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

An Lárionad Náisiúnta
Cibearshlándála
National Cyber
Security Centre

Cybersecurity

for Political Organisations and Election Candidates

Status: TLP:CLEAR

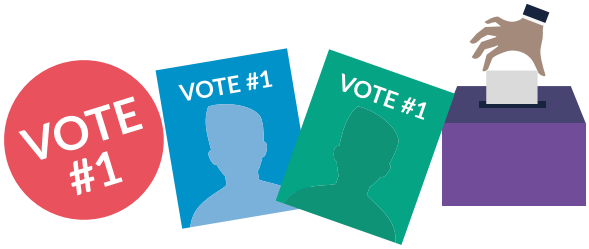
This document is classified using the Traffic Light Protocol. Recipients can spread this to the world, there is no limit on disclosure. Sources may use **TLP:CLEAR** when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, **TLP:CLEAR** information may be shared without restriction. For more information on the Traffic Light Protocol, see https://www.first.org/tlp/

Please treat this document in accordance with the TLP assigned.

www.ncsc.gov.ie

Background

Political organisations and election candidates have become targets for threat actors that wish to disrupt and interfere in the democratic process. This can be part of a wider hybrid campaign to influence voters. Cyber attacks that target election candidates or organisations can be very damaging to the candidate themselves, the political party they represent, or to society's overall trust in the democratic process. This guidance aims to raise awareness of cyber threats to democratic processes and institutions, and to help prevent attacks on both organisations and individuals.



What does this document cover?

This advisory is focused on cyber security issues which pose a risk to the security of the electoral process. **It should not be considered as a comprehensive guide for the overall security of an individual candidate or political parties' data or systems.** This advisory recommends implementing identity and access management policies, enhancing website security, preventing spoofing, educating constituents about misinformation, and preparing for ransomware and deep-fake attacks to safeguard the integrity of elections.

Securing your accounts

You or your team's personal accounts are prime targets for attackers. If compromised, attackers could access your stored information. If possible, you should prioritise the use of corporately managed accounts and devices for professional tasks, as they benefit from centralised management and enhanced security measures. If you do not have access to such software, implementing the following measures can still greatly reduce this risk.

- **Use of strong passwords:** Create complex passwords by using a minimum of 12 characters which include numbers and symbols to increase complexity. Alternatively, use three random words and make each password unique for every account, especially for critical accounts like email, social media, and online banking. Consider using a password manager to help you remember these different passwords.

An Roinn Comhshaoil, Aeráide agus Cumarsáide
Department of the Environment, Climate and Communications
NCSC
An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

- **Multi-Factor Authentication (MFA):** MFA should always be used when logging into internet facing accounts – this could be an app or website, or an email account. Use an authentication app like Google Authenticator or Microsoft Authenticator. MFA adds an extra layer of security, ensuring that even if an attacker knows your password, they still cannot access your account. If multi- factor authentication is not enabled, it is entirely possible for an attacker to use stolen credentials or to 'brute force' access to an account by simply guessing a password.
- **Social media use:** You should check for unusual logins. Set up notifications to send a text or email alert when your account is accessed from a new device or location. Exercise caution when sharing personal information publicly. Review your security settings to control who can view your information. Avoid accepting message requests from unfamiliar accounts; consider calling to verify their identity first. Please refer to the individual social media guides linked to on the Coimisiún na Meán site.

Multi Factor Authentication (MFA) Guidance

NCSC-IE

Can you keep a secret?

6 tips for account security

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

An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

Potential types of attack to be aware of:

Denial of Service (DoS) attacks

Attackers commonly launch destructive attacks against websites of interest, typically in the form of Denial of Service (DoS) attacks. Ensure that your website is resilient against the threat of DoS attacks, and have appropriate controls in place. Public-facing websites (e.g. those displaying party-related information) are vulnerable to these attacks, which are often unsophisticated but highly effective. Organisations should consider the use of content delivery networks (CDN), upstream internet service provider protection, cloud service providers' DoS protections and on-premises solutions.

Understanding and responding to DDOS attacks

CISA

Website defacements

Website defacements involve the unauthorised alteration of web pages by attackers exploiting vulnerabilities like SQL injections, primarily targeting unpatched or misconfigured sites. These attacks can damage public trust, spread disinformation, and highlight broader security issues. To mitigate risks, election officials should maintain updated software, implement the principle of least privilege, use web application firewalls, and enrol in vulnerability management programs.

Implement an **identity and access management policy** to determine who should have access to specific systems, data, and functionalities. Clarify the reasons behind their access requirements. Outline the circumstances under which access is permissible.

12 Steps to Cyber Security for Business

NCSC-IE

What Is Access Control? | Microsoft Security

Microsoft

Spear-phishing

Those targeting political groups often use spear-phishing, especially through emails, to manipulate specific individuals into revealing sensitive information. The use of artificial intelligence makes these attacks even more convincing. To combat this, political organisations and candidates should employ multi-layered defences against phishing, rather than solely relying on users to detect malicious emails.

Quick guide: Phishing

NCSC-IE

Spoofing

It is important to introduce anti-spoofing measures, as in the absence of adequate controls, an attacker might exploit your domain to send emails masquerading as an individual or organization, a tactic known as spoofing. This could enhance the credibility of spear-phishing emails.

Ransomware attacks

Protect against ransomware attacks by making sure access to critical data is locked down, and that you have MFA systems in place. Data should be encrypted and backed-up regularly. Attackers can block access to critical files or delete them completely. Attacks involving the exfiltration and leaking of data or documents can be hugely damaging to the reputation of a party or candidate.

Getting Started With DMARC

DMARCLY

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

NCSC
An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

How can devices be protected?

Cyber attackers may attempt to gain access to your electronic devices; including computers, phones, or tablets, to obtain sensitive information. If successful, they could compromise your privacy, monitor your activities, or engage in identity theft. However, there are proactive measures you can take to enhance the security of your devices:

- replace outdated devices and make sure software is up to date, especially your device's operating system (OS);
- use complex passwords and/or biometrics to lock your device;
- make sure your device is set to auto-lock when not in use;
- enable 'Lockdown Mode';
- secure and backup data from your devices as well as limiting physical access;
- ensure you can maintain and or recover access to all online services if your device is lost or stolen. Password managers can help here. **It is good practice for a candidate's team to practice tracing missing devices, remote wiping and securing accounts;**
- enable the track location functions – 'Find My' on an iPhone and 'Find My Device' for Android;
- if there are signs that your device may be infected such as unexplained apps appearing on the device or reduced performance, you should restore from a backup from a time before the issues began to arise. If you do not have a good backup, consider a factory reset of the device;
- where possible, have a separate work device from a personal device that has access to any of your sensitive data such as email. Remove or block the installation of any non-work-related applications on the work device;
- if social media is required, then such apps should be installed on a separate device reserved for that sole purpose.

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

NCSC
An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

Emerging Technologies: Artificial Intelligence (AI)/Deepfake

Artificial intelligence and the advancements in the capabilities of Generative AI such as Large Language Models (LLMs) have recently garnered significant attention. Generative AI can be used to assist with the creation of malware, enhance DDoS attacks, and improve phishing and social engineering techniques, including lifelike audio, realistic fake images, counterfeit social media profiles, and deepfakes. AI-powered chatbots can also be used in phishing attempts, information manipulation, and cybercrime. These tactics are not new, but AI enables their deployment with greater speed, sophistication, and lower cost, posing enhanced risks to election security.

To safeguard against these threats, individuals and organisations should educate employees and users about recognising phishing attempts. Remember to regularly update software and security protocols. Maintain a healthy scepticism towards unsolicited communications, and separately verify the authenticity of sources through a different medium (such as telephone). This can significantly reduce the risk of falling victim to these phishing attempts.

Many of the best mitigation measures for generative AI-enhanced threats are the same cybersecurity best practices that have been recommended in the NCSC's guide on Generative AI for public service bodies. The Department of Enterprise, Trade and Employment have published a national strategy on the country's approach to AI - available at this link

Social media companies can remove content if it is deemed inappropriate or contains misinformation. Coimisiún na Meán have recently published guidance on this, available at this link.

Remember, candidates can also play a role in educating the public about the existence of deepfake technology and how to critically evaluate information online. By promoting media literacy and encouraging scepticism, they can help mitigate the impact of misinformation on the electoral process.

NCSC's guide on Generative AI for public service bodies

NCSC-IE

National Artificial Intelligence Strategy for Ireland

Government of Ireland

Information Pack for election candidates

Coimisiún Na Meán

Responding to a suspected attack

It is important to remember that often an attacker's goal is to undermine the public's trust and confidence in the security of the electoral system. Don't play into their hands by inadvertently amplifying false, misleading, or malicious content, or overstating the impact of a cyber incident.

If you receive a suspicious email, refrain from clicking on any links or responding until you've verified the sender's authenticity. Report it to your organisation's IT support, even if it's directed to a personal account. The NCSC offers guidance on recognising and handling phishing emails .

Quick Guide: Phishing

NCSC-IE

If you've clicked on a link or suspect a security breach, it's important to stay composed, even if you think you've made a mistake. If the problem arises on devices or accounts provided by your organisation, inform the IT support team.

Reporting incidents is a crucial step in addressing and preventing cyber attacks.

For individuals dealing with a suspected attack please contact An Garda Síochána at your local Garda station and review the below links.

Cyber Crime

An Garda Síochána

Fraud

An Garda Síochána

For organisations that have had a breach please contact incident@ncsc.gov.ie, or refer to the NCSC webpage https://www.ncsc.gov.ie/incidentreporting/.

Incident Reporting

NCSC-IE

Protecting yourself online and criminal activity

If a candidate feels threatened or targeted by an individual or group, they or their team should contact An Garda Síochána. Some good guidance in relation to this can be found here:

Safety Guidance for Candidates

AGS/SHE/WomenForElection

Regardless of your setup, it is important to regularly review and understand all the risks you manage. The NCSC offers guidances which will assist in supporting your IT infrastructure. They can be found here:

NCSC Guidance

NCSC-IE

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

NCSC
An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

Contact Details

National Cyber Security Centre,
Department of the Environment, Climate and Communications,
29-31 Adelaide Road, Dublin, D02 X285, Ireland.

info@ncsc.gov.ie

+353 1 6782333

https://twitter.com/ncsc_gov_ie

www.ncsc.gov.ie

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

An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre