social media and freely sharing too much information online.

Try to regularly review what **privacy settings** you have enabled on your social media and who you are “friends” with. Since settings vary by platform, you can check out official guides by searching **“Platform ___ Privacy Settings.”**

Always **check** to see whether your personal information is mandatory for filling in forms online. If it is mandatory, you can often **bypass** this by putting in a pseudonym or using “X’s” to fill in the form fields.

Consider creating a **‘Junk’** email address for less important accounts that require your email details.

Do not save your login information or select “Remember Me” on devices that are not your own, such as library computers. Using public Wi-Fi networks for sensitive transactions such as accessing your banking or online shopping is also **not recommended.**



Staying Private in Public

When entering passwords, PIN codes, or making online transactions in public places, it's important to stay aware of your surroundings. **Shield your screen** and keypad when typing sensitive information, as onlookers could capture your details.

When it comes to **public Wi-Fi** networks, these are often **unsecured**, making it easier for hackers to intercept your data.

For this reason, **disable automatic connection to open networks** on your device. You should also **avoid** making online payments or logging into important accounts while using **public Wi-Fi**, such as in cafés, airports, or libraries.

If you must access sensitive accounts, consider using your own **mobile data** or a **VPN** (Virtual Private Network) to encrypt your connection for added security.

Make sure to always **log out** of accounts when using shared or public devices, and never save passwords on them. Taking these precautions helps protect your personal and financial information from being stolen.

What are Cookies?

Cookies are small files that are downloaded onto your device when you visit a website. They can remember your **browsing preferences**, your **location**, and your **login information**.

There are many types of cookies.

Essential: These are used to remember your activities on a website. They keep you logged in, and remember what you have done on the website, such as what is in your shopping basket and your log in details.

Non-Essential: These include analytics and customisation cookies that track your activity in their browsers. This allows website owners to better see how their site is being used.

Advertising cookies: These are used to customise your ad experience on websites, based on your browsing history and social networking tracking cookies allow users to share content on social media and help link the activity between a website and a third-party sharing platform.

Third-party cookies: These are created by websites other than the one you're currently visiting. They are used to track your activity across different sites, usually for advertising purposes. For example, if you visit a clothing website, third-party cookies might help advertisers show you ads for similar products on other sites.

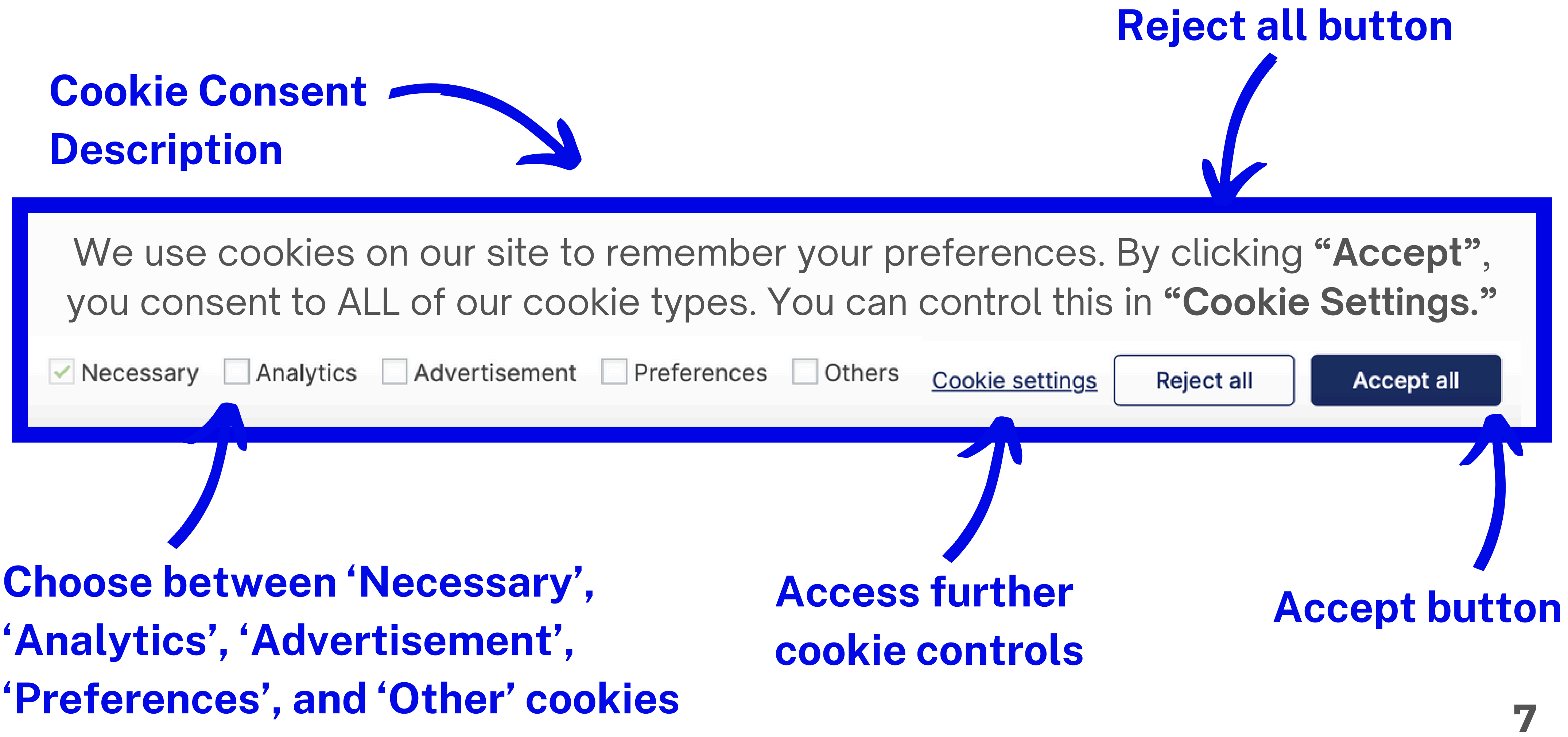
How to Manage Cookies

Cookies can be harmless, but they still contain your personal details. It's fine to accept cookies on sites where you want to receive **targeted** ads and content, **stay logged in** to your account, or **keep track** of items in your cart if you leave a site while online shopping.

However, cookies can also be used by websites to sell your data to **third parties**. When browsing online, you should have the option to **“decline”** or **“manage”** cookies in cookie banners. There may also be a **“reject all”** option if you wish to do that.

If the **“decline”** option is not visible, click **"options"** or **"manage"** and select **“use necessary cookies only”.**

Make sure to click **"save"** to keep these custom settings.



Reject all button

Cookie Consent Description

We use cookies on our site to remember your preferences. By clicking **“Accept”**, you consent to ALL of our cookie types. You can control this in **“Cookie Settings.”**

☑ Necessary □ Analytics □ Advertisement □ Preferences □ Others

Choose between ‘Necessary’, ‘Analytics’, ‘Advertisement’, ‘Preferences’, and ‘Other’ cookies

Access further cookie controls

Accept button

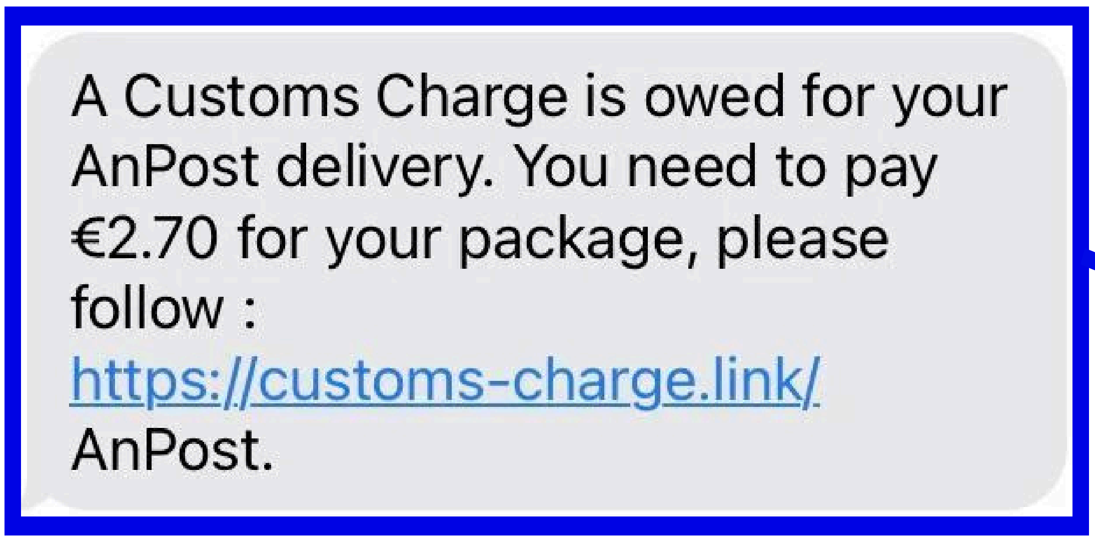
Suspicious Texts (Smishing)

Common scams include fraudulent texts (smishing), calls (vishing), and emails (phishing).

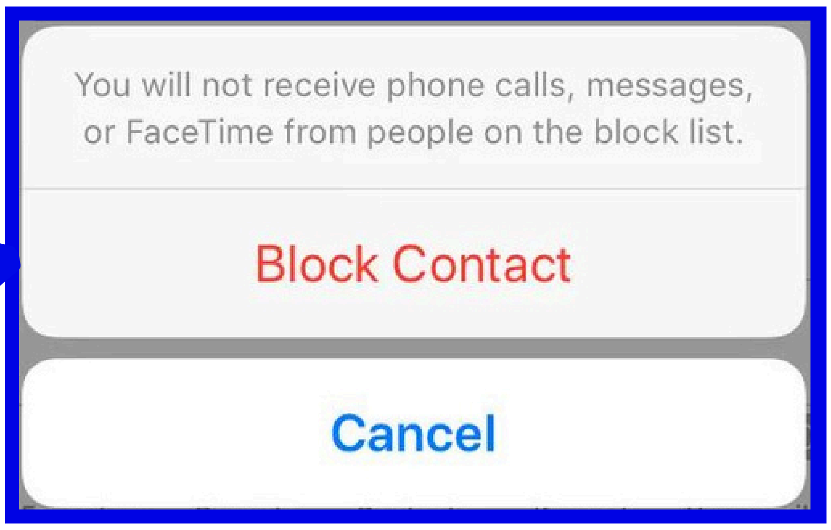
Smishing is a type of cyberattack where scammers use fraudulent messages or websites to trick victims into providing **sensitive information**, such as personal, login, or financial details. It usually happens like this:

Attackers send a **text message** that appears to be from a **legitimate source**, such as a bank, social media platform, or a trusted person. The message may create a **sense of urgency, fear, or curiosity** as **"bait"** to prompt you to act quickly without questioning the legitimacy of the message.

Your personal information can be used for malicious purposes. Be cautious of unsolicited messages, and **verify the legitimacy** of the sender before responding.
If you suspect a message might be a scam, **block the sender and avoid clicking any links or sharing personal information.** This protects you from potential fraud.



A Customs Charge is owed for your AnPost delivery. You need to pay €2.70 for your package, please follow : https://customs-charge.link/ AnPost.



You will not receive phone calls, messages, or FaceTime from people on the block list.

Suspicious Calls (Vishing)

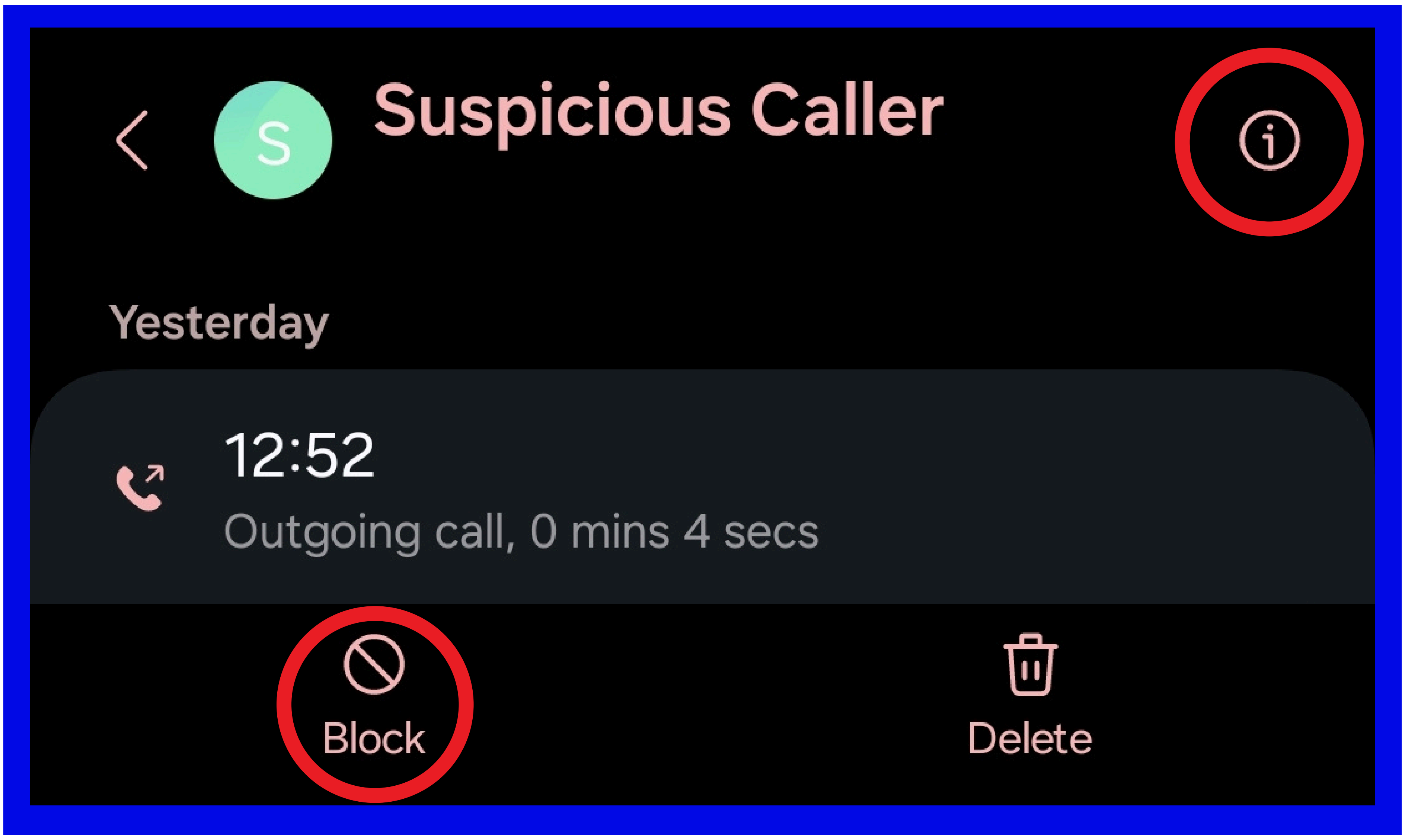
If you receive a suspicious call that you believe is a scammer impersonating an organisation such as a bank or organisation, **do not** share any personal information. Instead, do the following:

1. Hang up **without** providing your name, account number, PIN, or any other sensitive details.

2. If you are nervous about the issue raised in the call being genuine (eg. an unauthorised payment from your card), **contact** the company or organisation **directly** using their official phone number to verify whether they attempted to reach you.

3. Then, use your phone's settings to **block** the caller to prevent future contact.

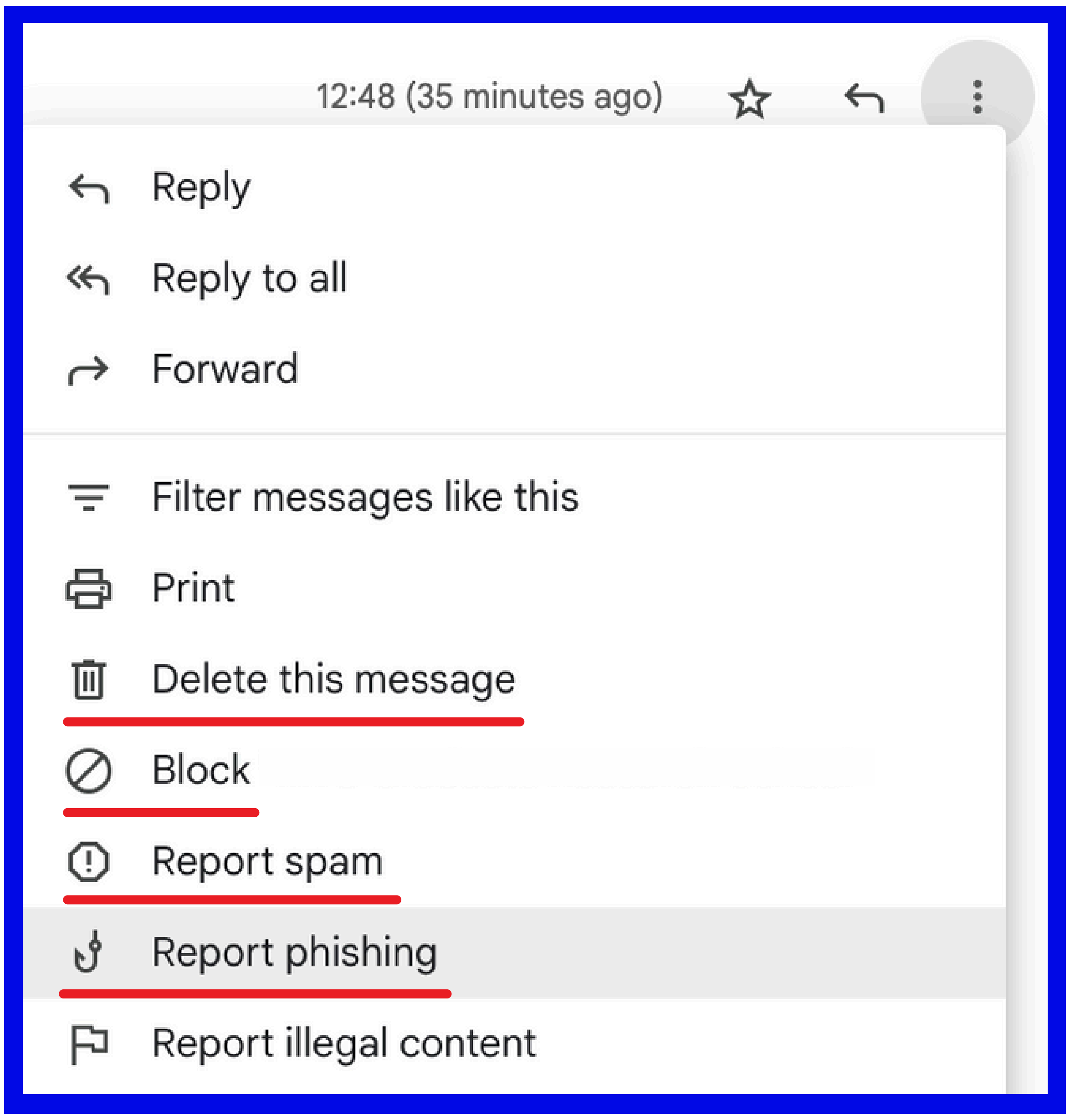
4. If you would like to report the incident, **notify** the organisation the scammer claimed to represent, and **report** the phone call to the Gardaí.



Suspicious Emails (Phishing)

If you suspect an email is fraudulent, avoid interacting with any links or attachments in the message. Instead, do the following:

1. Check the sender's email address for inconsistencies like misspellings. If it claims to be from a legitimate company, contact the company directly using their official channels to confirm.

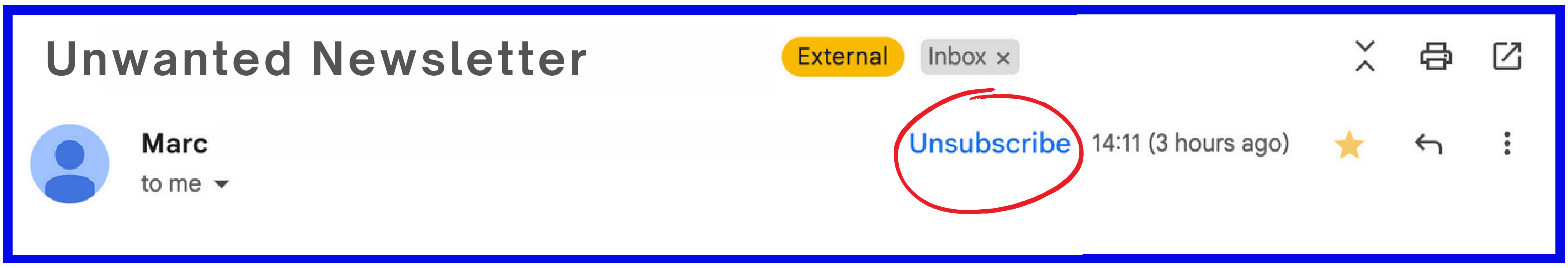


2. Use your email provider's **"Block Sender"** and **"Report Phishing"** options to help block similar messages in the future.

3. Once reported, **"Delete"** the email from your inbox to avoid interacting with it.

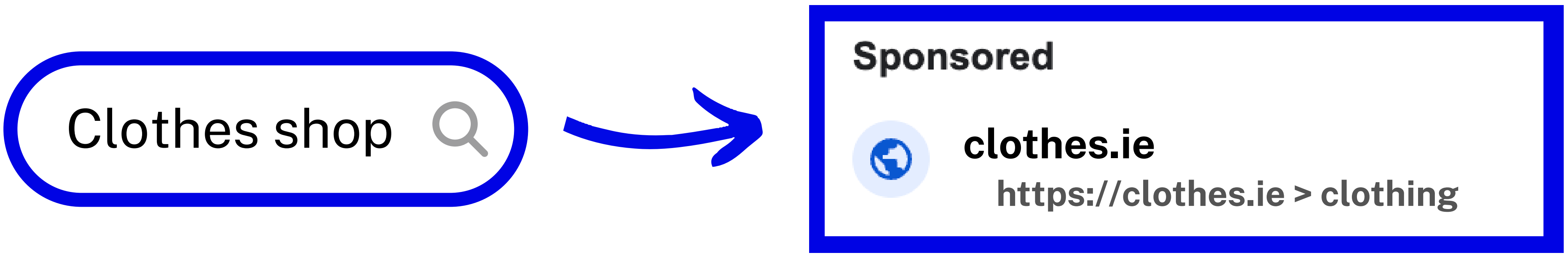
4. If you accidentally clicked a link or provided information, change your passwords immediately and check for unusual activity on your accounts.

Bonus tip: If you have subscribed to a spam newsletter, **one-click unsubscribe** in Gmail can automatically request removal of your email address from its mailing list.



Online Advertisements

Sponsored links, or paid ads, are links that businesses pay search engines (like Google or Bing) to display prominently on search results pages. These links are marked with small labels like **"Ad"** or **"Sponsored"** to distinguish them from "organic" search results.



Clothes shop

Sponsored

clothes.ie
https://clothes.ie > clothing

Search engines aim to show ones that match the keywords or topics you searched for, as ads generate revenue for them.

Many trustworthy businesses use sponsored links for visibility. However, some ads might lead to untrustworthy websites, especially if they are poorly monitored.

To use sponsored links safely, make sure you:

- **Hover** over the web address (URL) to ensure it leads to a trusted, official website.
- Look for clear information about the product or service **before clicking or making a purchase.**
- **Cross-check** the sponsored link with "organic" search results to see if it is too good to be true.

Scam Websites

When browsing a website, if you are still unsure if it is legitimate or not, check the following:

1. **Double check the website's URL** for inconsistencies or misspellings.

2. Be wary of sites found through **unsolicited emails or pop-up ads**, especially if they request personal or financial information.

3. Be cautious if the website **lacks secure payment options** like PayPal.

4. Watch out for **spelling and grammar errors** in the site.

5. Scam websites often lure shoppers with discounts that seem **too good to be true**. Be cautious and research the legitimacy of the site before making any purchases.

6. If in doubt, you can copy and paste a link into

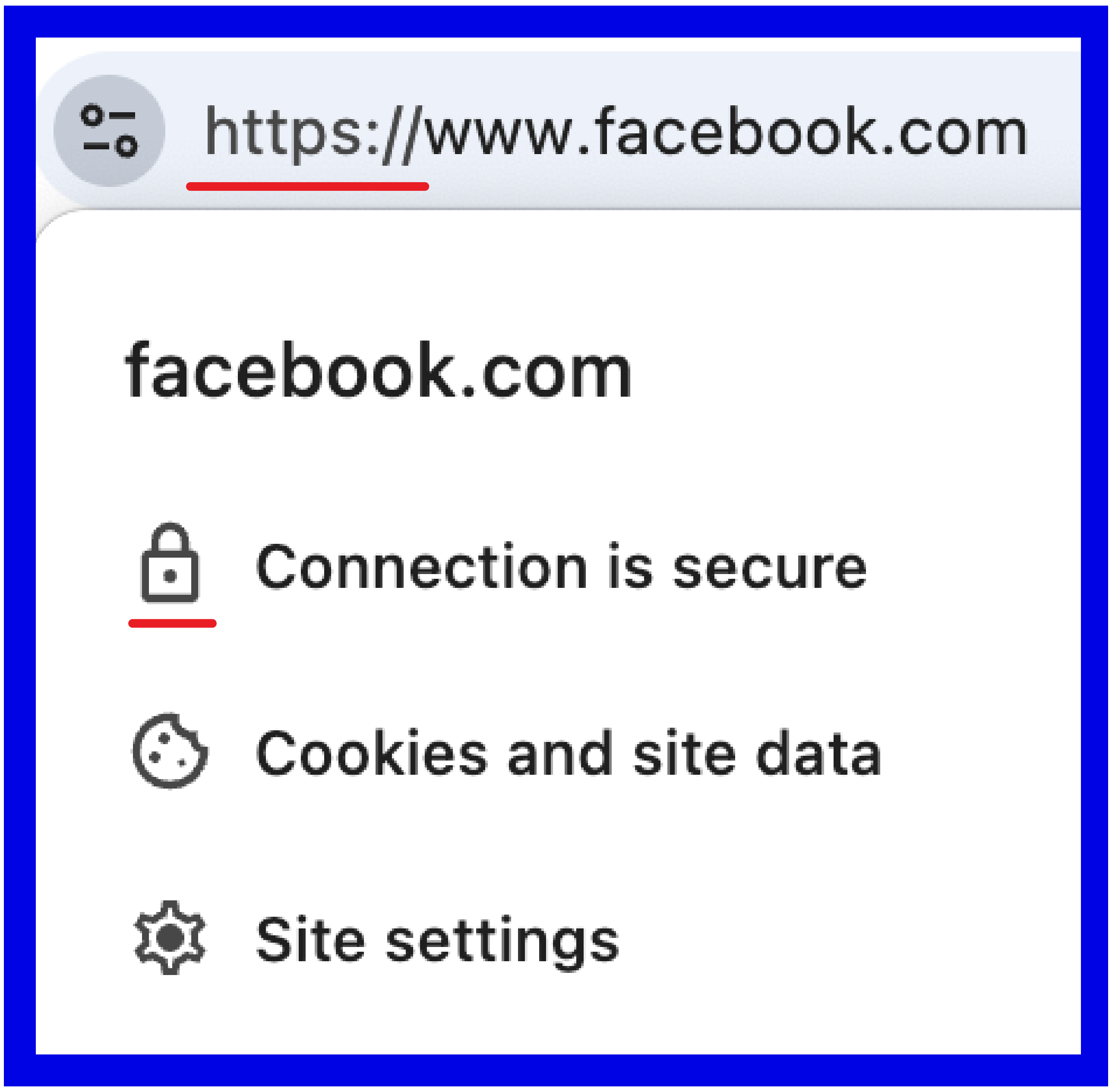
check.cyberskills.ie

to see if it is legitimate.

If you are still in doubt, **avoid clicking the link.**

Online Browsing

There is a common misconception about HTTPS encryption. The **padlock symbol** and **"https://"** in website's URLs indicate that information entered into a site is “encrypted” - this gives the false impression that a site is legitimate.



https://www.facebook.com

facebook.com

Connection is secure

Cookies and site data

Site settings

Both fake and legitimate websites can set up this **HTTPS encryption** by applying for an SSL certificate, so it is not a definite indicator of a sites safety - it just means that the connection between your browser and the website server is encrypted.

It is recommended to check if a site has a "https://" prefix before entering passwords or card details, but it **does not guarantee complete safety** when browsing.

Creating Strong Passwords

When creating a password, try to:

- Make it **at least** 12 characters long.
- Use a combination of uppercase letters, lowercase letters, numbers, and symbols. Spaces are also valid characters in a password.
- Make it easy for **you** to remember but difficult for **others** to guess. (For example, through a string of word association.)
- Consider using a memorable **passphrase** like "I-make-Tea-at-9:30am". If you are using personal associations for your password (like a childhood memory), combine it with random elements to make it more unique (e.g., "Blue Bicycle Was My 1st Toy".)
- Use unique passwords for your **most sensitive accounts**, such as your banking and email. If your account information is compromised from one site, those credentials can be tried on other sites, hoping you've reused the password elsewhere. This is known as a **"Credential stuffing attack".**

Protecting Passwords

Once you've created a password:

- Do not share your passwords for sensitive accounts unless absolutely necessary (eg. with a trusted family member).

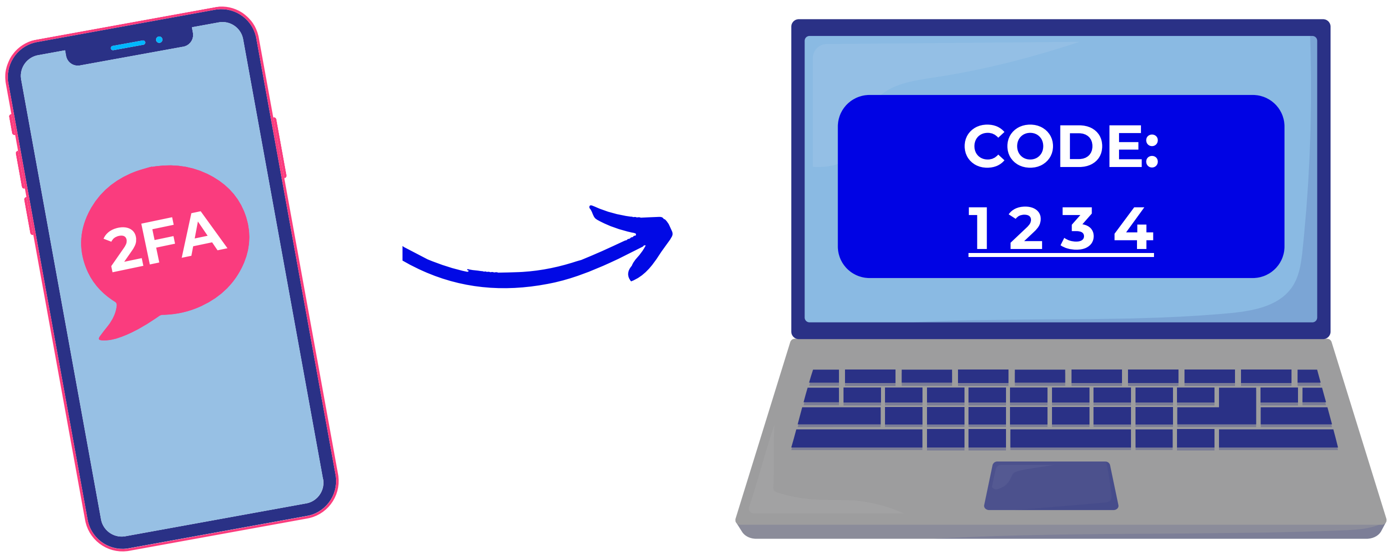
- Never send a password by email, text, or any other method that is not secure.

- If you don't want to memorise multiple passwords, consider using a **password manager.** This is an online tool that stores and encrypts your passwords so you only have to remember one master password.

- It's also fine to write your passwords down, as long as you keep them in a safe place.

- Change passwords immediately on accounts you suspect may have been compromised.

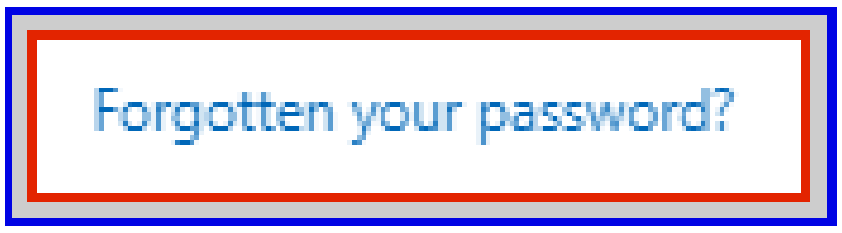
- You can also enable **two factor authentication**. This is an added security measure that requires **two separate forms of identification** - a password and a notification with a code sent to your smartphone. 2FA is often used for online banking and payments, and can be enabled on a number of accounts such as email and social media. Examples of these include Authy and Microsoft Authenticator.



Changing Passwords

If you need to change your password, follow these steps:

1. Visit the login page of the account you need to recover your password for. Look for options such as **"Forgot Password?"** or **"Need Help Signing In?"** and click on it. This is the easiest way to change a password if you forget it ***or*** if it is **compromised,** meaning that someone **unauthorised** has gained access to your details.


Forgotten your password?

2. Then, provide **verification** to confirm your identity - your email address, phone number, or answers to security questions.

3. The website will then send **instructions** to **reset** your password. This may involve **clicking on a link** in an email or **entering a verification code** sent to your phone.

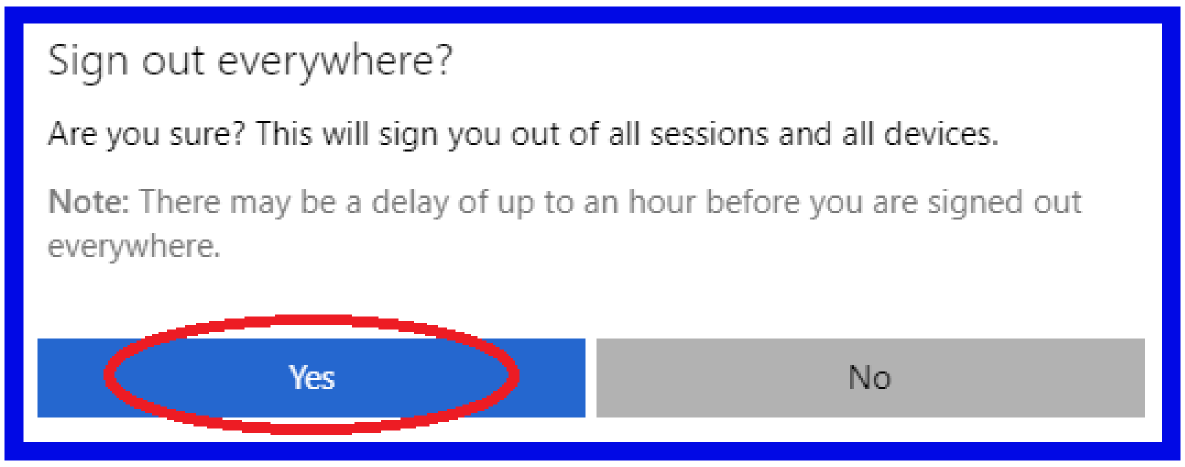
4. **Create a new password** for your account. Store this safely. Use unique passwords for your important accounts, with **at least 12 characters** (Remember the passphrase technique, e.g. **Is.this.a.Toyota?**)

5. Remember to consider enabling **two-factor authentication**, meaning you can use **two forms of identification** in order to access an account (usually a password and a text).

Responding to a Cyberattack

If you notice suspicious activity and believe you have been compromised, take the following steps:

1. Immediately change any compromised passwords.
If there is a **“Log out of all devices”** option, select this to remove any unauthorised access to your account.



Sign out everywhere?

Are you sure? This will sign you out of all sessions and all devices.

Note: There may be a delay of up to an hour before you are signed out everywhere.

2. Contact the compromised account’s **service provider** (For example your bank or An Post.)

3. Check important accounts that contain personal or banking details for any unusual activity. Then, check your other accounts, such as your email, banking, or any other account that contains personal or banking details. This can avoid multiple accounts being compromised, or malicious messages being sent to your contacts.

4. You can contact your local Garda station to report the crime and request a **PULSE ID.** This is a number allocated to an incident in the Garda system, which means the Gardaí have opened a criminal case.

5. You can then **provide the PULSE ID to your service provider** to show that you were a victim of a crime.

Notes

CYBER SAFETY

Get in touch:

✉ cyber-advice@cyberskills.ie

www.cybersafety.ie

If you have fallen victim to a cybercrime, you can contact
the **Crime Victims Helpline** on
Freephone: 116006 or **Text: 085 133 7711**
for emotional support and information.

MTU
Ollscoil Teicneolaíochta na Mumhan
Munster Technological University

NCSC
National Cyber Security Centre

CYBER EXPLORE

NATIONAL CHALLENGE FUND
From Ingenuity to Research and Solutions

Rialtas na hÉireann
Government of Ireland

Taighde Éireann
Research Ireland

Maoinithe ag an Aontas Eorpach
Funded by the European Union
NextGenerationEU