



CYBER
SAFETY

E-Learning Course Companion Guide

CyberSafety for Vulnerable Populations,
2025.





CYBER
SAFETY

TABLE OF CONTENTS

Table of Contents	01
Introduction	02
Icebreaker Activity: Cyber Safety Stories	03
Password Strength Challenge	05
Spot the Scam	08
Cybersafety Quiz	12
Data Detective	15
Cyber Safety Emoji Quiz	18
Cookie Conundrum	20
Cyber Safety Role-Play	23
Two Truths and a Lie	28
Cyber Safety Wordsearch	33

Introduction

This companion document includes ten activities made to share what you have learned from the Cyber Safety E-Learning Course, with Digital Newcomers, or anyone else interested in learning about Cyber Safety.

This collection features a variety of engaging and educational activities, ideal for group or solo lessons, and at-home learning. Inside, you'll find a mix of printable resources and activities that can be presented for classroom use.



We hope these exercises inspire creativity and foster meaningful learning experiences for you and any individuals you work with.

Please visit our website to contact us with feedback at cybersafety.ie.

- The Cyber Safety team

1. Icebreaker Activity: Cyber Safety Stories

Objective: Reflect on personal or public experiences of cyberattacks to prompt discussion and learn from others.

Activity:

This activity can act as a quick icebreaker to prompt conversation within the group.

The tutor, or participants, if comfortable doing so, can share a time when they or someone they know encountered a cybersecurity challenge (e.g. a phishing email or a hacked account) and explain how they responded. The group can put forward lessons learned, and ideas for how they think they should react in a similar situation.

Then discuss strategies to prevent similar situations in the future.

An example persona story is included on [Page 4](#) in case the participants or tutor aren't comfortable sharing a personal example.



Persona Example: Máire's Story

Name: Máire Murphy

Age: 37

Occupation: Teaching Assistant



Máire, a 37 year old teaching assistant loves staying connected with her family and friends online. She uses her email daily to keep in touch and occasionally shop online. One morning, she received an email from what appeared to be her bank. The subject line read: **“ACCOUNT SUSPENDED: Confirm your phone number”**

The email looked official, with her bank's logo and a warning that her card and account would remain frozen unless she confirmed her contact details within 24 hours. The email included a link labeled: **“Verify Your Account Now.”** She remembered making a purchase on a new website the week before, and worried that it had compromised her banking information somehow.

Feeling panicked, she clicked the link. It directed her to a webpage that looked exactly like her bank's website. Trusting its appearance, she went to enter her phone number and password.

However, she decided to call her bank directly using the Customer Service number on her bank card. The representative informed her that there had been no unusual activity on her account, and the email was a phishing attempt - a cybercriminal had **created a realistic imitation website to try and steal her information.**

XX1223075780XX (IE))



Bank of Ireland

info@jdecorconcept.be

To **Bank of Ireland** info@jdecorconcept.be

Monday, 28 January, 11:03

Bank of Ireland

We have automatically suspended your account.

This is because your accounts may have been accessed from two different devices (a PC, Laptop, Tablet or Mobile), within a short period of time.

We have been trying to contact you to inform you that your account has been placed on hold due to possible errors.

After you provide us a valid phone number, you will receive a phone call in 24-48 hours to confirm your data.

[Confirm your Contact Number >>](#)

The following notifications are important.

© 2018 Bank of Ireland

Contact us



Bank of Ireland Help centre
Frequently asked questions



@talktoBOI
Talk to us on Twitter



365 online Service Desk
Login to 365 online



Boards chat forum
Talk to us on Boards.ie



Send us a mail
Fill out a quick form online



Useful Numbers
Useful & Freephone emergency numbers



Reply

Bank of Ireland 365 online

Welcome to 365 Online

Secure Login

Please enter your Date of Birth: 11 / 11 / 1911

Please enter the 1st, 2nd and 3rd digits of your PIN: 111

[Forgot details](#) [Register](#) [Continue](#)

Stay safe and secure. We will never email you requesting your online login details - please report any suspicious emails to 365secure@boi.com

What Máire Learned:

After working with her bank to secure her account, Máire took steps to protect herself in the future:

- She learned to never click on links in unsolicited emails.
- She now verifies any suspicious communication by calling the organisation directly.
- Máire also started using two-factor authentication to add an extra layer of security to her accounts.

2. Password Strength Challenge

Objective: Teach participants about creating strong, secure passwords.

Activity:

Divide participants into small groups.

Show the **Password Creation Guidelines**, attached on [Page 6](#), and discuss them as a group.

Challenge each participant/group to write down a strong and memorable passphrase (eg. I-make-Tea-at-9:30am) using limitations such as:

- Making it at least 12 characters
- Including uppercase and lowercase
- Including numbers and symbols
- Trying Camel Case “YouPutATimeMachineInADeLorean?”

Compare each result between the groups.

You can then discuss how they can make their passwords more secure and where they should be stored (written down in a secure place, or in a password manager.)

Password Reset Guidelines are also included on [Page 7](#) for participants to reference at home.





Creating a Password



When creating a password, try to:

- Make it at least 12 characters long.
- Use a combination of uppercase letters, lowercase letters, numbers, and symbols.
- Create something significantly different from your previous passwords.
- Make it easy for you to remember but difficult for others to guess.
- Consider using a memorable passphrase like "I-make-Tea-at-9:30am".

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 message, or any other method that is not secure.
- Use unique passwords for your most sensitive accounts. 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".
- If you don't want to memorise multiple passwords, consider using a password manager.
- 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 (2FA) to require both a password and a one-time code generated by an app on your phone. This adds another layer of security.

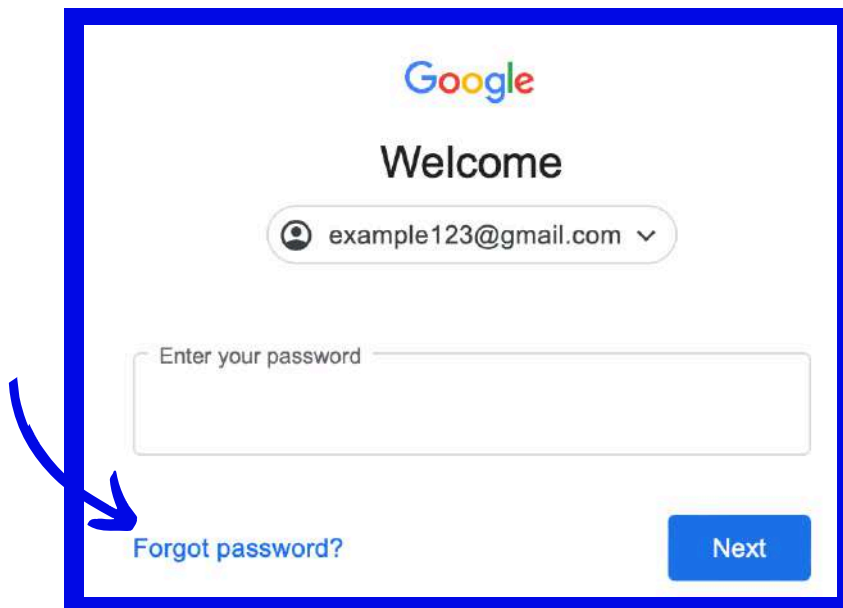


Resetting a Password



If you need to reset a password:

1. Access the Password Recovery Page: Visit the login page of the website or service for which you need to recover your password. Look for an option such as "Forgot Password?" or "Need Help Signing In?" and click on it.



The screenshot shows a Google login interface. At the top is the Google logo, followed by the word "Welcome". Below this is a text input field containing the email address "example123@gmail.com" with a dropdown arrow. Underneath is a larger text input field with the placeholder text "Enter your password". At the bottom left, there is a blue link that says "Forgot password?". To the right of this link is a blue button labeled "Next". A thick blue rectangular border surrounds the entire login area, and a blue arrow points from the left side of the border to the "Forgot password?" link.

2. Provide Information: You may be asked to provide verification information to confirm your identity. This could include your email address, phone number, or answers to security questions that you set up when creating your account.

3. Receive Recovery Instructions: After providing information, the website will send instructions on how to reset your password. This can be in the form of an email, text message, or notification.

4. Follow Recovery Instructions: Follow the instructions provided to reset your password. This may involve clicking on a link in an email or entering a verification code sent to your phone.

5. Create a New Password: You will then be prompted to create a new password for your account. Remember to store this password safely after resetting it.

3. Spot the Scam

Objective: Improve skills in differentiating between genuine messages and phishing or scam messages.

Activity:

Provide participants with printed examples of fake emails and text messages, attached on [Pages 9-11](#).

Have them work individually or in pairs to identify and circle signs of phishing (e.g., misspellings, suspicious links, requests for personal information).

Then show the examples of legitimate messages, so that participants can discuss whether they would have believed them to be genuine or not if they received them.

Debrief and discuss as a group, and write a checklist to identify what the most common "Phishing Red Flags" are to watch out for.



Text Message Scam Examples


eFlow: Hi, our system has recorded that you have missed two payment deadline dates, please proceed to <https://motorway-penalties.net/> to avoid incurring any further penalty charges. Failure to acknowledge this penalty notice will result in a court summons and on conviction a fine of up to €5000.00

Hey mam texting you off a friend's phone I broke my phone. I'm currently using an old phone, this is my new number [+353834434533](tel:+353834434533) save it and Whatsapp me please.

BOI: We have temporarily restricted access on your BOI account due to suspicious activity, to re-authenticate visit: online365-verify.com

< OPEN24

Tuesday 8 February 2022

 Attempts have been made on your card at 11:28
Please secure account: open24securiyouonline-review.com
Thanks, PTSB

12:41

eFlow: Your eFlow account will be disabled, due to failure to accept the new update. To accept Please visit: <https://e-flowaccount.com/due>

gov ie: You are eligible for a discounted electricity bill under the Energy support scheme. You can apply here: <https://register-refund-esb.com>

AN POST: Your package has a €1.99 unpaid fee. To pay this visit anpost-online-reschedule.com If this is not paid the package will be returned to sender

Email Scam Examples

From: BOI - Notification <test@boulangerboisvert.com>
Date: 23 September 2020 at 14:43:44 BST
To: [REDACTED]
Subject: BOI - Notification #31335213
Reply-To: vr4nk09b99ezhecamlvxc4@hotmail.com



Bank of Ireland

New Mobile Banking app

What do you need to get ready?

Make sure that you have your most up-to-date mobile phone number registered to your online banking profile.

[Check that we have your correct mobile](#)

©2020 Bank of Ireland

From: Revenue Online Service <noreply@legal-ros.ie>
Sent: 14 August 2023 10:59
Subject: [ACTION REQUIRED] Time-Sensitive Information



Dear

You have been selected for an audit. We chose to audit you for any one of the following reasons:

- to analyse your business accounts or tax returns
- to check someone else's records (such as your employer or a bank that pays you interest) and match them to your records
- information received in another audit which suggests your records should be checked
- your compliance record (whether you have kept to the tax laws in the past)
- your payment record (whether you have paid your taxes on time in the past)
- selecting a particular industry
- examining a particular issue or problem that affects a group of taxpayers
- where you live, or run your business (if we are auditing a particular area)
- local knowledge, perhaps arising from media reports or unexplained wealth
- information we get from other people about you
- we may choose you randomly

At this time, we ask that you please schedule your audit immediately. Failure to schedule your audit by August 21, 2023 will result in financial penalties.

[Schedule Audit](#)

For more information about the Inland Revenue audit process, visit our [About audits](#) webpage.

Sincerely,
Revenue Online Service

Refund invoice ID:
87388229479223203/2022/
P87074



Revenue Commissioners
to me ^



From Revenue Commissioners • support114a374d
0577744abff0ad9a394bd042@forcus.co.jp

To

Date

[See security details](#)



Dear Taxpayer,


We would like to notify you that you still have an outstanding tax refund of **362.48 £** from overpaid tax from year ending 2021.


*** You have until 29 August 2022 to make your claim**
[Claim Your Refund Now \(Login Now\)](#)

myAccount

(Reference No: 2402487717295124/2022/P871)

Legitimate Message Examples





1 security issue found on your account


We've upgraded the Security Checkup to give you specific, personalized recommendations to strengthen the security of your Google Account.

Take the [2-minute checkup](#) today to see the actions you should take to make your account more secure.

TAKE ACTION

Security Checkup is available in My Account (<https://myaccount.google.com>)



You received this email to let you know about important changes to your Google Account and services.
© 2018 Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA



Change your password

The password that you just used was found in a data breach. Google Password Manager recommends changing your password now.

OK

  **AnPost**

Item CA575033743IE details have been shared by the sender. Download our app to see updated tracking once it arrives with An Post

Saturday, 7 Dec • 23:10

Item CA567407877IE is due for delivery on the next working day. Manage delivery options here pm.anpost.com/CA567407877IE/O539475357

  **AIB**

Sunday, 15 Sept • 15:49

Your AIB verification code is 302336. This code lasts for 5 minutes. Do not disclose this code to anyone, even us. If you didn't request this code, please call us.

There's a new message for you in the Portal. AIB

09:17

4. Cybersafety Quiz

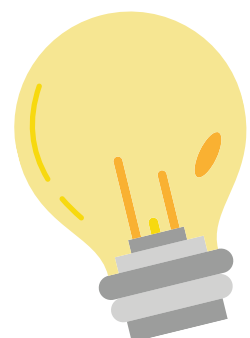
Objective: Reinforce knowledge on cybersafety concepts.

Activity:

On [Page 8](#) there is a quiz with 10 quick fire questions covering topics such as "Cookies," "Phishing," "Data Privacy," and "Passwords.", with varying levels of difficulty.

The answers are on the following page.

Let participants compete in teams or solo to complete the quiz, then check the answers together. You can add a competitive element by rewarding the team with the highest score.



Cyber Safety Quiz

- 1** What is phishing?

- 2** Name two ways to identify a phishing email.

- 3** What does VPN stand for?

- 4** What should you do if you receive a suspicious link in a text message?

- 5** What are cookies?

- 6** Name two types of cookies that websites use:

- 7** What is one way to limit the amount of personal information you share online?

- 8** What is two-factor authentication, and why is it important?

- 9** What's the first step you should take if one of your accounts is hacked?

- 10** What is one way to protect your devices when using public Wi-Fi?

Cyber Safety Quiz Answers

- 1** What is phishing?

A type of scam where attackers trick people into providing sensitive information by pretending to be a trusted entity.
- 2** Name two ways to identify a phishing email.

Check for spelling mistakes, illegitimate links that don't match domains, strange attachments, unpersonalised information.
- 3** What does VPN stand for?

Virtual Private Network.
- 4** What should you do if you receive a suspicious link in a text message?

Do not click on the link, copy and paste it into check.cyberskills.ie to verify or hover over it with a mouse to view the actual domain destination.
- 5** What are cookies?

Small files stored on your device by websites to remember your preferences and track activity.
- 6** Name two types of cookies that websites use:

Necessary cookies, marketing cookies, or third party cookies.
- 7** What are two ways to limit the amount of personal information you share online?

Adjust privacy settings on social media, decline unnecessary cookies, and avoid oversharing.
- 8** What is two-factor authentication, and why is it important?

A security method requiring two forms of identification to sign in, making it harder for attackers to access accounts.
- 9** What's the first step you should take if you suspect one of your accounts is hacked?

Change your password immediately, log out of all devices, and check for other unusual activity.
- 10** What are two ways to protect your devices when using public Wi-Fi?

Use a Virtual Private Network (VPN) to encrypt your internet connection, avoid accessing sensitive accounts, like banking or email, over public Wi-Fi, and disable automatic connection to open networks on your device.

5. Data Detective

Objective: Raise awareness about how much personal information can be harvested from what people share online.

Activity:

Ask participants to review each of the mock social media profiles (Facebook and Instagram), on [Pages 16 and 17](#).

(If in a group, you could also view the social media profile of a consenting participant.)

Identify what personal information could make someone vulnerable to hacking (e.g., birthdate, address, check-ins at locations, posting about holidays).

Discuss strategies to limit personal information shared online by utilising privacy settings, while maintaining connections with family and friends.





Maire

Home



Máire Murphy

Teaching Assistant at Killeagh Primary School



Timeline

About

Welcome

More ▾

About Me

Name: Máire Murphy

Birthday: March 15, 1990

Lives in: Killeagh, Co. Cork

Education: Sacred Heart Secondary School, Class of 2008; University College Cork, Class of 2012

Work: Teaching Assistant at Killeagh Primary School

Email: maire.murphy@gmail.com

Relationship Status: Married June 12, 2015



Weekly morning walks with Roo <3

at [Inch Beach](#)



Tom just surprised me with tickets to see his parents in Portugal in June!!! Feeling excited (:



Robbie having a sprint through the woods this morning .. Can't believe hes 10 already !!



Máire Murphy created an event

6 minutes ago



Lilys 5th Birthday Bash!!!
18th May at Cork Play Centre, 2-5pm

RSVP



Comment



Share



Máire Murphy added a photo

2 days ago

Finally got the keys, so excited to step into our forever home! - with [Thomas Murphy](#)



Comment



Share

kieran.o.dr



90
Posts

3240
Followers

1023
Following

Kieran O'Driscoll

@marie.donovan ❤️🔒 29/11/2024

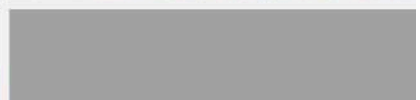
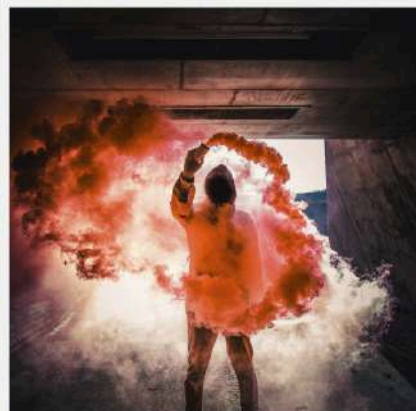
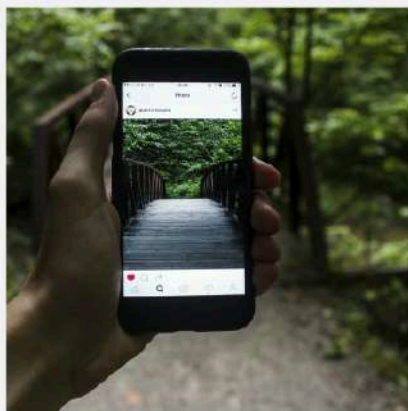
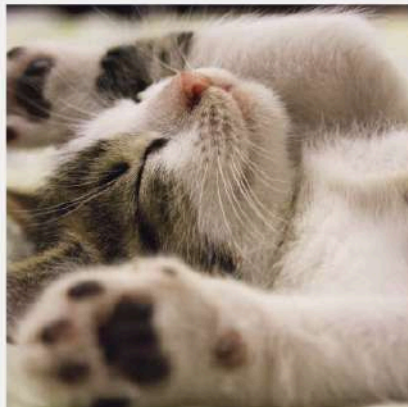
2nd year Psychology UCC

Limerick born and bred 100

Snap @kierano2004

Follow

Featured Stories



6. Cyber Safety Emoji Quiz

Objective: This is a rapid-fire activity where participants guess the meaning of each emoji set that represents cybersecurity terms, concepts, or scenarios.

Activity:

Show on screen or print the list of emoji combinations on [Page 19](#), each representing a cybersecurity-related term, action, or concept.

Participants can write down or guess aloud what they think the emojis represent.

After everyone has guessed, reveal the correct answers and discuss their meanings.

Answer sheet:

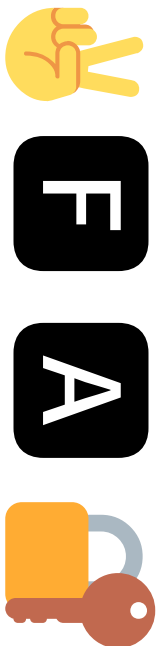


Cyber Safety Emoji Quiz Answers

 <p><u>Public Wifi</u></p>	 <p><u>Banking Fraud/Scam</u></p>	 <p><u>Password Management</u></p>
 <p><u>Two Factor Authentication</u></p>	 <p><u>Antivirus Software</u></p>	 <p><u>Cookies/Cookie Settings</u></p>
 <p><u>Email Scam/Phishing</u></p>	 <p><u>Computer Virus</u></p>	 <p><u>Phone Scam/Vishing</u></p>

Cyber Safety Emoji Quiz





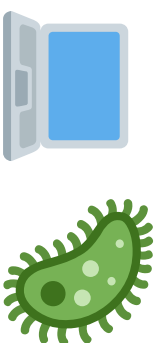














7. Cookie Conundrum

Objective: Understand what different types of cookies are, and the implications of accepting or declining them.

Activity:

Briefly explain what cookies are, their purposes (e.g., necessary, marketing, site preferences, third-party), and the importance of managing cookie preferences. Check [Page 21](#) for reference.

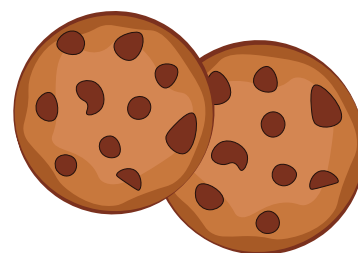
Introduce the spider diagram on the [Page 22](#) as a tool for making informed decisions about accepting cookies.

Ask participants to visit 1-3 websites of their choice, using the spider diagram to decide whether to accept, customise, or decline cookies for each one.

Make sure they note their cookie acceptance decision (e.g. accepted, customised, or declined), and the reasoning behind their choice (e.g., “I want personalised shopping recommendations” or “I don’t want to share my data with third parties, I just want to stay logged in”).

Then facilitate a short discussion on the following questions:

- How did the spider diagram help you decide?
- Did you find it easy or difficult to balance privacy with convenience?
- How did your choices change depending on the type of website?



What are Cookies?



Cookies are small files stored on your device by websites to remember your preferences and track activity.

There are a few different types.

Essential: Essential cookies are used to remember your activities on the website, they keep you logged in and remember what you have done on the website such as what you put in your shopping basket and recognise you by your log in details.

Non-Essential: Non-essential cookies 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.

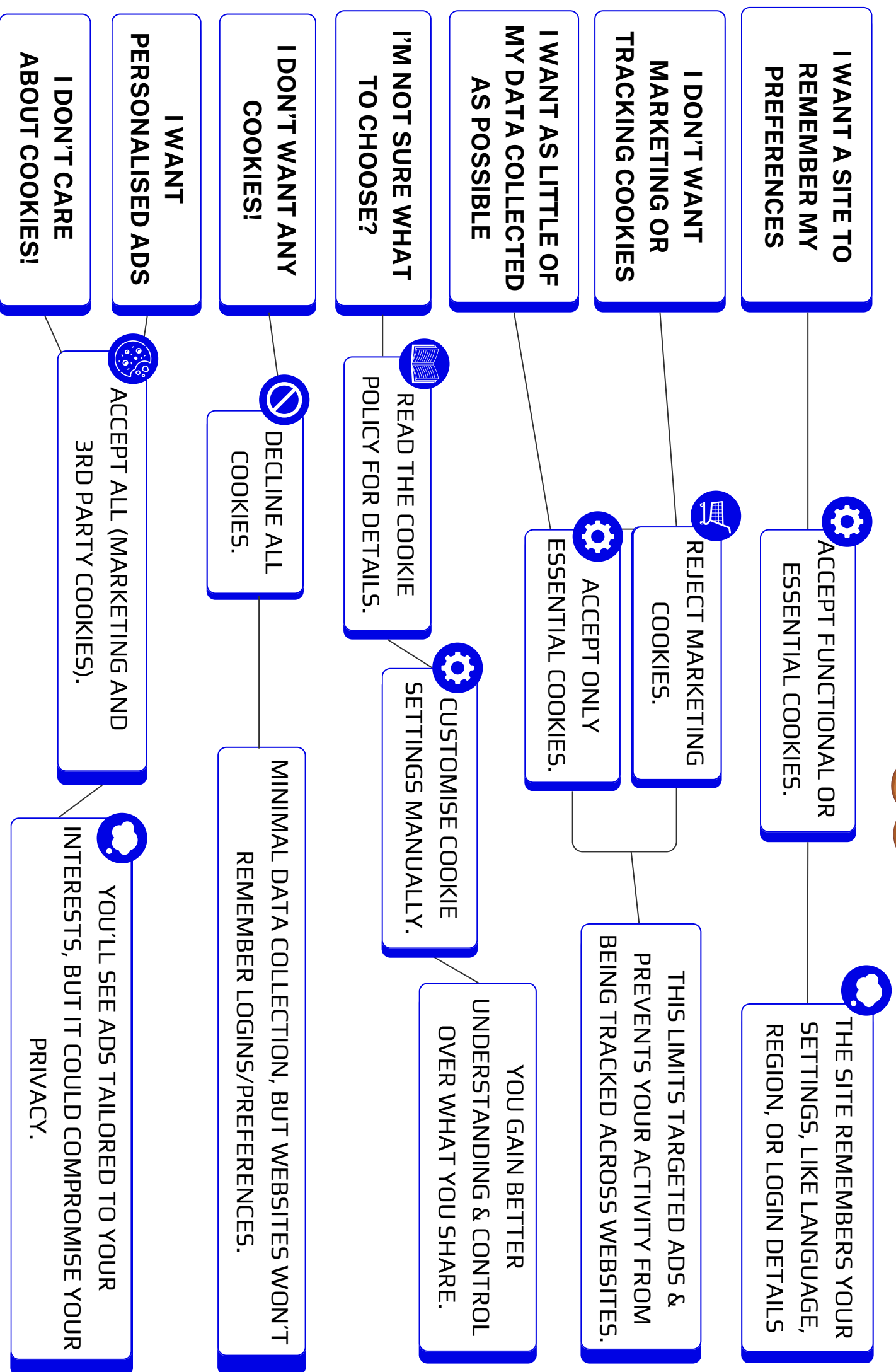
Advertising cookies are used to customise a user's ad experience on websites based on their browsing history and **social networking tracking cookies** allow users to share content on social media and help link the activity between a website and a third-party sharing platform.

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

The diagram shows a typical cookie consent banner with several annotations:

- Cookie Consent Description:** An arrow points to the text: "We use cookies on our website to give you the most relevant experience by remembering your preferences and repeat visits. By clicking 'Accept', you consent to the use of ALL the cookies. However you may visit Cookie Settings to provide a controlled consent."
- Choose between 'Necessary', 'Analytics', 'Advertisement', 'Preferences', and 'Others' cookies:** An arrow points to the list of checkboxes: ☒ Necessary ☐ Analytics ☐ Advertisement ☐ Preferences ☐ Others
- Access further cookie controls:** An arrow points to the [Cookie settings](#) link.
- Reject all button:** An arrow points to the "Reject all" button.
- Accept button:** An arrow points to the "Accept all" button.

SHOULD I ACCEPT COOKIES?



8. Cyber Safety Role-Play

Objective: Practice responding to real-world cybersecurity scenarios.

Activity:

Split participants into groups of three and assign them different roles: **a scammer, a victim, and a cybersecurity advisor.**

Provide a scenario from the story templates attached on [Page 24](#).

The "victim" can first react to the situation with the "scammer", and the "advisor" can then direct them on how to respond.

Provide a "Cybersafety Response Checklist" to each participant, outlining steps to take when dealing with a scam and after hacking is suspected, such as:

- Disconnecting their device from the internet.
- Changing their password and logging out of all connected devices.
- Reporting the incident to the Gardaí or their service provider, if relevant.
- Checking for unusual activity on other accounts.

Each group member should provide input into the steps that should be taken for each scenario. Then, discuss key takeaways and rate the advice given as a group.

Pages 25-27 are included for advice on **‘Steps to Take After a Notification of Unfamiliar Login Activity’**, **‘Steps to Take After a Phishing Attempt (Suspicious Email)’**, and **‘Steps to Take After a Phishing Attempt (Suspicious Phone Call)’**.



Cyber Safety Role-Play Scenarios

SCENARIO 1: A SUSPICIOUS HOLIDAY DEAL

Setup: The "victim" receives an email offering a discounted holiday package to a luxury resort. The email includes a link to a site to claim the offer that asks for personal details, including a full name, address, and credit card information, to secure the deal.

Roles:

Scammer: Sends the email and explains why the deal is "urgent."

Victim: Reacts to the email, unsure whether it's legitimate.

Advisor: Offers guidance on how to verify the email's authenticity and what steps to take next.

SCENARIO 2: A "BANK" PHONE CALL

Setup: The "victim" gets a phone call from someone claiming to be from their bank. The caller says there's been suspicious activity on their account and requests their account number, PIN, and security answers to "verify their identity."

Roles:

Scammer: Plays the caller, trying to sound convincing and urgent.

Victim: Responds to the request, unsure if it's legitimate.

Advisor: Advises on how to handle the call and the importance of verifying the caller's identity before sharing any information.

SCENARIO 3: AN UNFAMILIAR LOGIN NOTIFICATION

Setup: The "victim" receives a notification from their email provider stating their account was accessed from an unfamiliar location. They panic, unsure what to do next.

Roles:

Scammer: Pretends to be a hacker, explaining what they might do with the compromised account.

Victim: Reacts to the notification and considers their options.

Advisor: Provides advice on securing the account, checking for other breaches, and reporting the incident.

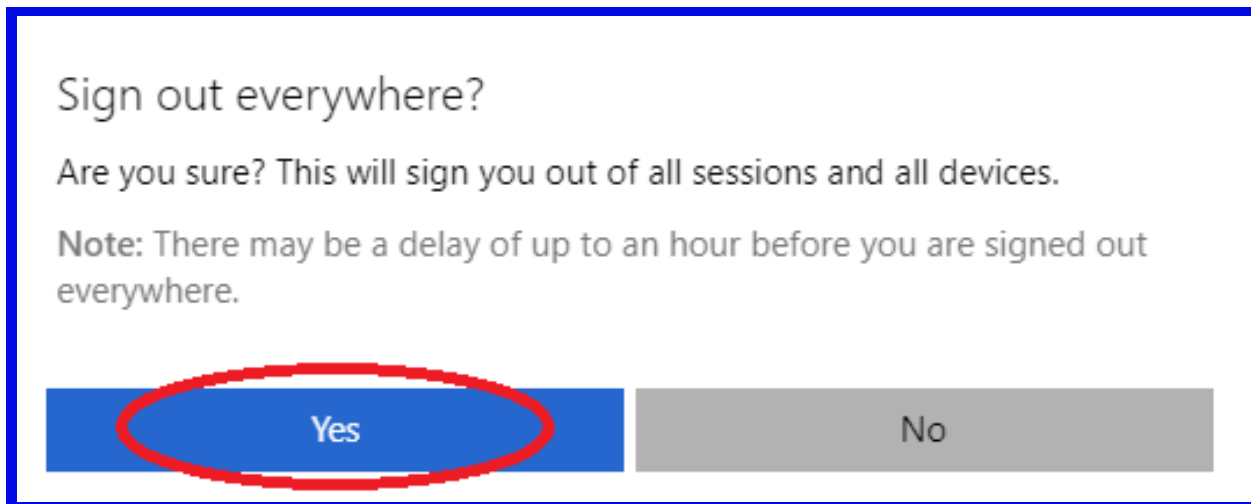
Steps to Take After a Notification of Unfamiliar Login Activity

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.

You can also enable two-factor authentication (2FA) if it’s available.



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.

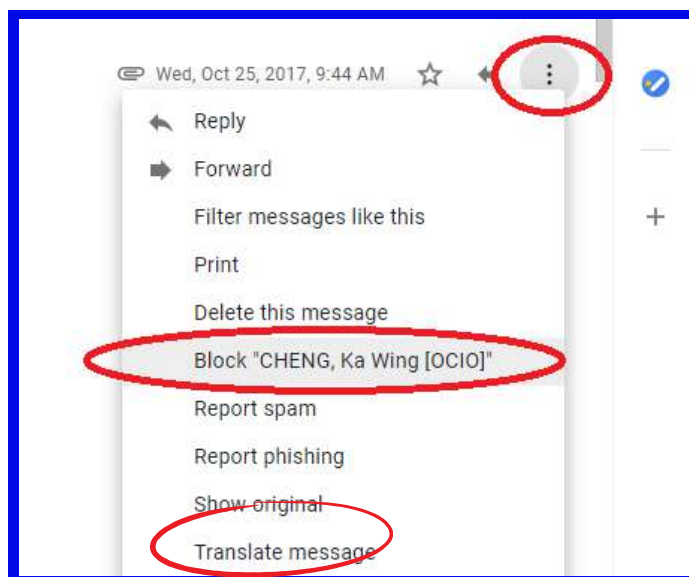
4. Also review your account’s security settings for any changes (e.g., a new email address added for recovery) and undo them if necessary.

5. Then, you can phone or 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.

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

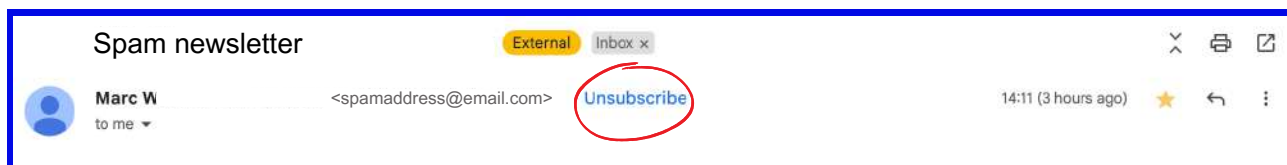
Steps to Take After a Phishing Attempt (Suspicious Email)

1. If you suspect the email is fraudulent, avoid interacting with any links or attachments in the message.
2. Check the sender's email address for inconsistencies or subtle misspellings. If it claims to be from a legitimate company, contact the company directly using their official contact information to confirm.
3. Use your email provider's "Block Sender" and "Report Phishing" options to help block similar messages in the future.



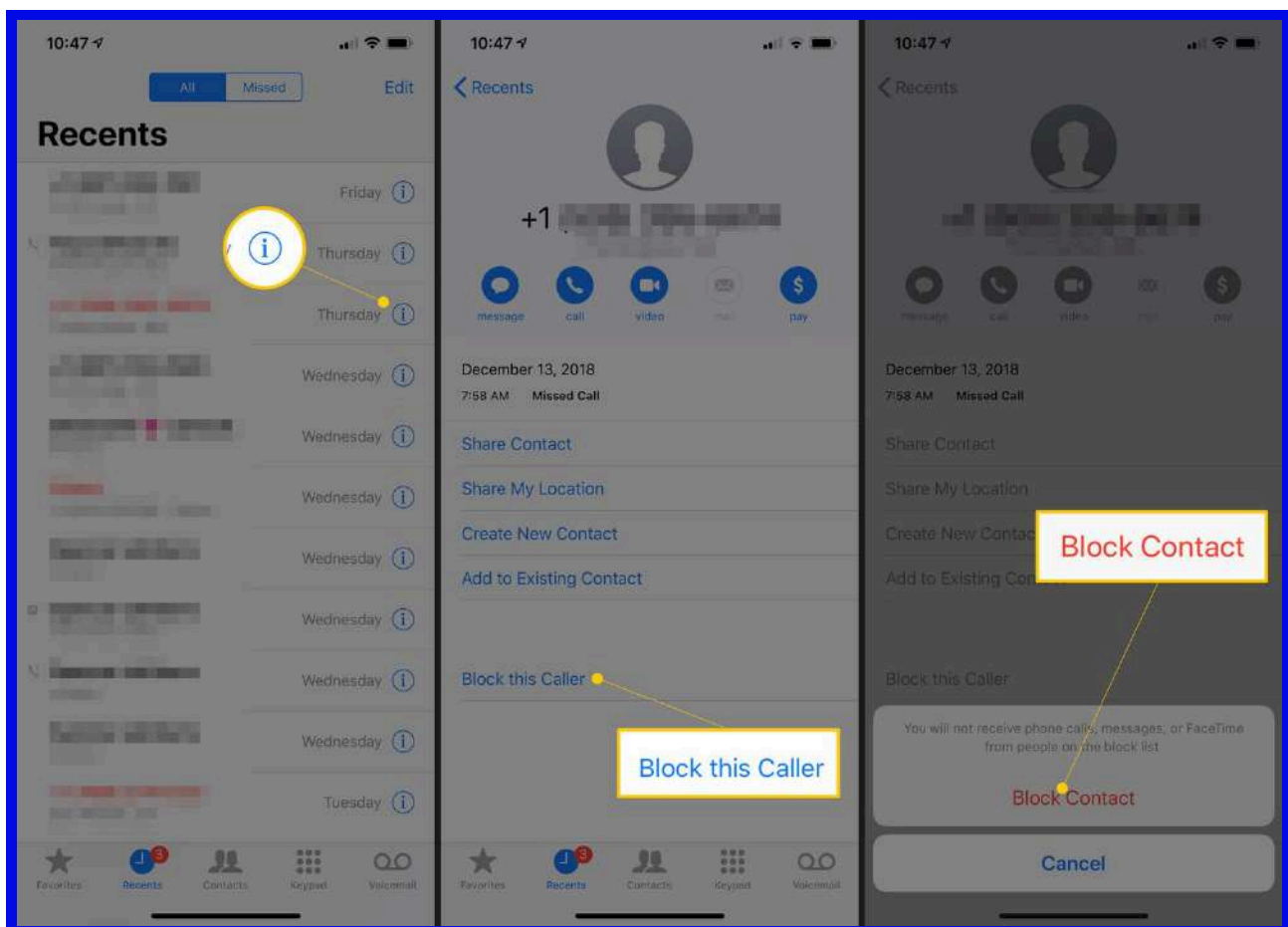
4. Once reported, "Delete" the email from your inbox to avoid interacting with it.
5. If you accidentally clicked a link or provided information, change your passwords immediately and check for unusual activity on your accounts.

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.



Steps to Take After a Vishing Attempt (Suspicious Phone Call)

1. 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.
2. Hang up without providing your name, account number, PIN, or any other sensitive details.
3. 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.
4. Then, use your phone's settings to **block** the caller to prevent future contact.



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

9. Two Truths and a Lie (Cyber Safety Edition)

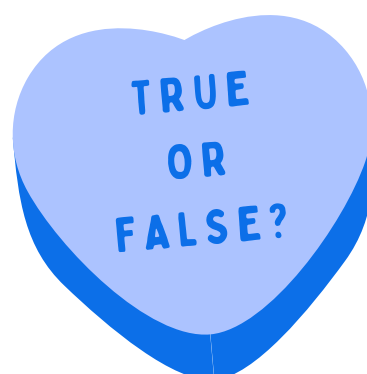
Objective: Reinforce knowledge of cybersecurity myths and facts.

Activity:

Share the quiz on [Pages 29-30](#), showing two true statements and one false statement about cyber safety (e.g., “Public Wi-Fi is always safe,” “Phishing emails often have spelling errors”, “Never write your passwords down”).

Participants guess which statement is false, crossing out the “lie”.

Then check the answer sheet and follow up with a discussion to clarify misconceptions.



Two Truths and a Lie

- 1**
 - Writing passwords in a secure notebook is good practice.
 - Using two-factor authentication improves account security.
 - You can trust any website that has "https" in its URL.
- 2**
 - Phishing emails often contain spelling and grammar errors.
 - It's safe to use the same password for multiple accounts if it's complex.
 - Keeping your software updated helps protect against vulnerabilities.
- 3**
 - Password managers can securely store your passwords.
 - Clicking on unknown links can lead to a security breach on your device.
 - Antivirus software alone guarantees your device is safe.
- 4**
 - Public Wi-Fi is always safe.
 - A strong password should include a mix of letters, numbers, and symbols.
 - Backing up your data regularly helps protect against ransomware attacks.
- 5**
 - Hackers cannot access webcams remotely.
 - Avoiding downloading suspicious attachments can help you avoid malware.
 - Firewalls can add an extra layer of security to your network.
- 6**
 - Clicking "unsubscribe" in spam emails is a safe way to get rid of them.
 - Social media profiles can be used by hackers to gather personal information.
 - Using a notebook stored in a secure place is a safe way to write down and remember passwords.
- 7**
 - Software updates often include security patches to keep your device safe.
 - It's safe to download apps from unknown sources if they look legitimate.
 - Encrypting sensitive files and data makes it harder for hackers to access.
- 8**
 - Cybercriminals sometimes pose as trusted companies to trick you.
 - Public charging stations can be a risk for data theft.
 - All smartphone apps are thoroughly vetted for security.
- 9**
 - Strong passwords should not include easily guessable information like your name or date of birth.
 - Hackers cannot attack systems that are turned off, but they can attack online accounts that aren't "frozen" or disabled.
 - A computer with antivirus software doesn't need any other protection.
- 10**
 - Clearing your cookies will permanently stop websites from collecting data about you.
 - Cookies can track the websites you visit to show targeted ads.
 - Some cookies are necessary for websites to function properly, like keeping you logged in.

Two Truths and a Lie

- 11**
 - It's good practice to regularly change your passwords, especially if you suspect a data breach.
 - Hovering over a link can help you check its true destination.
 - Public Wi-Fi networks are encrypted and safe by default.
- 12**
 - Social engineering attacks exploit human psychology and emotions to gain personal information.
 - Emails from official-looking addresses are always trustworthy.
 - Avoiding common passwords like "123456" improves account security.
- 13**
 - Data breaches can expose sensitive information stored on websites.
 - Avoiding unknown websites helps reduce exposure to malicious content.
 - It's safe to use a USB drive found in public places.
- 14**
 - Enabling auto-lock on your devices adds security.
 - Pop-ups are legitimate advertisements and can always be trusted.
 - A virtual private network (VPN) can improve your privacy online.
- 15**
 - Avoiding oversharing personal details online reduces the risk of identity theft and impersonation.
 - Cookies are useful for storing preferences, like language settings or items in a shopping cart.
 - Emails from unknown senders should be opened immediately if they are marked "Urgent".
- 16**
 - Hackers cannot exploit outdated software.
 - Social engineering is the psychological manipulation of tricking people into giving away sensitive information.
 - Installing security patches as they are released can reduce vulnerability to attacks.
- 17**
 - Using biometric authentication (e.g., fingerprints) as an additional to a password phrase can improve security.
 - Avoiding accepting unnecessary app permissions reduces privacy risks.
 - Clicking on shortened URLs is always safe.
- 18**
 - Social media quizzes can be used to gather personal information.
 - All emails with a company logo are safe to trust.
 - Disabling unused accounts can reduce security risks.
- 19**
 - All downloadable apps are monitored by App Stores and are secure to use.
 - Ransomware locks users out of their devices or data until a ransom is paid.
 - Regularly reviewing privacy settings on social media enhances your security.
- 20**
 - Any website with a padlock icon is secure to use.
 - Avoiding suspicious links and inspecting them by hovering or using check.cyberskills.ie can reduce phishing risks.
 - Strong encryption makes data harder to intercept during transmission.

Two Truths and a Lie Answers

- 1
 - Writing passwords in a secure notebook is good practice. (True)
 - Using two-factor authentication improves account security. (True)
 - You can trust any website that has "https" in its URL. (False)
- 2
 - Phishing emails often contain spelling and grammar errors. (True)
 - It's safe to use the same password for multiple accounts if it's complex. (False)
 - Keeping your software updated helps protect against vulnerabilities. (True)
- 3
 - Password managers can securely store your passwords. (True)
 - Clicking on unknown links can lead to a security breach on your device. (True)
 - Antivirus software alone guarantees your device is safe. (False)
- 4
 - Public Wi-Fi is always safe. (False)
 - A strong password should include a mix of letters, numbers, and symbols. (True)
 - Backing up your data regularly helps protect against ransomware attacks. (True)
- 5
 - Hackers cannot access webcams remotely. (False)
 - Avoiding downloading suspicious attachments can help you avoid malware. (True)
 - Firewalls can add an extra layer of security to your network. (True)
- 6
 - Clicking "unsubscribe" in spam emails is a safe way to get rid of them. (False)
 - Social media profiles can be used by hackers to gather personal information. (True)
 - Using a notebook stored in a secure place is a safe way to write down and remember passwords. (True)
- 7
 - Software updates often include security patches to keep your device safe. (True)
 - It's safe to download apps from unknown sources if they look legitimate. (False)
 - Encrypting sensitive files and data makes it harder for hackers to access. (True)
- 8
 - Cybercriminals sometimes pose as trusted companies to trick you. (True)
 - Public charging stations can be a risk for data theft. (True)
 - All smartphone apps are thoroughly vetted for security. (False)
- 9
 - Strong passwords should not include easily guessable information like your name or date of birth. (True)
 - Hackers cannot attack systems that are turned off, but they can attack online accounts that aren't "frozen" or disabled. (True)
 - A computer with antivirus software doesn't need any other protection. (False)
- 10
 - Clearing your cookies will permanently stop websites from collecting data about you. (False)
 - Cookies can track the websites you visit to show targeted ads. (True)
 - Some cookies are necessary for websites to function properly, like keeping you logged in. (True)

Two Truths and a Lie Answers

- 11**
- It's good practice to regularly change your passwords, especially if you suspect a data breach. (True)
 - Hovering over a link can help you check its true destination. (True)
 - Public Wi-Fi networks are encrypted and safe by default. (False)
- 12**
- Social engineering attacks exploit human psychology and emotions to gain personal information. (True)
 - Emails from official-looking addresses are always trustworthy. (False)
 - Avoiding common passwords like "123456" improves account security. (True)
- 13**
- Data breaches can expose sensitive information stored on websites. (True)
 - Avoiding unknown websites helps reduce exposure to malicious content. (True)
 - It's safe to use a USB drive found in public places. (False)
- 14**
- Enabling auto-lock on your devices adds security. (True)
 - Pop-ups are legitimate advertisements and can always be trusted. (False)
 - A virtual private network (VPN) can improve your privacy online. (True)
- 15**
- Avoiding oversharing personal details online reduces the risk of identity theft and impersonation. (True)
 - Cookies are useful for storing preferences, like language settings or items in a shopping cart. (True)
 - Emails from unknown senders should be opened immediately if they are marked "Urgent". (False)
- 16**
- Hackers cannot exploit outdated software. (False)
 - Social engineering is the psychological manipulation of tricking people into giving away sensitive information. (True)
 - Installing security patches as they are released can reduce vulnerability to attacks. (True)
- 17**
- Using biometric authentication (e.g., fingerprints) as an additional to a password phrase can improve security. (True)
 - Avoiding accepting unnecessary app permissions reduces privacy risks. (True)
 - Clicking on shortened URLs is always safe. (False)
- 18**
- Social media quizzes can be used to gather personal information. (True)
 - All emails with a company logo are safe to trust. (False)
 - Disabling unused accounts can reduce security risks. (True)
- 19**
- All downloadable apps are monitored by App Stores and are secure to use. (False)
 - Ransomware locks users out of their devices or data until a ransom is paid. (True)
 - Regularly reviewing privacy settings on social media enhances your security. (True)
- 20**
- Any website with a padlock icon is secure to use. (False)
 - Avoiding suspicious links and inspecting them by hovering or using check.cyberskills.ie can reduce phishing risks. (True)
 - Strong encryption makes data harder to intercept during transmission. (True)

10. Cyber Safety Wordsearch

Objective: Reinforce knowledge of key cybersecurity terms.

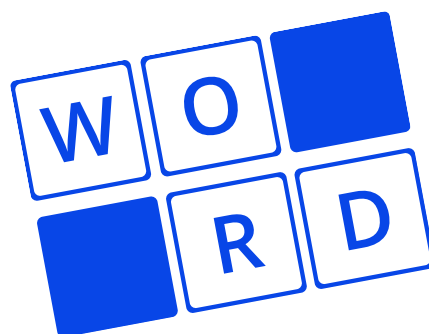
Activity:

Hidden within the grid on [Page 34](#) are key terms related to cyber safety.

Participants can search for words like "phishing," "malware," and "spam" to sharpen their cyber safety vocabulary.

The provided answer key on [Page 35](#) can then be used to check their work and ensure they have found all the hidden terms.

Words may be hidden horizontally, vertically, diagonally, or backward.





CYBER
SAFETY

WORDSEARCH

H	P	H	P	D	R	O	W	S	S	A	P
M	G	T	G	Y	G	K	Q	G	O	O	R
A	H	U	W	U	H	J	H	U	R	S	I
P	G	V	O	O	O	G	G	O	S	O	V
S	U	R	P	H	F	B	A	R	E	M	A
E	E	B	G	N	T	A	C	O	I	A	C
D	T	T	L	J	H	C	C	H	K	L	Y
A	O	R	T	W	M	K	O	T	O	W	H
T	U	T	M	I	O	U	U	H	O	A	T
A	T	A	G	F	N	P	N	S	C	R	D
B	C	U	G	I	T	G	T	U	O	E	P
S	K	C	O	P	H	I	S	H	I	N	G

DATA
BACKUP
TWOFACTOR
ACCOUNT
SETTINGS
WIFI
SPAM

PHISHING
MALWARE
PASSWORD
PRIVACY
SCAM
COOKIES
VPN



CYBER
SAFETY

WORDSEARCH ANSWERS

H	P	H	P	D	R	O	W	S	S	A	P
M	G	T	G	Y	G	K	Q	G	O	O	R
A	H	U	W	U	H	J	H	U	R	S	I
P	G	V	O	O	O	G	G	O	S	O	V
S	U	R	P	H	F	B	A	R	E	M	A
E	E	B	G	N	T	A	C	O	I	A	C
D	T	T	L	J	H	C	C	H	K	L	Y
A	O	R	T	W	M	K	O	T	O	W	H
T	U	T	M	I	O	U	U	H	O	A	T
A	T	A	G	F	N	P	N	S	C	R	D
B	C	U	G	I	T	G	T	U	O	E	P
S	K	C	O	P	H	I	S	H	I	N	G

DATA
BACKUP
TWOFACTOR
ACCOUNT
SETTINGS
WIFI
SPAM

PHISHING
MALWARE
PASSWORD
PRIVACY
SCAM
COOKIES
VPN

Notes



Lined area for taking notes, consisting of multiple horizontal gray lines.

Notes



Lined area for taking notes, consisting of multiple horizontal gray lines.



CYBER SAFETY