CYBERSAFETY

EMPOWERING A CYBER-SAFE SOCIETY

5 Tips for Safety Online

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
CYBERSKILLS
NCSC

Introduction

Welcome to our guide on cybersafety! Here, you'll find tips to help you stay safe online and avoid cyberattacks.

Cybersafety means taking measures to navigate the internet and technology safely, in order to protect against scams, fraud, and other forms of cyberattacks.

Cyberattacks are when someone tries to access your device or personal details to steal information or cause harm.

A crucial part of cybersafety 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.

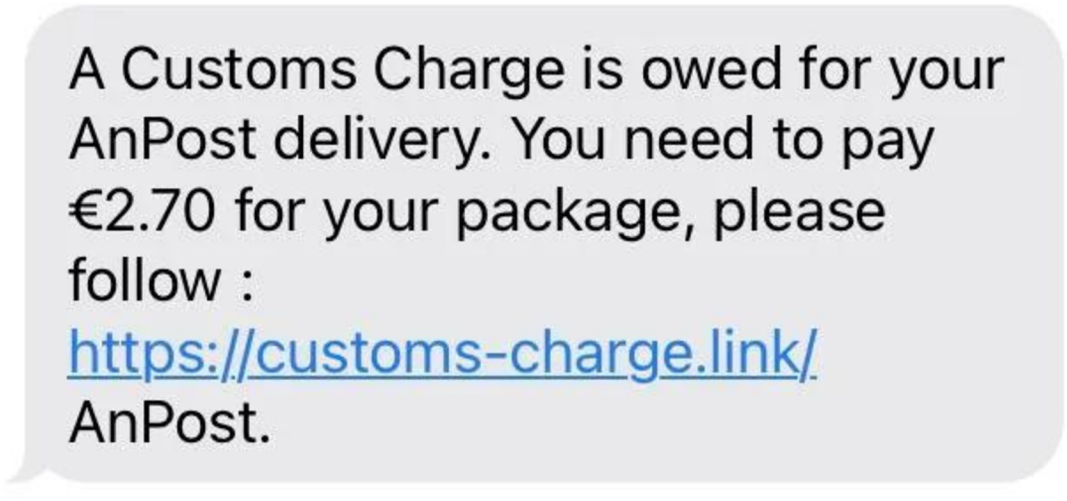
Avoiding Scam Messages

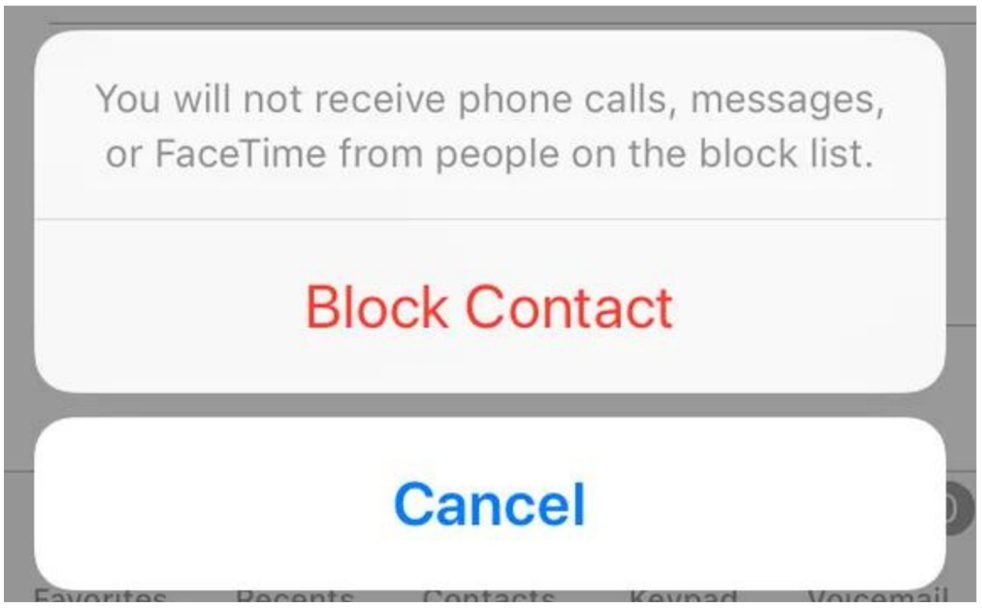
Common scams include fraudulent texts, calls, and emails.

Phishing 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 an **email or 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.**





Avoiding Scam Websites

When browsing the internet, if you are unsure if a site is legitimate or not, check the following:

1. **Check the website's URL** (web address) 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.

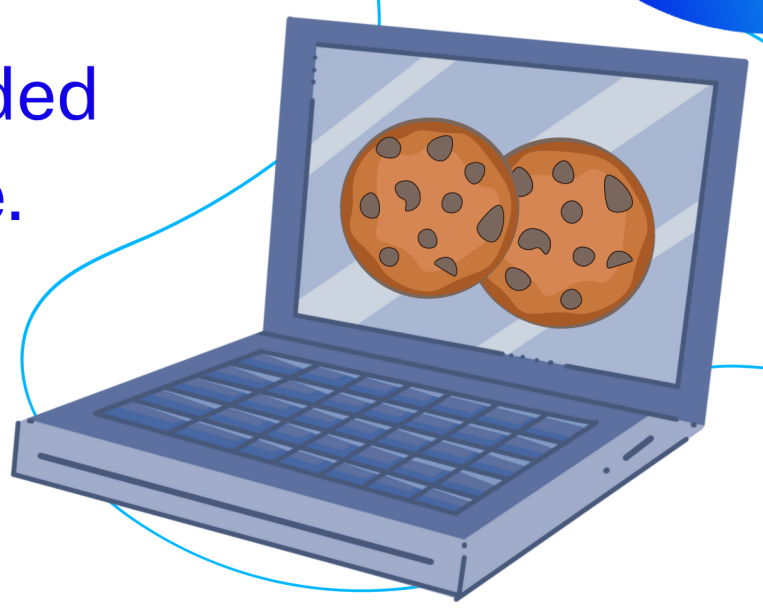
5. Scam websites often lure shoppers with discounts that seem **too good to be true**. Be cautious and research the legitimacy of the site before making any purchases.

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.

Staying Private Online



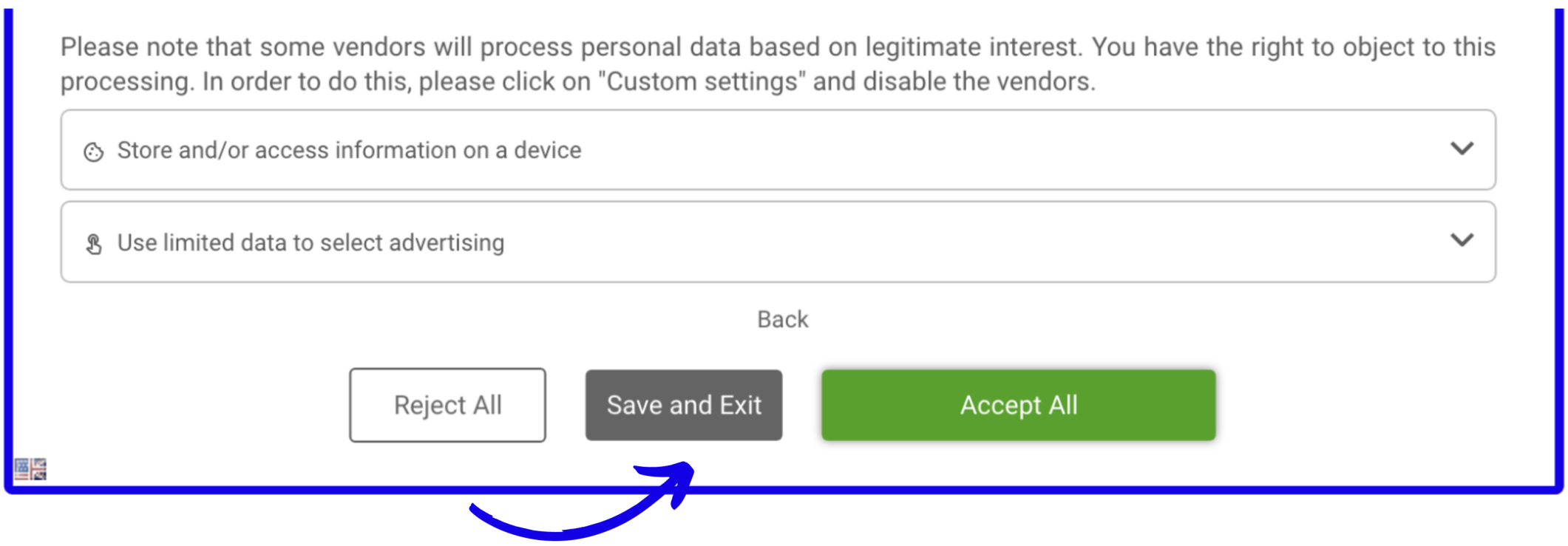
Cookies are small files that are downloaded onto your device when you visit a website. They can remember your **browsing preferences**, your **location**, and your **login information**.

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 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.



Managing Passwords

Passwords are essential for protecting your accounts.
If you need to change your password, follow these steps:

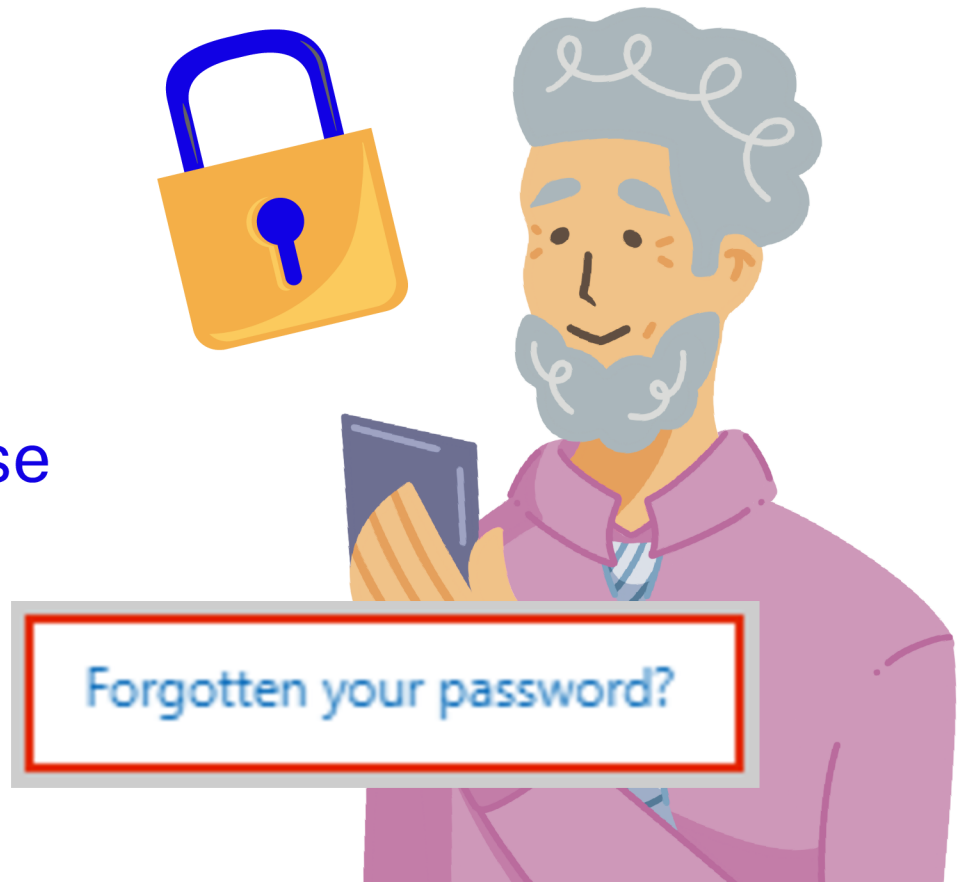
1. Visit the login page of the account you need to recover your password for. Look for options such as **"Forgot Password?"** or **"Need Help Signing In?"** and click on it. This is the easiest way to change a password if you forget it **or** if it is **compromised,** meaning that someone **unauthorised**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

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** (Think of a memorable phrase, e.g. **I-make-tea-at-9:30am**).

Also 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 Cyberattacks

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.

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 other unusual activity.

4. Then, you can go to 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.

Stay safe online!

CYBER
SAFETY

Get in touch:

cyber-advice@cyberskills.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
sfi Science Foundation Ireland
CYBERSKILLS
NCSC National Cyber Security Centre
National Challenge Fund — From Ingenuity to Research and Solutions
Rialtas na hÉireann Government of Ireland
Maoinithe ag an Aontas Eorpach Funded by the European Union NextGenerationEU