National Cyber Security Centre

2102260209-NCSC

A part of the **Department of the Environment, Climate & Communications**

NCSC Cyber Security for Political Parties and Candidates

Cyber security advice to assist political parties and candidates in securing their IT systems.

Status: TLP-WHITE

This document is classified using Traffic Light Protocol. Recipients may share TLP-WHITE *information freely, 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.*

Contents

1 Introduction

The National Cyber Security Centre (NCSC), which is part of the Department of the Environment, Climate & Communications is the national cyber security authority. Its roles include leading the management of major cyber security incidents, providing guidance and advice to citizens and businesses, and managing cyber security related risks to critical national infrastructure and key services.

The NCSC includes the state's Computer Security Incident Response Team (CSIRT-IE). CSIRT-IE is an internationally accredited response team tasked with incident response for national cyber security incidents and enhancing the situational awareness for constituents with regard to cyber security threats at a governmental and national level. CSIRT-IE is a national point of contact for all cyber security matters concerning Ireland.

In December 2017, Government established an interdepartmental group to consider the security and integrity of the electoral process in Ireland. The group includes representatives of key government departments and state agencies with a role in the security of the electoral process, including the NCSC and is coordinated by the Department of the Taoiseach

The first report[1] of that group considered these issues and made a series of recommendations for further action. The report found that that risks to the electoral process in Ireland are relatively low, considering the mitigating factors already in place, however there is a more substantial risk posed by the spread of disinformation online and the potential for cyber-attacks on the electoral system, including on candidates themselves. The report set out a series of recommendations that should be taken to enhance the cyber security of the electoral process in Ireland, including that advice be provided to political parties and politicians in relation to cybersecurity by the NCSC.

This advisory contains four distinct elements.

1. An outline of the potential cybersecurity risks for political candidates or political parties, which may have an effect on the security of the electoral process.
2. Advice for all political candidates for election so that they might better protect themselves and their data
3. Guidance for management and IT administrators in political parties
4. Services that the NCSC and others will be able to offer to candidates in securing their data.

[1] https://assets.gov.ie/2224/241018105815-07f6d4d3f6af4c7eb710010f2ae09486.pdf

2 Cyber security risks for political parties and candidates

Political candidates and parties face the same common threats as all other orgaisations. Succesful cyber attacks on organisations involved in politics creates additional risk to electoral proccess.

This advisory is focused on cybersecurity issues which pose a risk to the security of the electoral process. Therefore, it should not be considered as a comprehensive guide for the overall security of an individual or political parties' data or systems.

The 2018 report identified two major categories of cybersecurity risks to the political parties and candidates:

Destabilisation Events: This is a term used to describe the broad range of attacks that can be undertaken to attempt to undermine or influence the electoral process.
These include Distributed Denial of Service (or DDoS) Attacks on websites used by entities engaged in the electoral process (including media, political parties or campaign groups) and the defacement of websites or the destruction of data owned by any of those same entities. Social media accounts and other online platforms are also targets for destabilisation events.

Attack	Description	Attack Vectors
Defacement	Unauthorised alteration of public media belonging to or associated with a targeted ideology or organisation. Commonly associated with websites, now often targeted against social media accounts and services. Modifying organisation websites to attack visitors with malware.	Phishing and SMSishing emails and texts leading to credential theft, Abuse of user privileges by insiders, Vulnerabilities in website software.
Denial of Service	Preventing users/the public from using or accessing IT services. Trigger social media account lockouts by manipulating automatic abuse systems, and other legislation in other countries, most frequently abusing German laws.	Publicly exposed services, Social media policy abuse.
Ransomware	Locking organisations files from owners. using encryption. Recent attacks steal confidential files, and threaten to release them unless ransom is paid.	Phishing emails with malware payloads. Abusing compromised credentials
Deception	Internet resources similar to that of legitimate organisations may be registered, and used to mislead visitors or redirect internet traffic away from the targeted site.	Registering domains similar to governmental or political organisations

Data Exfiltration: The second type of attack mentioned in the Interdepartmental Group report refers to the theft of information from the IT systems of Government or any entity involved in the political process, and its subsequent exploitation by means of release (either in original or edited form). This could also include the possibility of data being stolen from political parties or individuals personal IT systems, including messaging services, social media and email.

Attack	Description	Attack Vectors
Information theft	Stealing organisation's files, without being detected, to exploit in additional operations. These may include tactical leaking the information to media.	Phishing emails with Remote access Trojan Malware payloads, and credential harvesting payloads
Information leak	Sharing of organisation private communications and documents with public or press. Examples are mass release of organisation email communication, but in recent years, sharing contents of messaging application groupchats, and private texts has also been observed in political context.	Phishing emails with remote access Trojan payloads, unauthorised access through poorly secured login portals, credential abuse.

3 Advice to Candidates

Candidates and their immediate campaign managers are responsible for the security of their data and systems. The vast majority of the the identified risks can be mitigated by implementing common cyber security practices, the priority actions are outlined below.

3.1 Account Security

Multi-Factor Authentication (MFA): All social media, email and remote access accounts should have multifactor authentication enabled. This is essential to protect any personal data stored on a system. 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. This remains an extremely common tactic, and enabling multi factor authentication is the single most important step that candidates should take. Ideally you should avoid using SMS for MFA as SMS messages may be intercepted, consider instead an authentication app . However, having SMS MFA is much better than no MFA at all.

Review Activity On Your Accounts: Most services will allow you to see a list of devices on which you are logged into an account (home computer, phone, tablet). Candidates should check for unusual logins. Set up notifications to send a text or email when your account is accessed from a new device or location.

Password: Strength, Reuse and Sharing: Password sharing is a significant risk and passwords should never be shared. If multiple users need access to a account, such as a social media account, most platforms can arrange this for political accounts. All users operating a political account must understand the risks associated with political accounts and should be able to recognise the signs of phishing.

Password strength is enforced by most platforms, but should be at a minimum 12 characters long and and contain numbers and symbols in order to increase complexity. Do not reuse passwords for multiple services, to minimise the damage from credential compromise.
Use of password managers [2] is highly recommended. Password managers allow you to create unique long complex passwords for all of your accounts, and prevent password reuse, and remove the burden of remembering multiple passwords or passphrases.

3.2 Device Security

- **Cleanup**
  - Clean up your devices. Ensure you are handling personal data in accordance with relevant data privacy legislation and guidance from the DPC. It is good practice to minimise and remove unnecessary personal data from your devices.

    Ensure that all your devices are set to automatically check for updates. Keeping your devices up to date with the latest security patches reduces the opportunity for an attacker to gain access. Minimise the number of applications installed and only from official application stores. Ensure all data is securely erased from devices which will be recycled. In most cases merely

[2] https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/password-managers

deleting the data is not enough – your IT Dept can offer advice/perform secure data erasure for your devices.

Recent information about mobile spyware has highlighted that a key defence against many forms of mobile malware, including spyware is simply turning the phone off, removing the malware from memory. Set a regular reminder to power off and restart at least once per week.

- **Backup**
  - Make backups of all your data and ensure one copy is always offline. Most devices have options to upload your data to a cloud service. Ensure that the cloud service allows you to recover from previous backups.

    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 a good practice for a candidates team to practice tracing missing devices, remote wiping and securing accounts.
- **Lockup**
  - Encrypting your devices can keep your data safe even when it is lost or stolen. Disk encryption is easy to enable and does not take much time.

    It is recommended that you enable location services that can track your device and help find them if lost. Some location services also offer remote wiping features. Teams should rehearse this process to be familiar with it.
- **Restore**
  - Signs that your device may be infected are the battery draining faster than normal, larger amounts of data being consumed than normal, unexplained apps appearing on the device, or reduced performance. If you suspect that your device is infected your 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.

3.3 Phishing

Phishing emails can be convincing to even seasoned IT users. A phishing mail contains a text lure to induce the user to activate the second part, the payload. The payload contains the initial attack vector, leading to malware or sites designed to install ransomware, steal credentials or banking detail, or enable further remote access by the attackers. There are some indicators that help users detect phishing email:

- Messages that create a sense of urgency may be trying to rush you into making a mistake.
- If it sounds too good to be true, it probably is.
- Grammatical errors should be red flag, official organisations will not usually send messages with simple spelling or grammatical errors.
- Official organisations will usually not send mail from personal email addresses (such as gmail.com or yahoo.com). Always hover over the sender to ensure it is who it says it is in the From field.
- Hyperlinks in the email will reveal their actual destination when cursor is hovered over the link. On a smartphone, holding your finger down on a link will open details about it.

- Some malware will compromise a victims email account, and use it to send to add malicious emails to an existing conversation with a person.
- Messages that begin with “Dear Customer” or some other generic greeting require closer scrutiny, if genuine they will usually personalise their greeting.

3.4 Actions On Compromise

In the event that you detect unauthorised access to your information, or are subject to another form of cyber attack, please consider the following actions, in order:

- Do not turn off computer or device.
- Remove device from any network. Disconnect network cable, turn off wifi, mobile network and bluetooth. Be prepared to send the device for analysis. This mean the device shouldn’t be used at all after removing it’s networks.
- Inform your IT support provider, inform IT support of the device owner, and notify the NCSC.
- Follow advice and instructions from technical support.
- Be prepared to restore your information from backups.

Incidents can be reported directly to certreport@decc.gov.ie mailbox.

The CertReport Inbox is managed by a duty responder between 09:30 to 16:00.

CSIRT-IE provides a telephone contact on +353-1-6782333.

This is monitored by the duty incident responder during office hours

4 Guidance For IT Administrators And Support Staff

All types of attackers need a way of getting initial access to targeted infrastructure. The most common vector for this is via emails and phishing. The next most common vector is via malware downloaded from compromised websites. Websites, especially those on third-party services are regularly scanned by threat actors [3] for vulnerabilities, to facilitate unauthorised access.
Additionally, credentials are routinely offered for sale on criminal forums, and stolen political organisation credentials offered for sale may be marketed as such during the run up to an election. Note that this is not an exclusive list of potential vectors or remediation policies, and there is vast amounts of research published on this topic.
These vectors offer the greatest return on attackers' effort and resources, and controls against these vectors are the most effective means administrators can employ to reduce the associated risk to users.

4.1 Phishing, Spear Phishing And Whaling Attacks

Phishing emails can be convincing to even experienced IT users. Spear phishing emails are phishing emails that are custom designed for a particular organisation's users. These may emulate normal business about current topics and appear to be from credible addresses. These phishing emails should be taken seriously, and investigated thoroughly. CSIRT-IE's response team welcomes all reports about spearphishing emails.

Types of Phishing emails:

Attack Type	Mitigation
Compromised Email attack Mail recieved from a trusted contact, whose account is compromised, and used to contact their correspondents with malicious email.	**User Awareness –** Check before opening links even from trusted contacts **Administrators –** de-fang URLs in email,implement MFA
Look-a-like/Impersonation Domains From: John.Doe@m1crosoft.com Subject: Urgent - please update payment details	**User Awareness –**Check the from address **Administrators –** Use SBRS/sender reputation, Email Filtering
Display Name Spoofing From:John.Doe@microsoft.com Spoofed email looks like its coming from a credible source	Incoming DMARC checks and blocks All of the above

Whaling is a more detailed spearphishing campaign, targeting high value targets, both in organisation leadership and IT administration. These are highly customised to the individual and may pretend to be from addresses that the target regularly communicates with. Any organisation that detects a whaling email should consider reporting it to CSIRT-IE immediately, in addition to their incident response process.

[3] Cyber attacks fall into three categories; **Hacktivist** compromise the security of a computer system, for politically or ideological purposes. These attacks are often very public, intended to draw attention to their cause. **Foreign Intelligence Agencies** (IA) seek to access confidential information while retaining their persistent access, and are rarely detected. Not every attack on a political organisation is politically motivated. The majority of cyber security incidents across all organisations are attacks by **criminals and casual hackers**.

There are few technical counter measures available to organisations to prevent targeted phishing emails from arriving into users' inboxes as they are designed to mimic legitimate emails. Anti spam services filter out the fast majority of spam and phising emails. However, these may not detect targeted emails since, by their nature; they won't be directed to other members of that community and advanced threat actors would use clean infrastructure.

Civic society organisations with suitable email infrastructure can sign up to Microsoft's Account Guard[4] which will help protect against account breach and unusual activity.
Training users to recognise and report phishing emails and to test the community on an ongoing basis is always recommended, and there are key points mentioned in the advice to candidates.

However organisations should operate on the principle that eventually, a user will open a malicious link and compromise the network. and this leads onto the need for additional controls and mitigation measures against malware and credential harvesting sites. Basic cyber security protocols such as multi-factor authentication, will significantly reduce the risk of damage to the organisation.

4.2 Malware

First stage malware seeks to gain access, and persistence[5]on the attacked computer, to allow additional more damaging and lucrative payloads to be installed, e.g. ransomware. The most common initial vector for malware is from phishing emails, followed by compromised websites. Malware can be also installed directly from External Storage Devices (USB), and organisations should consider security software policies that restricts use of these devices and scan these devices on mounting to a device.

Phishing emails with malware will contain a payload- a link to a malicious site, or an attachment containing first stage malware downloaders. These malware payloads may be difficult to detect, however there are controls available that make it harder for attackers to exploit successful phishing email.

- Prevent Macros running in MS Office documents, to mitigate against common threats.
- Ensure all users have some form of webfilter on their local computer, to mitigate against visits to known malicious domains.
- Ensure that user accounts have the least privileges needed for their role- additional privileges can be enabled as needed e.g. Local Admin to install software, but remove once complete. This provides some protection against misuse of credentials.

Compromised websites are legitimate sites that have been hacked to add hidden code, to either download malware directly to the computer or to redirect the visitor's browser to eventually visit a malicious site where first stage malware is downloaded onto the computer.
Watering hole attacks are a form of compromised site that has been hacked in order to target the audience of that page's' content. Reputable, known sites are chosen as they are less likely to be blocked on webfilters, and malicious resources from that site may be accepted by users more than a

[4]Microsoft offers Accountguard to civic society organisations at no cost. www.microsoftaccountguard.com/en-us/
[5]Persistence is the term that describe how a criminal sustains their access to a system

meaningless site.

4.3 Credential Abuse

All organisations are vulnerable to abuse of user credentials. These may be disclosed from phishing emails, harvested by malware from devices and webpages, or abused by insiders, as well as identified as a passwords reused from other services. As the credentials are valid, abuse may not be detected by systems. Implementing multi-factor authentication on all accounts will significantly reduce the risk of credential abuse.

Ensure that passwords are changed on a regular basis. There has been significant debate on the effectiveness of this advice, given the increased power of password crackers. Password expiry periods should be chosen to minimise the usefulness of a cracked, valid password to an attacker.

Enable logging on user account logons, and if using a cloud service, contact your provider for best security practice configuration on your service.

4.4 Operational Security

Staff and candidates are at increased risk when using remote IT resources . These risk are inherent to remote working, and parties should consider the advice provided by the NCSC [6] about remote working.

- General web browsing can pose certain risks and provide opportunities for an attacker to eavesdrop on confidential communications or infect a device. Ensuring HTTPS is always enabled helps secure and encrypt the traffic between your user and the website. HTTPS Everywhere is a Firefox, Chrome, and Opera extension that strengthens the encryption between your device and major websites.
- Another way to protect users is through a VPN. A VPN allows you to create a secure channel between your user and the VPN providers servers using encryption. VPNs encrypt the internet traffic and this makes it more difficult for third parties to track a users activities online and to steal data. A VPN is recommended where users often use public wifi networks, or share networks with a large amount of people.
- Secure Messaging Service (SMS) is a convenient messaging format, however it is not secure and can be easily intercepted or spoofed. It is recommended that when communicating with others, you use a trustworthy encrypted messaging app, such as SignalApp.[7]

4.5 Denial Of Service (DoS) And Defacements

Organisations' websites are attacked by Denial of Service (DoS) attacks, or by website defacement. In modern era, social media accounts are also targets for both DOS and defacement.

[6] https://www.ncsc.gov.ie/pdfs/WFH-Advisory.pdf

[7] Using SignalApp is encouraged by the EU commission for its stakeholders https://joinup.ec.europa.eu/collection/open-source-observatory-osor/news/signal-messaging-service

Website DoS can be accomplished by criminal groups who get paid for attacking sites. Few political parties have the scale to withstand largescale DOS attacks; however, there are services that protect sites by shielding them behind their own service. Project Shield[8]from Google will provide this service to political parties and other civic societies.

Social Media DoS is a more complex attack exploiting the service terms and conditions, to cause an automatic lockout. For example, an account may be locked by automatic policy enforcement after it is subject to mass reporting for policy breaches, or by triggering automatic suspension procedures through mass numbers of accounts follow/unfollowing an account. Some Social Media services have offered additional services for political candidates. Parties should contact the public policy departments of social media services that they rely on.

While some attackers or criminals may abuse credentials to deface websites, basic scripts can automatically detect and attack vulnerabilities in a website. There are free services provided by IT security companies that scan websites for vulnerabilities, and provide reports to administrators. Tenable's Nessus provides a charity license to qualifying organisation. The open source Wordpress site scanner WPScan can check WordPress sites and associated plugins for vulnerabilities.

The best practice is for website owners to check that their website software and plugins used are up to date using these scanners, and provide details to the administrators if patching is required. If websites are managed by a contractor, consider agreeing a patch level that they should maintain.

4.6 Incident Response Planning

The following best practices will help to ensure you are better positioned to respond to and recover from a cybersecurity incident. The key point is that minimising damage from a major incident is only possible with planning and practice.

- Develop a comprehensive Incident Response Plan that includes assigned roles and responsibilities of the response team, as well as backups so that each person knows exactly what is expected should an incident occur.
- Ensure procedures are available offline and include:

  - Log book which will detail the information that is needed to be collected per incident

  - Who to notify and up-to-date contact information.

  - If you feel that your organisation does not have the skills to manage a incident, consider arranging support from a specialist firm on a retainer.
- Conduct table top and if possible simulation exercises to ensure your team is trained on the incident procedures and tools and can operate efficiently and effectively during an incident scenario.
- Consider public interest in the incident and include communication planning as part of incident plannin.

This list is not conclusive- every organisation should plan its incident response according to its own assessment of risks and resources. An organisation that has not planned its response to a major IT incident places itself and its stakeholders at increased risk.

[8]Details about Project Shield are at https://www.projectshield.withgoogle.com/landing

5 Resources

CSIRT-IE operates the certreport@decc.gov.ie mailbox.

Incident reports can be submitted to this mailbox.

CSIRT-IE provides a telephone contact on +353-1-6782333 within office hours (09:30hrs - 16:30hrs).

NCSC regularly publishes news, alerts and advisories on its website https://www.ncsc.gov.ie

Follow NCSC on Twitter @ncsc_gov_ie

For less urgent matters and general inquiries please mail certreport@decc.gov.ie

Registered Political organisations can subscribe to the NCSC's proactive monitoring of vulnerabilities and activity in cyber security by signing up to NCSC's Alerts & Advisories service. This will allow NCSC to send relevant information and to contact them directly if the need should arise. Alerts and Advisories will be sent to a single point of contact email.

The CSIRT-IE welcomes all reports of cyber security incidents and/or attempts to attack constituents. If a report gives enough detail, NCSC may be able to provide significant additional information to impacted organisation. This service is conditional on registration with the CSIRT-IE.

Advice From The Office Of The Data Protection Commissioner

The Office of the Data Protection Commissioner published advice on data protection and electronic canvassing. This advice should be considered by parties and candidates.

https://www.dataprotection.ie/en/dpc-publishes-guidance-data-protection-and-electoral-and-canvassing-activities

Advice From Facebook

Facebook's public policy department has provided this advice, in relation to their Social Media service.

"Protecting election integrity is one of Facebook's highest priorities. It's why we've worked to develop smarter tools, greater transparency and stronger partnerships to address current and emerging threats.
As a candidate standing in the general election on 8 February, it is important for us that you have a safe experience on our platforms and are aware of the tools available.

- **Safety for Page Admins:** We provide a number of useful moderation tools to help with content management, including a Facebook Safety Guide for Page Admins, which provides guidance on protecting your own Page and the tools available to do so.
- **Account Security:** Facebook accounts may be targeted to gain access to sensitive information. Set up two-factor authentication to protect your account in addition to your password. Also, use our Security Check-up tool to help you log out of unused apps and browsers, manage your alerts and strengthen your password. For additional security features and tips, see here.
- **Advertising on Facebook and Instagram:** Advertisers who create or edit ads about social issues, politics and elections must complete an authorisation process, place "Paid for by" disclaimers on ads, and have their ads entered into the public Ad Library for seven years.
- **Facebook for Government, Politics & Advocacy:** Our website, https://www.facebook.com/gpa, provides best practice information and resources across a range of areas, including account safety and security, tips for connecting with your audience, and page admin tools."

Advice From Google

Google offers two services that may be of interest to candidates and organisation:

- "Protect Your Election provides tools to help stay protected from these digital attacks, and resources that support reliable election information and reporting"
- "The Advanced Protection Program safeguards the personal Google Accounts of anyone at risk of targeted attacks – like journalists, activists, business leaders, and political campaign teams

Advice From Twitter

Twitter has provided this advice with relation to their service, this has been sent to some political groups by Twitter. If your group didn't recive the advice, contact Twitter directly or CSIRT-IE can provide their contacts .

Political Advertising As you may have seen, we recently announced a change in policy political advertising. Twitter now prohibits the promotion of political content.

We define political content as content that references a candidate, political party, elected or appointed government official, election, referendum, legislation, regulation, directive, or judicial outcome.

For practical purposes, this means that political parties and candidates will not be able to engage in promoted campaigning on Twitter during the election. You can read more here and see the FAQ here.

Verification: For your awareness, in accordance with the Twitter Terms of Service, Twitter may remove the verified badge and verified status of a Twitter account at any time. A verified account may also lose its verified status if changes to the profile settings modify the account's original purpose. Twitter reserves the right to remove verification at any time without notice. Further information is available here.

Resources: Campaigns on Twitter can be highly participative and impactful. To help you make the most of this unique platform, we've created a best practice handbook for political organisations, NGOs, and anyone involved in public service. Please find it linked here .

Reporting: Reporting in-app or via the Help Center is the most efficient way to flag potential violations of the Twitter Rules - you can find more information on the reporting process here. The Partner Support Portal is a dedicated reporting pathway in the Help Center that provides escalated support to onboarded accounts. The Portal is available to political party administrators who can report on behalf of both institutional and candidate accounts. Contact certreport@decc.gov.ie for the contact point in Twitter.

Advice From Microsoft

Microsoft runs its Defending Democracy program using its product Accountguard. This "...provides prescriptive best-practice security guidance to enable identification and notification of incidents related to your organization." This project is available to civic society organisations, that use Microsoft Exchange365, which is their cloud email service. Contact accountguard@microsoft.com for details.

Feedback and Reporting

NCSC and CSIRT kindly requests any feedback users may wish to provide in relation to this advisory as regards the relevance and accuracy of the information provided. Feedback can be provided by emailing info@ncsc.gov.ie or certreport@decc.gov.ie.

DISCLAIMER: *This document is provided "as is" without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.*

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@decc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie