Cyber Threat Landscape
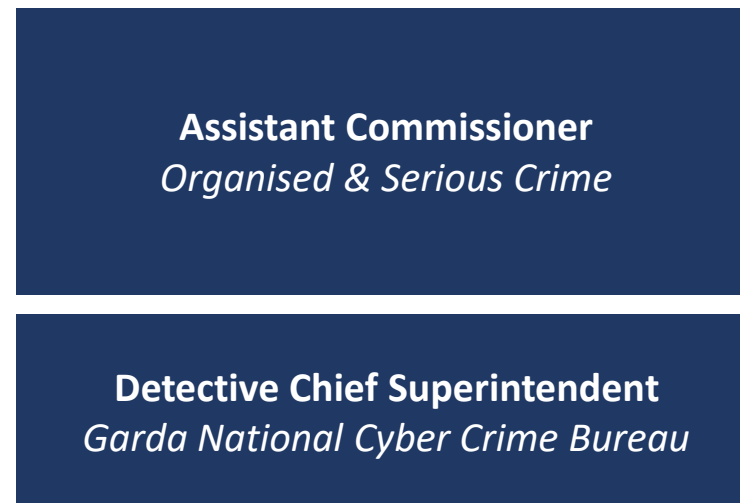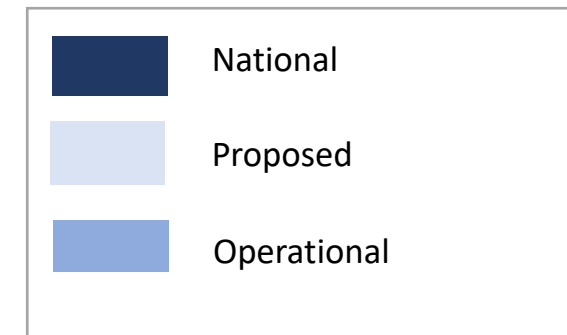## ISME Roadshow 2022

Garda National Cyber Crime Bureau

Garda National Cyber Crime Bureau
## Structure

Assistant Commissioner
Organised & Serious Crime

Detective Chief Superintendent
Garda National Cyber Crime Bureau

	National
	Proposed
	Operational

| **Detective Superintendent** *Technical Operations, Training and Cyber Safety*		**Detective Superintendent** *Investigations and Liaison*	
Detective Inspector *Cyber Technical Operations*	**Detective Inspector** *Cyber Supports & Liaison*	**Detective Inspector** *Cyber Investigations, Innovation & Training*	**Higher Executive Officer** *Administration, Governance & CTU*
Computer Forensics: Triage & Assessment	Satellite Cyber Hubs	Cyber Investigations Unit	GNCCB Governance
Computer Forensics: Enhanced Forensic Analysis	Cyber Safety & Security	Training & Innovation	PEMS
Top Tier Mobile Phone Forensics	Cyber Intelligence	Digital Evidence First Responders	Coordination & Tasking Unit
	NCSC Liaison	Planning & Future Proofing	GNCCB ICT Operations Support
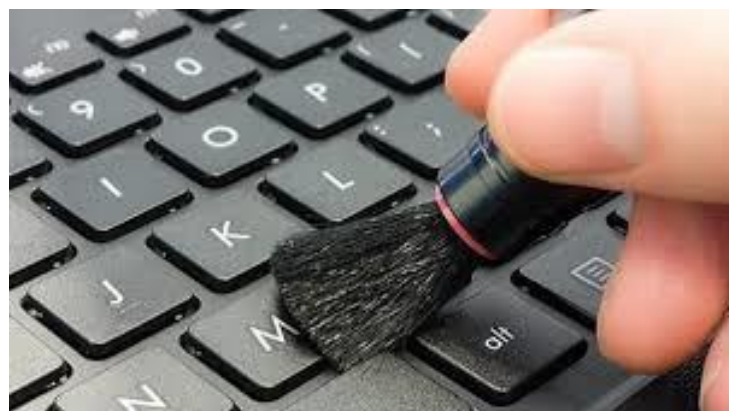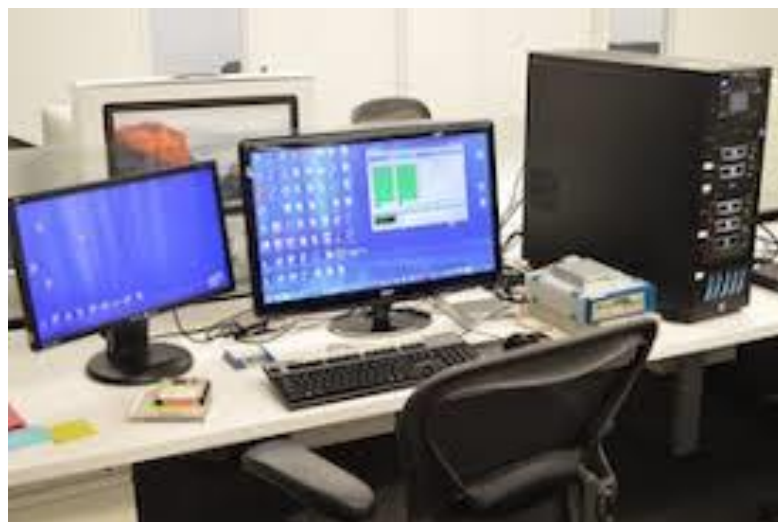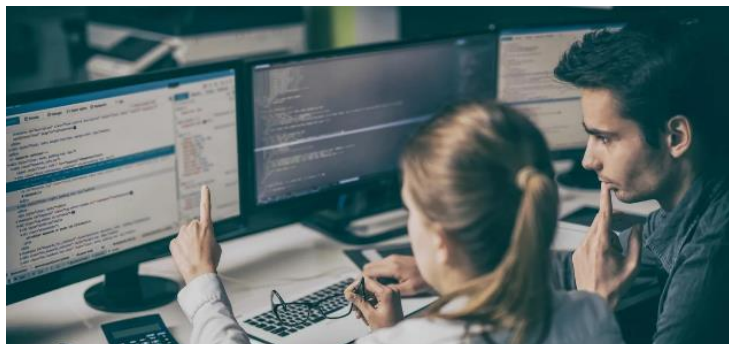
MSc Forensic Computing &
Cybercrime Investigation
IACIS
Software trained
CISCO trained

Wexford

Galway

Harcourt Square
Dublin

Cork

Mullingar

'There are only two types of companies: those that have been hacked and those that will be.'

Robert S Mueller, Former FBI Director.

Garda National Cyber Crime Bureau
Cyber Crime Trends & Statistics

Ransomware

- Europe #2 targeted region
- 150% ↑ on 2021
- SMEs are the new target

Phishing

- 300% ↑ on 2020
- 83% of companies experienced Phishing in 2021
- Method of entry in 41% of cyber attacks

To Pay or Not to Pay?

- 29% got only half the data back
- 8% got all their data back
- 80% were victim to repeated demands

Garda National Cyber Crime Bureau

Ransomware

7 tips on how to #BreakTheChain

Rialtas na hÉireann
Government of Ireland

Reduce entry points
Minimise the parts of your network that are exposed to the internet

Multi-Factor Authentication
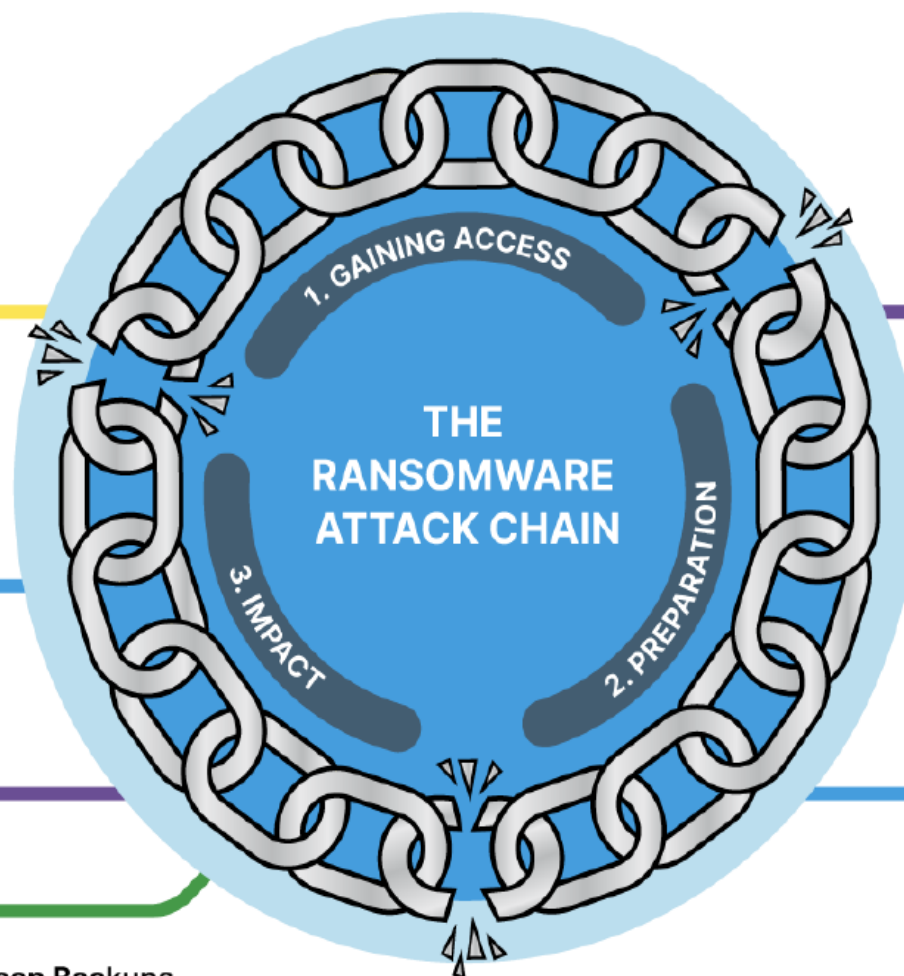Make sure all user accounts have MFA enabled, where possible use an authenticator app

Log & Monitor
Effective logging and monitoring helps early detection of attackers on your network

Keep Backups
Try to follow the 3-2-1 rule: 3 copies on 2 separate systems with 1 offline

THE RANSOMWARE ATTACK CHAIN

1. GAINING ACCESS
2. PREPARATION
3. IMPACT

Update Security
Ensure hardware and software, particularly edge devices have up to date security patches

Have A Plan
Be prepared, test how you would deal with a serious data breach

User Awareness
Educate end users about the threat and how they can prevent it.
Think before you click!

www.ncsc.gov.ie/resources

Phishing is **a type of social engineering attack in which cyber criminals trick victims into handing over sensitive information or installing malware**. They do this via malicious emails that appear to be from trusted senders, but sometimes use other means

Garda National Cyber Crime Bureau

Dear 365 online Client,

UPDATE TO PERSONAL 365 CREDIT CARD TERMS AND CONDITIONS

Your 365 Online account has been temporarily suspended,due 3 incorrect login a

> https://learn2work.eu/sv/
> Click to follow link

The link looks like it is to a genuine Bank of Ireland website but if you hover over the link with your mouse, you can see that clicking it would send you to a different, fraudulent, website.

Please click on the link to reactivate : https://www.365online.com/authentication

Some of these changes reflect new legislation around persoal credit card contracts. Other changes are to make things easier to understand.

If you have a personal 365 Credit Card or are in the process of getting a new personal 365 Credit Card, these changes will affect you and it is important that you read the changes.

If you do not completed this action as soon as possible, your account will be locked permanently.

Yours sincerely,
Central Bank of Ireland .
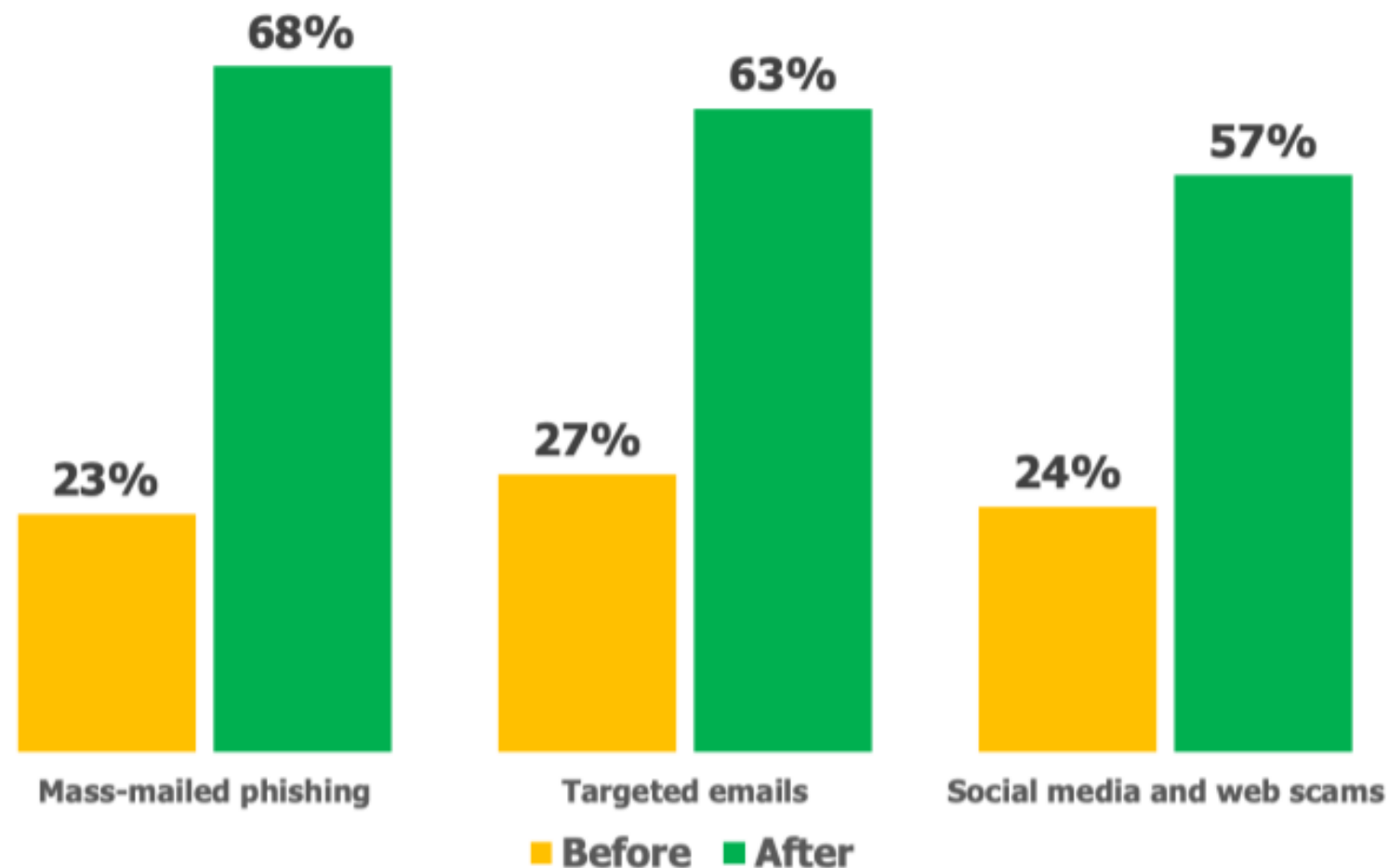
Garda National Cyber Crime Bureau
Why Report?

ALLOWS FOR CRIMINAL INVESTIGATION & VICTIM SUPPORT

EXPERIENCED EXAMINERS & INVESTIGATORS

IDENTIFY CURRENT AND EMERGING TRENDS & METHODS OF ATTACK

INFORMS ADVICE TO THE PUBLIC & CORPORATE SECTORS

REINFORCE CUSTOMER CONFIDENCE IN YOUR RESPONSES

SUPPORT VICTIMS OF CRIME & RECOVERY

STATUTORY OBLIGATIONS – DATA PROTECTION & S19 CRIMINAL JUSTICE ACT 2011

In a recent study, 80% of organisations said that security awareness training had reduced their staffs' susceptibility to phishing attacks. That reduction doesn't happen overnight, but it can happen fast — with regular training being shown to reduce risk from 60% to 10% within the first 12 months.

Perceived Ability of Employees at Recognizing Various Threats Before and After Security Awareness Training
Percentage Indicating "Capable" or "Very Capable"

	Before	After
Mass-mailed phishing	23%	68%
Targeted emails	27%	63%
Social media and web scams	24%	57%

Source: Osterman Research, Inc.

- Always have safe and up to date backup(s) which are kept separate from the network or computer system

- Only use official sources to update your antivirus software and computer system patches

- Don't open attachments or links unless you know and trust the source

- Don't mix data from work and personal activity online

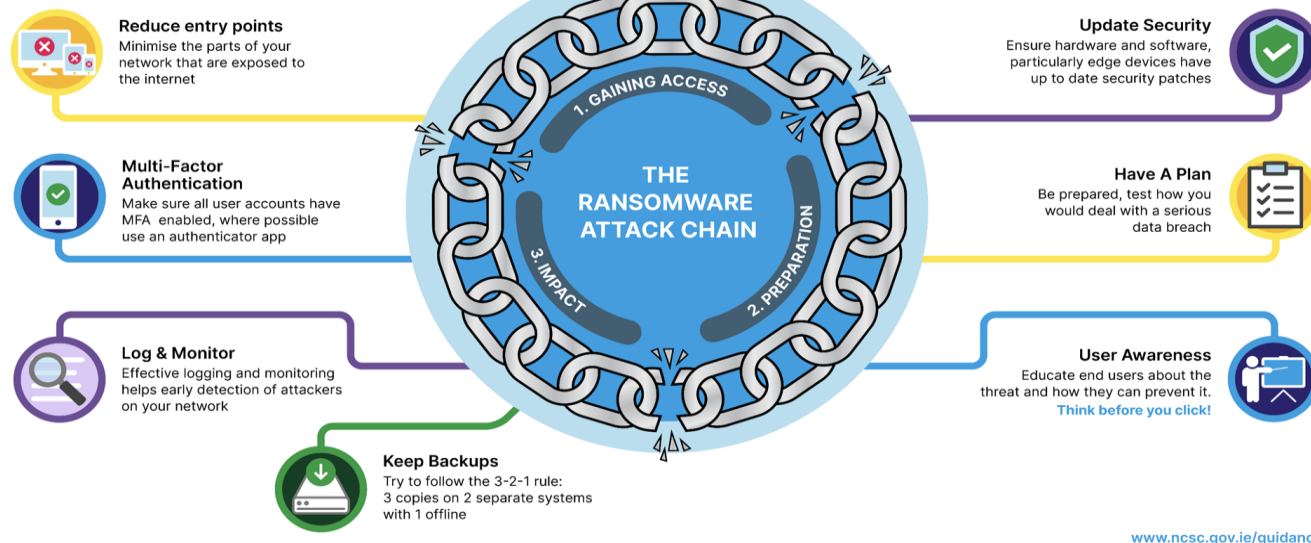- Be careful when using remote access methods to your company network
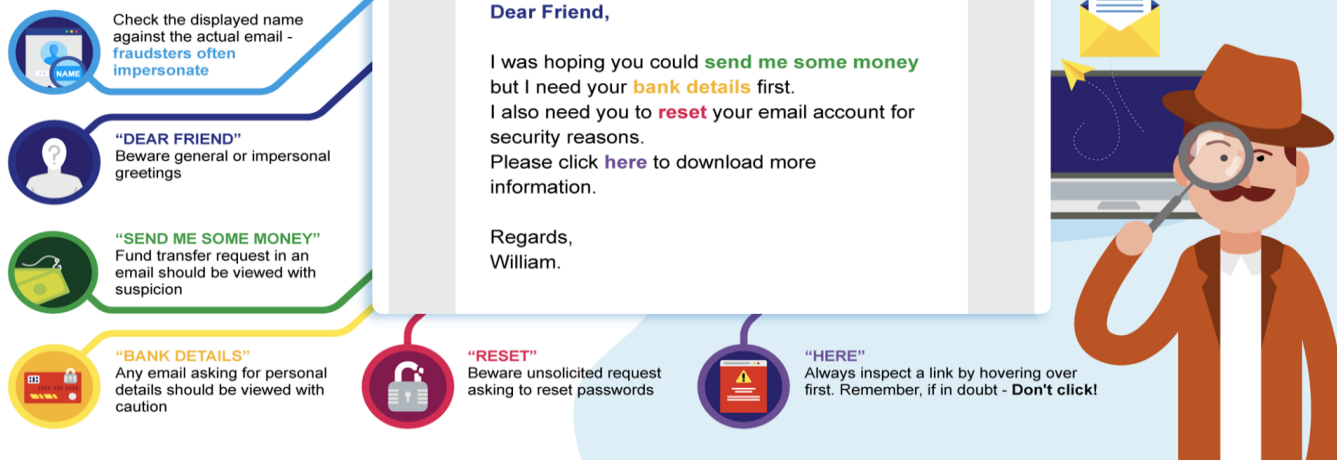
Garda National Cyber Crime Bureau
Contacts

Detective Superintendent

Garda National Cyber Crime Bureau

Harcourt Square

Harcourt Street

Dublin 2

D02 DH42

Tel: 01 6663708

Email: GNCCB@garda.ie

Or

YOUR LOCAL GARDA STATION