



**Change the advice  
category by  
reviewing the  
information below:**

**Phishing attempts often  
mimic trusted sources**

**Cyber con artists use  
urgency, fear, or curiosity to  
obtain your personal  
information**

©



**Change the advice  
category by  
reviewing the  
information below:**

**Google Search is an effective  
method for verifying  
information across multiple  
sources**

**Pay attention to customer  
reviews and news sources**

©



**Change the advice category by reviewing the information below:**

Two-factor authentication (2FA) makes it more difficult for hackers to access your account

You can receive 2FA codes through SMS, email or authenticator apps

©



**Change the advice category by reviewing the information below:**

Passphrases are a combination of words used to secure access to your accounts

An example of a passphrase would be “I make tea at 9:30am”

©



**Change the advice category by reviewing the information below:**

The PULSE ID is a unique number allocated to an incident in the Garda system

Expect a Garda Victims Service Office letter with the Garda's name and PULSE ID after you report a cybercrime

©



**Change the advice category by reviewing the information below:**

“Compromised”, “breached”, “hacked” and “unauthorized access” all refer to similar situations

Contact the Crime Victims Helpline at 116006 for support after a cybercrime

©



**Change the advice  
category by  
reviewing the  
information below:**

Cookies remember your  
browsing preferences,  
location and login  
information

Reject unnecessary  
cookies to keep your  
personal information  
safe

©



**Change the advice  
category by  
reviewing the  
information below:**

Use a disposable virtual card  
from a trusted bank to  
protect your main card when  
shopping online

Regularly check your  
transactions for any  
unauthorized activity

©

**1**

## **Responding to Cyber Attacks**



**Stay calm and assess  
the situation**

©

**1**

**2**

## **Responding to Cyber Attacks**



**Immediately change your  
compromised passwords and  
log out of all devices**

©

**2**

**3**

## Responding to Cyber Attacks



Check if your other accounts,  
including social media and  
email, have been compromised  
([haveibeenpwned.com](https://haveibeenpwned.com))

©

**3**

**4**

## Responding to Cyber Attacks



Enable two-factor  
authentication

©

**4**

**5**

## **Responding to Cyber Attacks**



**Collect evidence (e.g.,  
take screenshots)**

**5**

©

**6**

## **Responding to Cyber Attacks**



**Contact your service provider  
(e.g., bank) by calling,  
physically going in or going  
online**

**6**

©

**7**

## **Responding to Cyber Attacks**



Go to your local Garda  
station and request a  
PULSE ID

**7**

©

**8**

## **Responding to Cyber Attacks**



Provide the PULSE ID to  
your service provider so that  
they can rectify the situation

**8**

©





## Responding to Cyber Attacks



Ignore the hack and  
continue using your  
personal accounts

©



## Responding to Cyber Attacks



Anti-virus software is  
enough to keep you  
protected

©



**1**

## Password Management



Use “remember my password” on your personal devices

©

**1**

**2**

## Password Management



Never use “remember my password” on shared or public devices

©

**2**

**3**

## Password Management



Use a 3-word sentence  
as your password

**3**

©

**4**

## Password Management



Write down your  
passwords and keep them  
in a secure location

**4**

©

5

## Password Management



Avoid using the same passwords for multiple accounts

5

©

6

## Password Management



If your password is compromised, change it immediately

6

©

**7**

## Password Management



Consider using a digital password manager

**7**

©

**8**

## Password Management



Enable two-factor authentication

**8**

©

—

## Password Management



Use your date of birth and the names of family members as your passwords

© —

—

## Password Management



Always change passwords on a regular basis

© —

1

## Staying Private



Only fill in mandatory  
fields in forms

©

1

2

## Staying Private



Decline unnecessary  
cookies to avoid tracking  
online

©

2

3

## Staying Private



Select “manage” or  
“options” on cookie pop-ups  
and select “necessary only”

3

©

4

## Staying Private



Reject unnecessary requests  
from websites/apps to get  
your location and contacts

4

©



5

## Staying Private



Regularly clear cookies in  
your browsing settings

5

©

6

## Staying Private



Limit the amount of personal  
information shared on social  
media

6

©

**7**

## **Staying Private**



Regularly review and  
update privacy settings on  
your devices and accounts

©

**7**

**8**

## **Staying Private**



Avoid entering usernames  
and passwords on public  
Wi-Fi

©

**8**



## **Staying Private**



The padlock icon is proof  
that a website is  
definitely secure

©



## **Staying Private**



Declining cookies denies  
you access to the  
website

©



1

## Handling Scams



Block suspicious calls  
and texts

1

©

2

## Handling Scams



Be wary of sites found  
through unsolicited emails  
or pop-up ads

2

©

**3**

## Handling Scams



Be cautious of deals that seem too good to be true

©

**3**

**4**

## Handling Scams



Use Google Search to check if it's a known scam

©

**4**

**5**

## Handling Scams



Agree on a “safe word” with family members to verify suspicious communications

©

**5**

**6**

## Handling Scams



Collect evidence (e.g., take screenshots) if you are a victim of a scam

©

**6**

7

## Handling Scams



Check links before you  
click ([check.cyberskills.ie](https://check.cyberskills.ie))

7

©

8

## Handling Scams



Go directly to the source (e.g.,  
bank) by calling, physically  
going in or going online

8

©

—

## Handling Scams



Open all email attachments  
and text message links from  
unknown senders

©

—

—

## Handling Scams



Scammers only target  
people for large sums of  
money

©

—