NILGA SAFETY INFORMATION WEBINAR

18th December 2025

The Police Service Response

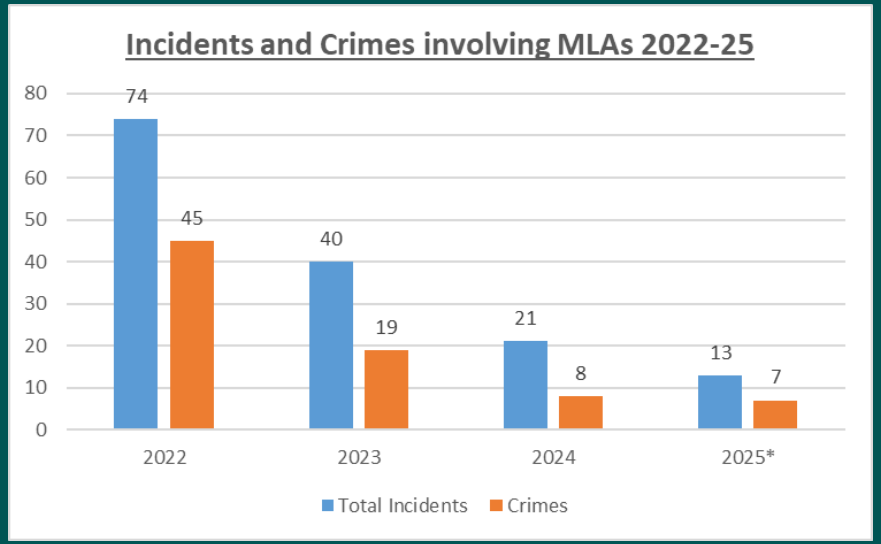
Elected representative safety officer – Chief Superintendent Stephen Murray

Elected Rep Safety - Headlines

Since 1st January 2022 MLAs have reported:

- **149 incidents**, including
- **79 crimes**.

Under-reporting appears to be an issue.

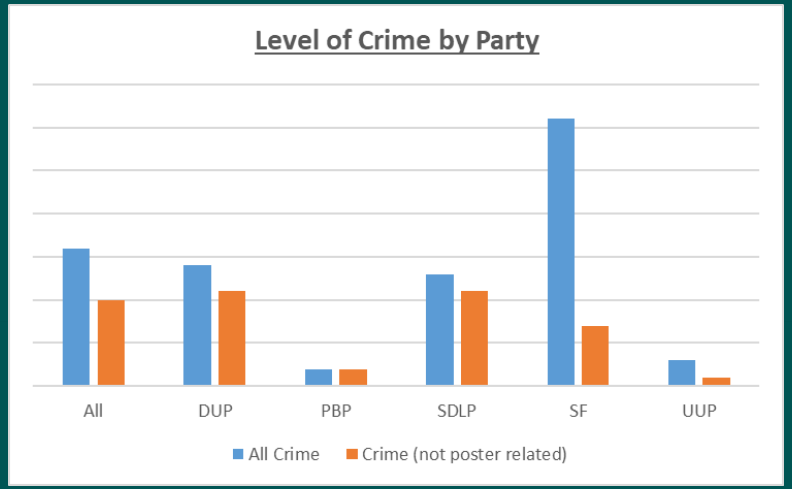


Police Service of Northern Ireland

Elected Rep Safety - Headlines

Elected representatives from **all parts of Northern Ireland** are affected by crime

Party affiliation makes no difference



Police Service of Northern Ireland

Elected Rep Safety - Headlines

Elections are a major factor

- Election posters were a factor in 47% of reported crimes

26% of current MLAs have been a victim of a crime in the past three years

- This rises to 44% if poster / election crime is included

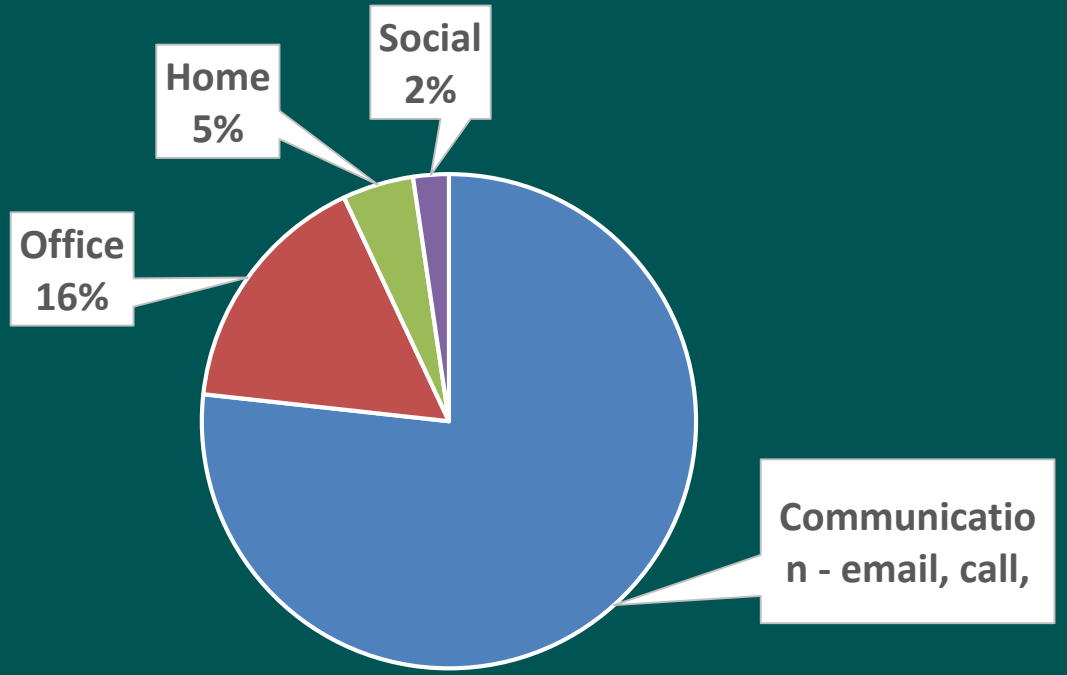
Repeat victimisation is an issue

- Some MLAs are repeatedly targeted

Police Service of Northern Ireland

Where is crime happening?

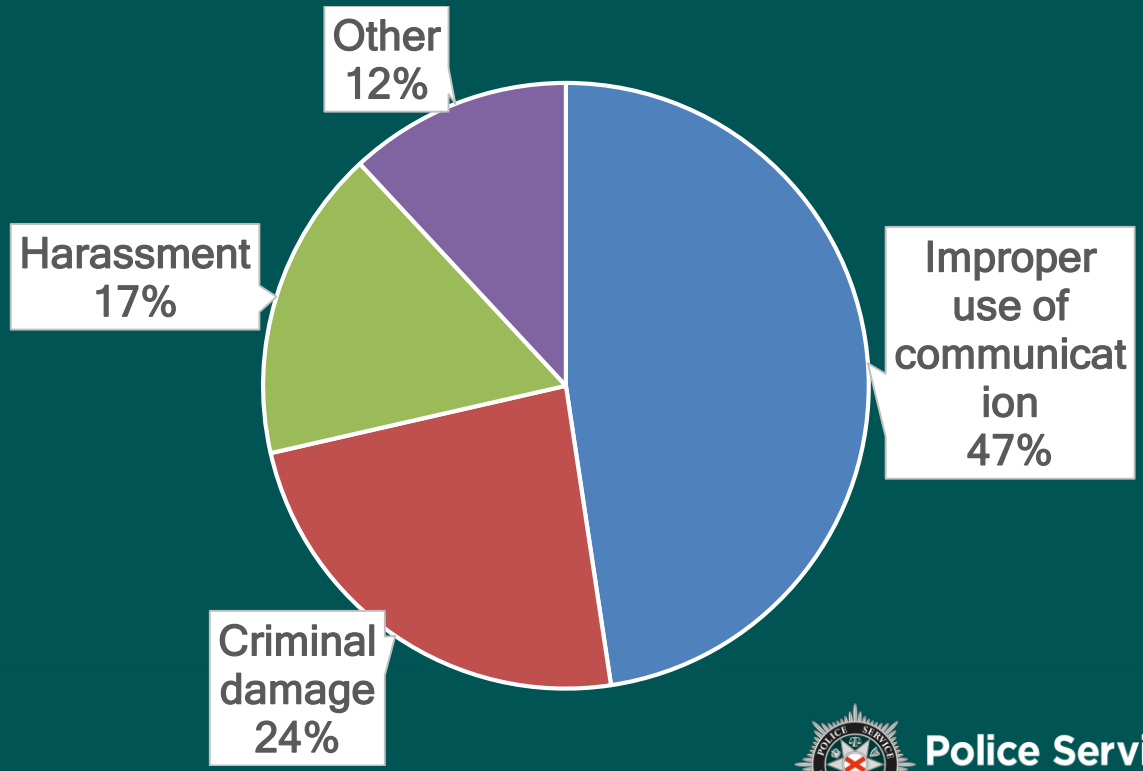
Most offences are ‘remote’: abusive, intimidating or obscene communications



Police Service of Northern Ireland

What crime is happening?

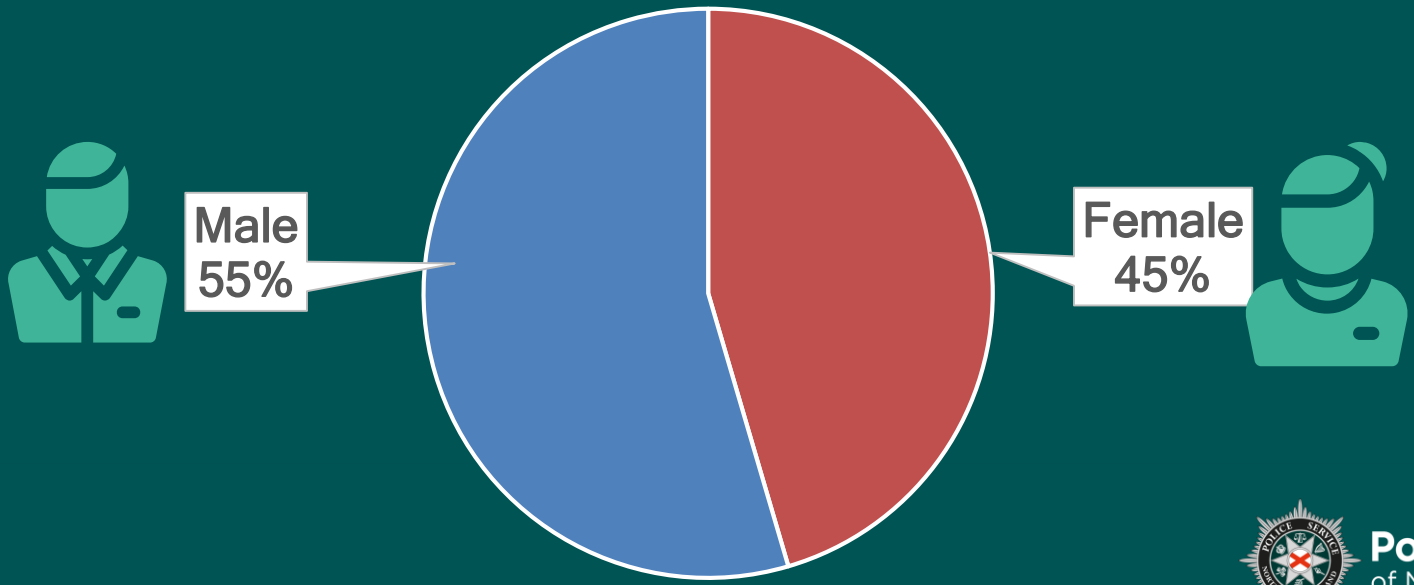
- Often multiple offences but **Communications offences** are the most common.
- ‘Cyber enabled’ / online offences a recurring theme



Police Service of Northern Ireland

Gender Breakdown

- 38% of MLAs are female but they suffer 45% of crime



Police Service
of Northern Ireland

What are we doing?

Joint working with NI Assembly and other partners

- Building understanding of the issue

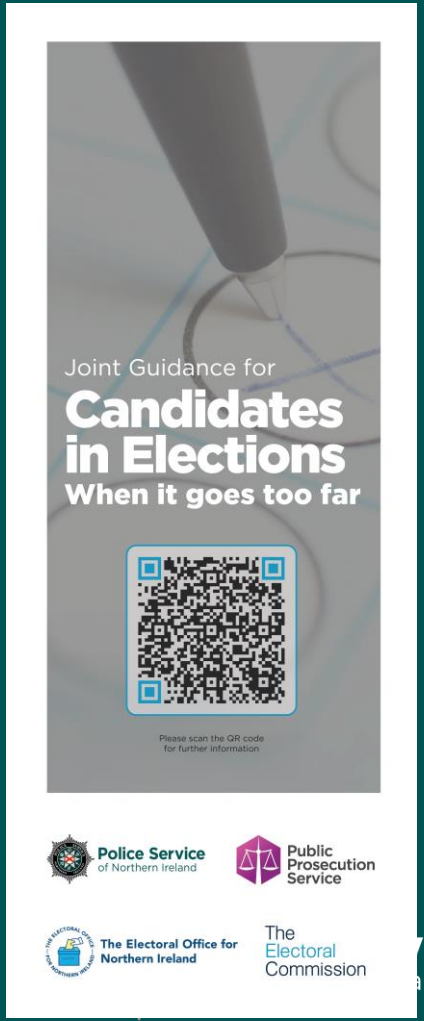
A focus on **prevention** of crimes and incidents

Providing advice and guidance

- Crime Prevention – surveys and risk assessments
- Cyber crime
- Online Resources

MLA Safety officer and MLA safety group

- Increased reassurance for victims and enhanced response



Personal & Premises Safety

Chris Sloan

Strategic Lead Designing Out Crime & Crime Prevention

AWARENESS

Prevention is Better Than Cure

Desiderius Erasmus (1466-1536)

Police Service of Northern Ireland

When are you vulnerable?

- Where patterns are set / predictable routines
- When travelling by vehicle
- Online - when using technology
- Unfamiliar surroundings
- When we are complacent

Police Service
of Northern Ireland

Engaging with the Public

- Avoid lone working –conduct visits accompanied
- Keep a record of any intimidating behavior
- Don’t engage with anyone harassing you (on and offline)
- Use “report abuse” tools on social media
- Block and report trolls
- Know what to do if you are confronted on the street
- Set up your phones emergency SOS function

Police Service of Northern Ireland

Canvassing Safety

- Be prepared – not scared
- Focus on group safety - planned activity / regular check ins
- Have a plan if followed / confronted
- Keep a record
- Use technology to canvass more safely
- If you feel threatened call the police

Police Service of Northern Ireland

Situational Awareness

Awareness of what is happening around you – recognizing threats to your safety and security

Identifying threats early = quicker reaction to danger

BE ALERT – NOT ALARMED

‘Plan ahead – Know what to do’

Police Service of Northern Ireland

Cyber Protect

D/Constable Samuel Kinkaid
NI Regional Cyber Protect Officer

Protect & Prepare

- The majority of cyber crime is preventable by taking simple steps to secure your cyber security. (Protect)

- It is important to be in a position to respond appropriately if you should experience a cyber incident. (Prepare)

we care
we listen
we act

Police Service
of Northern Ireland

NCSC - High Risk Individuals

High-risk individuals include those working in political life (elected representatives, candidates, activists and staffers).

Focus on good cyber behaviours

- *Strong Passwords*
- *Two Step Verification / MFA*
- *Protect Devices*
- *Think about what you post*

National Cyber Security Centre

Cyber security for high-risk individuals

Follow these steps to be significantly safer online and help defend against targeted attacks.

Help if you're targeted

Don't panic if you've clicked on something – report it to your organisation's IT support, even if it happened on a personal device.

Also tell them about suspicious emails or messages you receive, even if you haven't clicked on anything.

How could I be targeted?

Attackers have used spear-phishing – sending targeted emails which direct the recipient to a bad link or website – to compromise high-risk individuals and try to steal information of interest.

Be aware that your personal accounts and devices may also be at risk, as an attacker may consider them 'easier' targets.

As far as possible, you should continue to use corporately managed accounts and devices for your work, as they will be centrally managed and secured.

Protect your accounts

Use strong passwords

- Use three random words to increase complexity – and make passwords unique for each account.
- Particularly for your most important accounts, like email, social media and online banking.
- You can also use a password manager which helps you remember different passwords for different accounts.

Set up two-step verification

- Use an authentication app like Google Authenticator or Microsoft Authenticator.
- 2SV adds another layer of security so that even if an attacker knows your password, they still can't access your account.

What is a high-risk individual?

If the nature of your work means you have access to certain sensitive information, you may be of interest to nation-state actors. This includes people who work in:

- politics (elected representatives, candidates, activists and staffers)
- academia
- journalism
- the legal sector

Protect your devices

Install updates

- If you receive a prompt to update your device or apps, do it – it stops attackers taking advantage of security flaws which they can exploit to get access.
- Enable the auto-update option, so you don't have to remember.
- Only download software and apps from official stores, like Google Play or Apple App Store

Replace old devices

- Old phones and laptops that are no longer supported are more vulnerable to attack as they can't be updated – upgrade your device if support is ending soon.

Use 'Lockdown Mode'

- On Apple devices, 'Lockdown Mode' provides added security for individuals who might be targeted by sophisticated threat actors – enable it.

Protect physical access

- Use a password or pin that must be entered when the device is powered on.
- Enable the track location functions – 'Find My' on an iPhone and 'Find My Device' for Android.

Think about how you use social media

- Be careful about how much personal information you share publicly.
- Review your security settings to decide who can see what.
- Avoid accepting message requests from unknown accounts – consider calling first to verify who they are.

NCSC.GOV.UK @NCSC @CYBERHQ @CYBERHQ National Cyber Security Centre

© Crown copyright 2024. Photographs and infographics may include material under licence from third parties and are not available for re-use. Text content is licenced for re-use under the Open Government Licence v3.0

Police Service of Northern Ireland

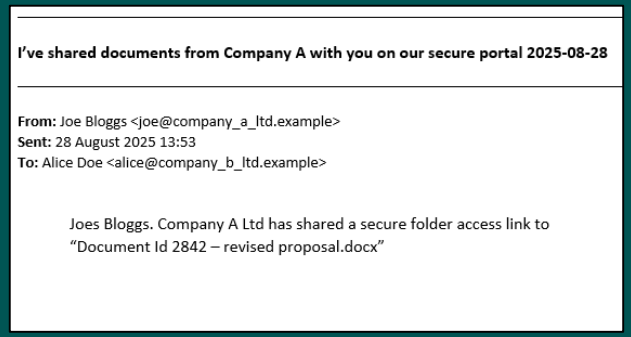
Spear Phishing

Star Blizzard

- Open Source research identifying areas of interest
- Impersonating known contacts or experts
- Targeting personal accounts
- Building a rapport
- Delivering a malicious link or attachment
- Credential harvesting

Police Service of Northern Ireland

NI Case Study



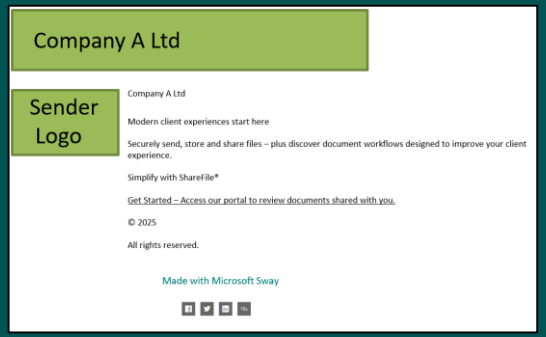
I've shared documents from Company A with you on our secure portal 2025-08-28

From: Joe Bloggs <joe@company_a_ltd.example>
Sent: 28 August 2025 13:53
To: Alice Doe <alice@company_b_ltd.example>

Joes Bloggs. Company A Ltd has shared a secure folder access link to "Document Id 2842 – revised proposal.docx"

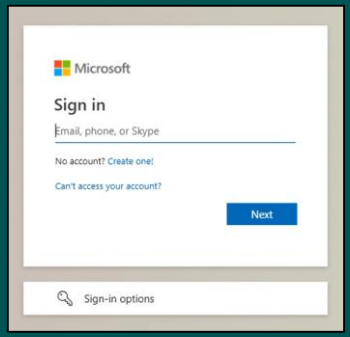
Stage 1

Email received from a known but compromised 3rd party



Stage 2

User directed to 3rd party service & asked to review documents.



Stage 3

Credentials requested Account compromised

12 Compromised organisations across NI in 4 weeks
Previous example impacted Councilors, MLAs & MPs

we care
we listen
we act

Police Service of Northern Ireland

Local Government Partnerships

NIA Information Systems Office

- Review of reported incidents, sharing of threat intel and post incident support to members.

Councils:

- Threat intel sharing and support to Council IT teams.
- Engagement with Local Government Business Continuity Group.

Police Service of Northern Ireland

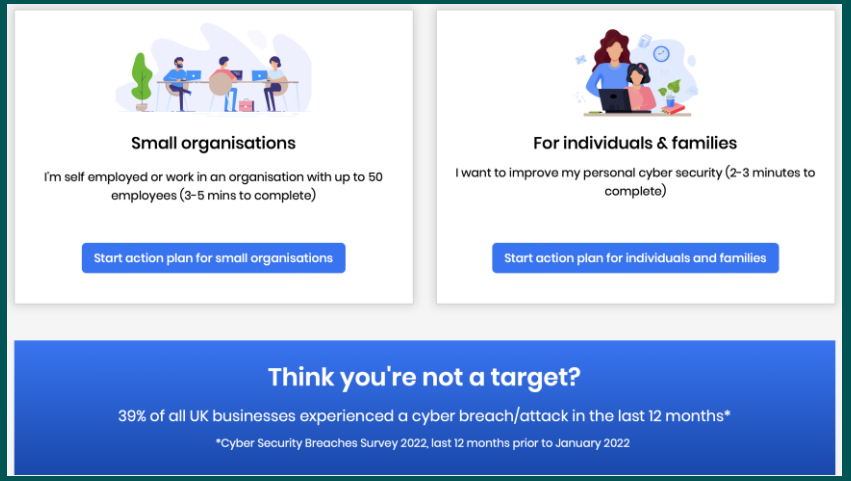
NCSC – Cyber Action Toolkit

- Free service
- Tailored & Actionable Guidance
- Step by Step actions
- Progress Tracking
- Starting Point for Cyber Security

Police Service of Northern Ireland

NCSC – Cyber Action Plan

- Free service
- Consider when onboarding
- Email passwords
- 2SV
- Backups
- Access Controls



Police Service of Northern Ireland

Contact:

Incident reporting 999, 101 or online

Report Fraud (Service for Cyber and Fraud)

www.reportfraud.police.uk / 0300 1232040

Reporting Advice

www.gov.uk/guidance/where-to-report-a-cyber-incident

PSNI General Cyber Safety Advice

cyberprotect@psni.police.uk

Thank you for Joining Us

Joint guidance available at:-
www.psni.police.uk/safety-and-support/keeping-safe/protecting-yourself/joint-guidance-election-candidates

PSNI Public Affairs Team (PublicAffairs@psni.police.uk)

Police Service of Northern Ireland