An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications

NATIONAL CYBER SECURITY CENTRE

FSSU Training Day 14/06/2023

Mission

The mission of the National Cyber Security Centre is to lead in enhancing the security of essential network and information systems in the State against cyber threats, facilitating a free, open, secure, and stable digital ecosystem for the people of Ireland.

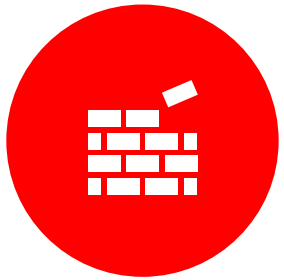
What we do

INCIDENT DETECTION & RESPONSE

RISK ANALYSIS & SITUATIONAL AWARENESS

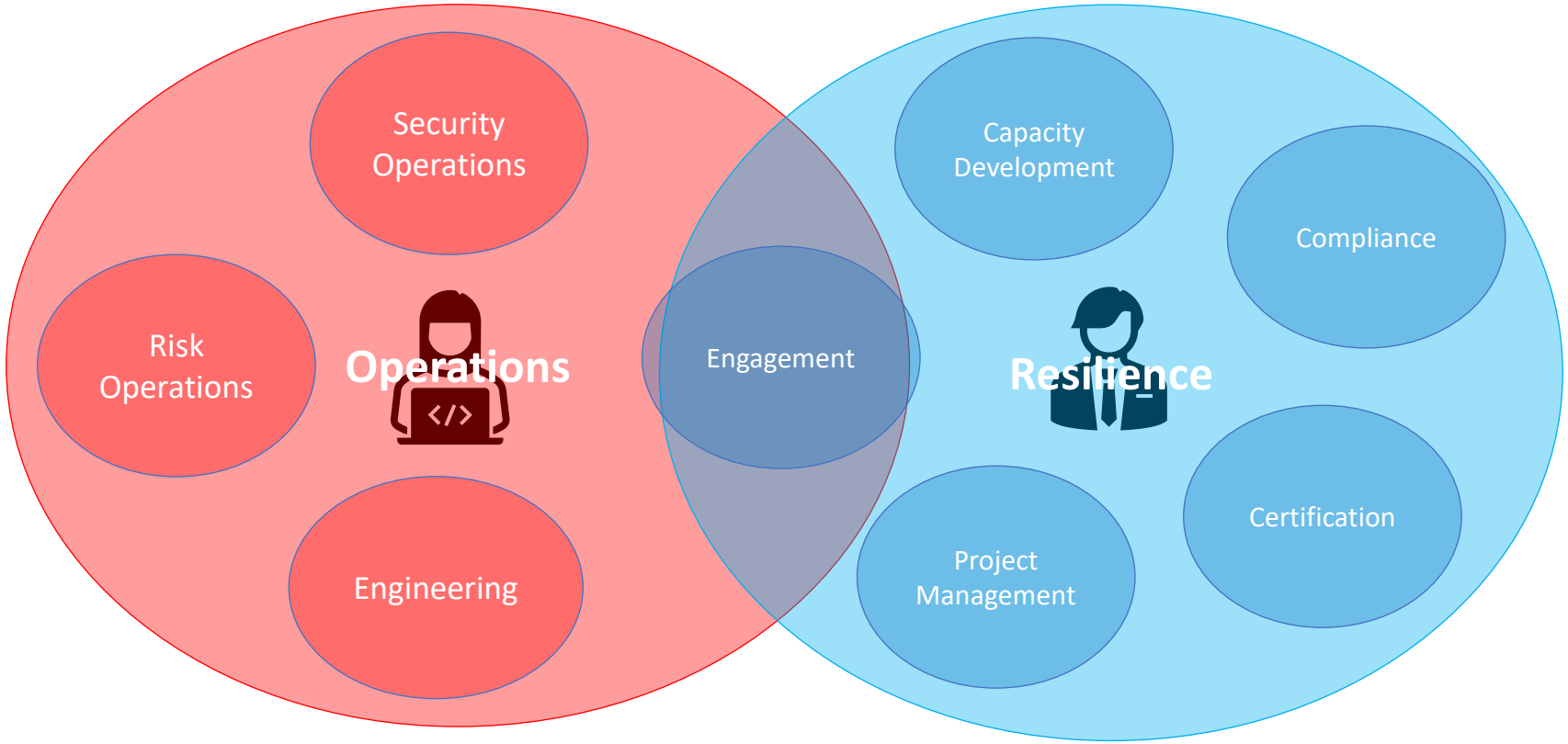
ENGAGEMENT

CYBER RESILIENCE



CAPACITY DEVELOPMENT

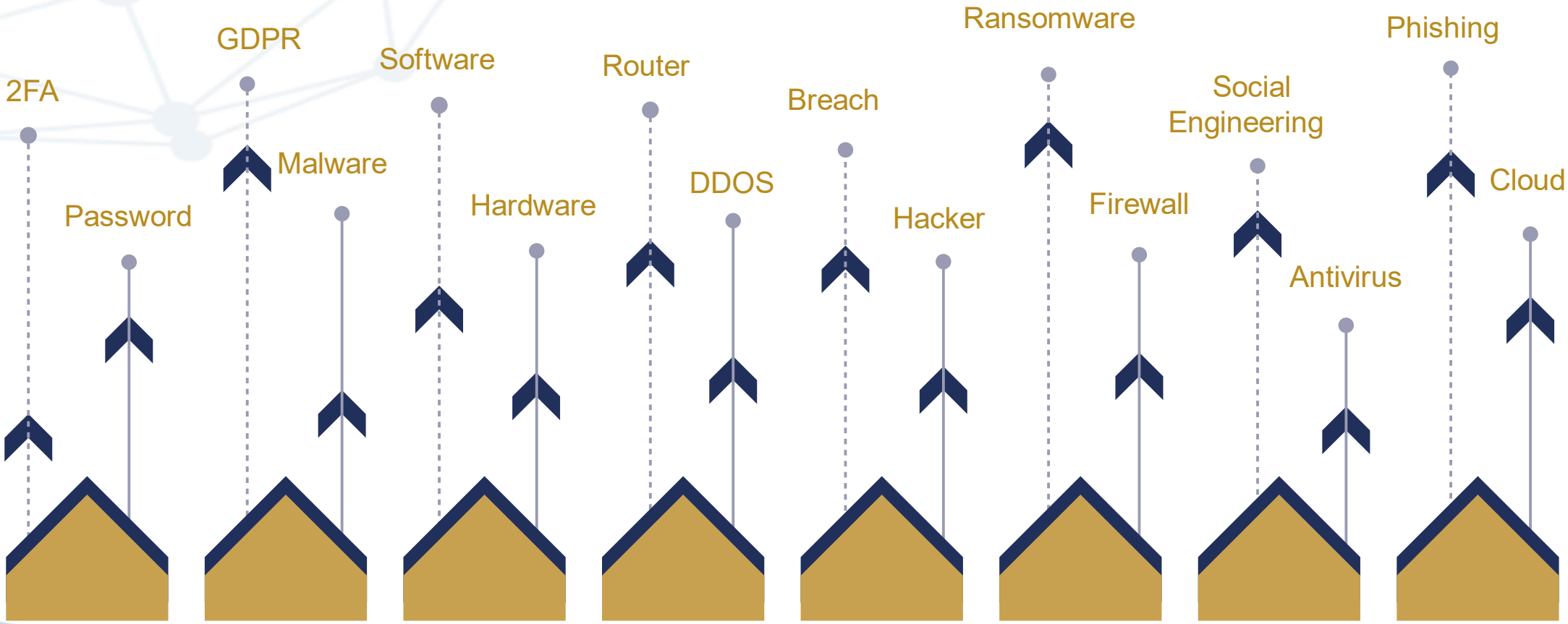
NCSC Teams


Security Operations
Risk Operations
Operations
Engineering
Engagement
Capacity Development
Compliance
Resilience
Certification
Project Management

An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications

What is cybersecurity, who should care about it, and why is it important?

What is cyber security?



Cyber security: a definition

"Cyber security is how individuals and organisations reduce the risk of cyber attack.

Cyber security's core function is to protect the **devices** we all use (smartphones, laptops, tablets and computers) and the **services** we access - both online and at work - from theft or damage.

It's also about preventing unauthorised access to the vast amounts of **personal information** we store on these devices, and online."

Cyber security: myths and reality

1. Cyber security is too complex for me to understand.

2. Cyber attacks are sophisticated. We can't stop them.

3. Cyber attacks are highly targeted. Our organisation is unlikely to be interesting and/or valuable enough to attackers.

Cyber security as a board level responsibility

1. Nearly all organisations depend on digital technology to **function.**
2. The potential **cost** of remedying a cyber incident can be significant.
3. The risk of **reputational damage.**

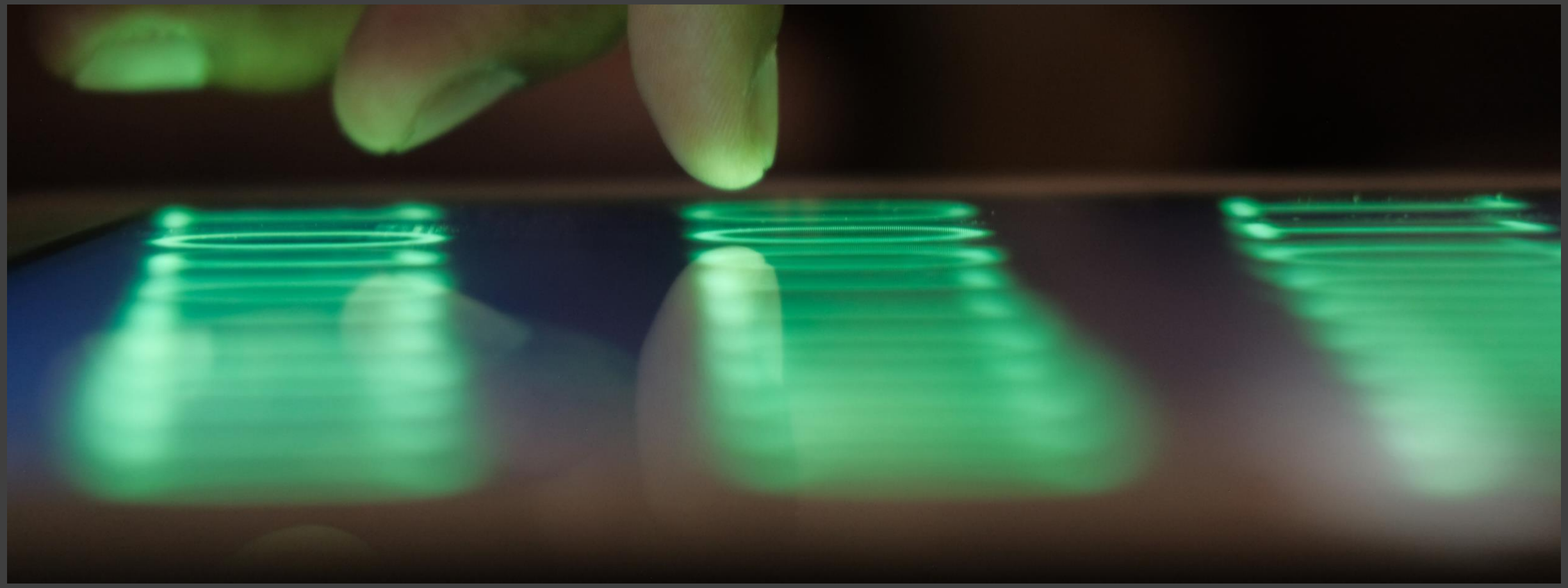
Cyber security is therefore **essential** and needs to be understood as an **enabler.**

An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications

Who is responsible for cyber attacks?

Nation State Actors

- Geopolitical events drive cyber operations.
- Destructive attacks & OT specific malware.
- Information Operations
- Espionage is still the main activity.



Criminal Actors

- Increasing specialisation, sophistication & collaboration.
- Weaponisation of discovered vulnerabilities.
- Crime is migrating to the cloud

Ransomware

- Continues to be the highest threat.
- Industrial/Education Sector
- Disruption efforts.

NCSC Advice & Guidance

An Roinn Comhshaoil, Aeráide agus Cumarsáide
Department of the Environment, Climate and Communications

MULTIFACTOR AUTHENTICATION –

STRONG, LONG, COMPLEX PASSWORDS

DON'T SHARE ACCOUNTS

ENCRYPTED MESSAGING APPS

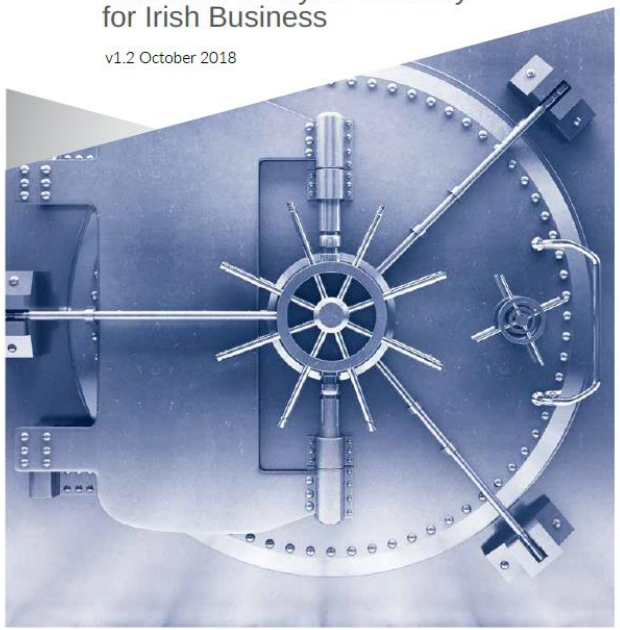
BE AWARE OF PHISHING MAILS

KEEP DEVICES UPDATED

DON'T USE PERSONAL ACCOUNTS FOR OFFICIAL BUSINESS

NCSC
NATIONAL CYBER SECURITY CENTRE
Cyber Vitals Checklist V1.0

Rialtas na hÉireann
Government of Ireland



NCSC Quick Guides

Guidance for schools

NCSC
NATIONAL CYBER SECURITY CENTRE

Quick Guide: Cyber Security for Schools

Cyber Security for Schools

Rialtas na hÉireann
Government of Ireland

NCSC NATIONAL CYBER SECURITY CENTRE

An Roinn Comhshaoil, Aeráide agus Cumarsáide
Department of the Environment, Climate and Communications

Guidance for schools

Who Might Want to Target Schools?

Online Criminals

Online criminals may attempt to steal and sell important sensitive personal data, or they could carry out a ransomware attack, encrypting files and preventing access to systems so they can hold a school to ransom.

Hackers

There may be individuals, for reasons beside financial motivation who wish to access a school's IT systems so that they can cause disruption or reputational damage to schools.

Human Errors

Staff and pupils who are using the devices and online systems may make mistakes or fall victim to phishing e-mail campaigns which allow sensitive information or credentials to fall into the wrong hands and possibly be exploited.

Malicious Insiders

Disgruntled staff or unhappy students/pupils may use their access to a school's IT systems to carry out malicious activity to cause disruption or reputational damage.

Guidance for schools

Impact of Cyber Attacks

Encryption

The attacker will push out their encryption to as many devices as possible. The attacker will also focus on encrypting backups they can access in order to prevent recovery. The attacker will demand a ransom payment in return for a decryption key.

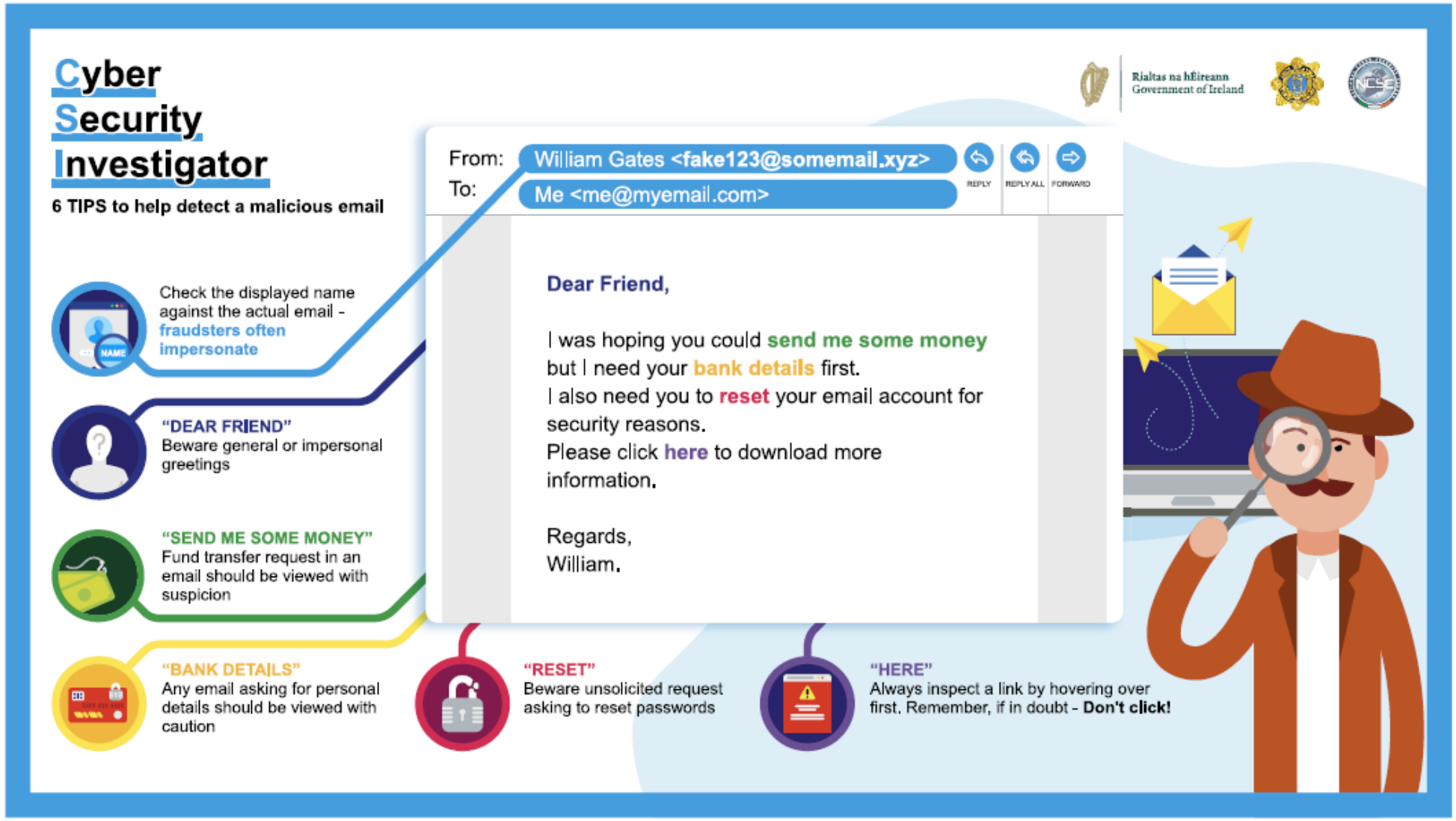
Data Theft

Before encrypting the system, the attacker will likely have stolen sensitive and personal data, in order to conduct 'double extortion' whereby they will demand a further ransom payment to prevent the data being leaked or sold.

Defacement

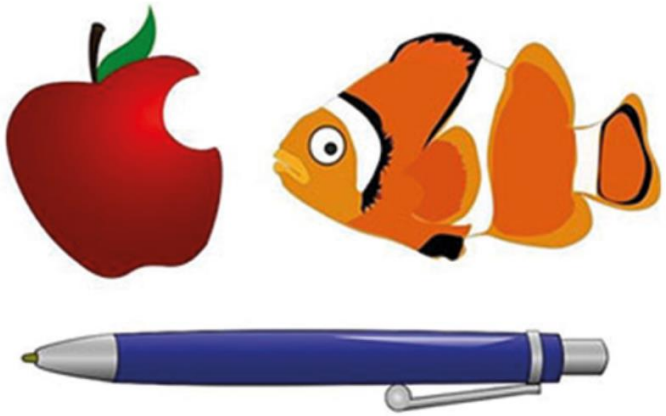
Hacking of school websites or social media accounts to deface them or publish damaging disinformation to cause reputational damage.

Phishing


Cyber Security Investigator
6 TIPS to help detect a malicious email
Rialtas na hÉireann
Government of Ireland
From: William Gates <fake123@somemail.xyz>
To: Me <me@myemail.com>
REPLY
REPLY ALL
FORWARD
Dear Friend,
I was hoping you could send me some money but I need your bank details first.
I also need you to reset your email account for security reasons.
Please click here to download more information.
Regards,
William.
Check the displayed name against the actual email - fraudsters often impersonate
"DEAR FRIEND"
Beware general or impersonal greetings
"SEND ME SOME MONEY"
Fund transfer request in an email should be viewed with suspicion
"BANK DETAILS"
Any email asking for personal details should be viewed with caution
"RESET"
Beware unsolicited request asking to reset passwords
"HERE"
Always inspect a link by hovering over first. Remember, if in doubt - Don't click!

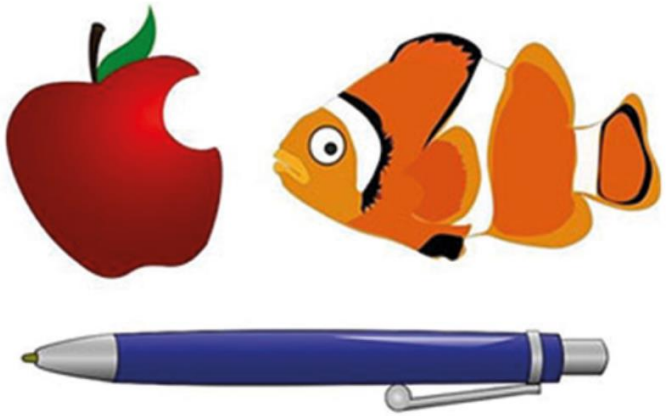
Defending against phishing

Three random words



Defending against phishing

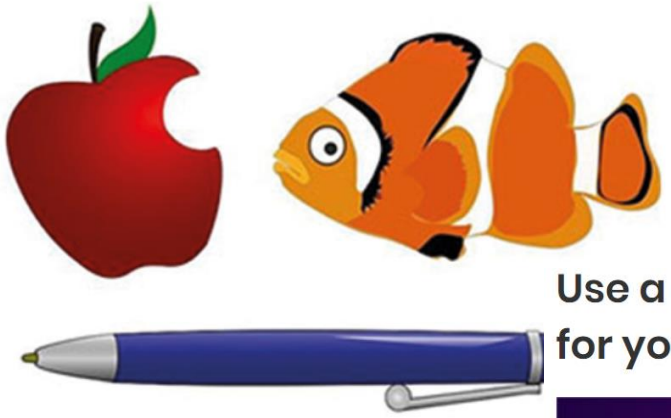
Three random words



Turn on 2-step verification (2SV)

Defending against phishing

Three random words



Turn on 2-step verification (2SV)

Use a strong and separate password for your email

Summary

Your checklist

Review

Review the privacy settings for your social media, professional networking sites and app accounts.

Know

Know who to report any unusual activity to. If you're not sure, ask your line manager or IT team.

Check

Check your device is set to receive updates automatically.

Set

Set a strong password and switch on two-factor authentication, if available, for your most important accounts.

Remove

Remove any apps that have not been downloaded from official stores.

Check

Check that the password for your work account is unique.

Flag it

If it's not possible to follow security advice, process or policy - flag it to your IT team.

An Roinn Comhshaoil, Aeráide agus Cumarsáide
Department of the Environment, Climate and Communications

NCSC National Cyber Security Centre

For more information and guidance

www.ncsc.gov.ie/guidance