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

NCSC

NATIONAL CYBER SECURITY CENTRE

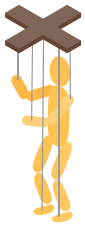
Quick Guide: Cyber Security Best Practice for Electoral Candidates

Background

In today's environment, political parties have become targets for threat actors that wish to disrupt and interfere in the democratic process which can be part of a wider hybrid campaign to influence voters. Cyber-attacks that target electoral candidates can be very damaging to the candidate themselves, the political party they represent or to societies overall trust in the democratic process.

This cyber security best practice document has been produced by the NCSC to assist electoral candidates in implementing key priority preventive measures that can help to reduce the likelihood of them becoming a victim of a cyber-attack and the negative impacts that may result.

Common Cyber Attacks



Hack and Leak

Hacking of messaging service, social media and e-mail accounts to steal sensitive data which is then leaked publicly to discredit an individual candidate. Sometimes attackers will alter documents or plant false leaks amongst the facts in their release of information.

Defacement

Hacking of social media accounts and candidate websites to deface them or publish damaging disinformation.

Malicious Insider

Leaking of sensitive information by an insider to expose internal communications between members of a group.

These types of attacks are often enabled by phishing e-mails sent to the targets e-mail account to steal account credentials or trick the user in to downloading a malicious file.

Best Practice to Reduce the Risk of a Cyber Attack

Enable multi-factor authentication (MFA) on all messaging services, social media, e-mail and remote access accounts to prevent attackers gaining access to these accounts even if they have access to your password.

Lookout for indicators of phishing within e-mails and messages and never click on links or attachments unless you know the sender and why they were sent to you.

Use strong unique passwords for each of your accounts particularly your important accounts like e-mail and social media. If more than one person operates the account, contact the relevant platform to setup a multi-user account and never share passwords. Consider using a password manager.

Encrypt your devices to safeguard your data. Keep your devices updated regularly with the latest software and security patches. Secure your mobile device with a passcode or other form of identification (fingerprint or face). Power off and on your device at least once a week.

Backup your data, including credential data, store it separately in a secure location and know how to recover it if your device is lost or stolen. Consider backing up your data to a cloud service. Ensure data is securely erased if device is to be recycled.

Use trustworthy encrypted messaging apps to ensure your private conversations are kept private. When using messaging apps, ensure you know who the recipients are in group conversations.

Avoid public or open Wi-Fi and use a reputable virtual private network (VPN) product where possible to encrypt your internet traffic and make it more difficult for third parties to track your activities online and steal data.

Reporting

Political organisations can subscribe to the NCSC's Alerts & Advisories service. Organisations and candidates can register with the NCSC by emailing certreport@decc.gov.ie

Further Information

Further information for Political Parties and Candidates is available at NCSC Guidance for Political Parties and Candidates