ADVISORY ON CYBERSECURITY FOR ELECTIONS IN SINGAPORE

Introduction

Election campaigns were traditionally conducted physically. As the world rapidly digitalised, election campaign activities are increasingly being conducted online or in hybrid format. While the transition online has made it more convenient for election candidates and political parties while increasing the reach to the voters, the IT systems underpinning such activities are susceptible to cyber-attacks.

Examples of online campaign activities range from holding online rallies on social media platforms like Facebook to organising Q&A sessions on video conference platforms such as Zoom. To ensure that all online campaign activities are protected from cyber threats, election candidates and political parties should take appropriate precautionary measures to protect their digital assets. These assets include smartphones, computers, storage devices and online websites and accounts.

The purpose of this advisory is to provide election candidates and political parties with information on potential cyber threats to their activities and the preventive measures they can take to mitigate the risk of cyber incidents disrupting their activities.

Potential Cyber Threats

There have been reports from several countries of cyber-attacks that use a variety of techniques to target political parties, elected parliamentarians and election candidates. These attacks may be part of a wider intent to influence voters, undermine public confidence in the election process or disrupt campaign efforts. Some potential cyber threats may include:

Data Theft / Breaches

A data breach occurs when a threat actor successfully infiltrates a data source and extracts sensitive information. These assets can be compromised via various attack vectors, including social engineering, exploitation of software vulnerabilities or malware infection. Data that was exfiltrated could be published or sold, potentially damaging the credibility or reputation of the party or candidate. If the stolen data included account credentials, the threat actor could also leverage that information to launch further attacks on related IT systems, which may disrupt campaign efforts.

Website Defacement

Website defacement takes place when a threat actor gains unauthorised access to a website and changes its visual appearance. The defacement may be performed on the homepage or the sub-pages. Disturbing or graphic images or messages expressing a certain point of view may be left on the website, potentially damaging the credibility or reputation of the party or candidate. The threat actor could also delete website content to disrupt access or publish misleading information that could affect the party or candidate’s reputation.

Distributed Denial of Service (DDoS)

A DDoS attack is a malicious attempt to make an online service unavailable to legitimate users by flooding the victim's network with traffic from various sources. Such attacks use multiple compromised internet-connected devices to exhaust the capacity of the victim's network to handle multiple requests or connections. This could result in potential voters being unable to access online services and information, and potentially undermining the effectiveness of campaigning by the party or candidate.

Ransomware

Ransomware is a type of malware designed to encrypt files stored in a compromised system until a ransom is paid. All affected (encrypted) files are not recoverable unless a decryption key is available. Some ransomware variants may also perform lateral movement to encrypt files stored in shared or network drives, including backups connected to the compromised network. There is no guarantee that victims will get the decryption key or recover their data after paying the ransom.

A ransomware attack is typically carried out via phishing emails that contain malicious attachments or links. Users' devices could get infected when they click on these attachments or links. It could also occur when unsuspecting victims unknowingly visit an infected website that downloads and installs the malware onto their device. The inability to access encrypted files may disrupt campaigning by the party or candidates.

Exploitation of Vulnerabilities

Vulnerabilities in IT systems refer to flaws in the code or design that creates a potential point of compromise for a computer or network. When successfully exploited, it can lead to unauthorised access to the IT system, allowing the threat actor to steal, modify, or delete data. This could potentially disrupt campaign activities.

Compromised/Fake Social Media Accounts

Threat actors could compromise social media accounts belonging to election candidates or political parties to spread misleading information. Impersonation accounts mimicking legitimate candidates or parties may also be created on various social media platforms for the same purpose. Where possible, candidates are advised to get their social media accounts verified.

Insider Threats

Insider threats refer to threats that come from someone inside the organisation who has authorised access to a network. He may wittingly or unwittingly use such access to harm the network. A malicious insider within an election campaign may intentionally steal sensitive information or degrade the network's security to allow unauthorised access from external sources. Data that may be exfiltrated as a result could potentially damage the reputation or credibility of the party or candidate.

Social Engineering

Social engineering is a manipulation technique that exploits human error to gain confidential information, access, or valuables. There are several types of social engineering attacks, including phishing, vishing, or baiting. All these types of attacks rely on human errors to successfully attain information, gain access, or reap monetary gains. Successful exfiltration of data could potentially damage the credibility or reputation of the party or candidate.

Precautionary Measures for Election Candidates and Political Parties

Various IT equipment and systems may be used to support election candidates or political parties' campaigns. The use of such technologies may introduce potential cyber threats highlighted in the previous section. Election candidates and political parties need to be responsible for their own cybersecurity and are advised to take precautionary measures to safeguard their digital assets.

Election candidates and political parties should appoint a responsible person to take charge of their campaign's cybersecurity matters. Due consideration should also be placed on engaging a cybersecurity vendor to review and manage the cybersecurity posture of the election campaign systems as well as to respond to any cybersecurity incident.

Some precautionary measures that can be implemented by election candidates and political parties to safeguard their cybersecurity are provided below. Please note that the measures provided are not exhaustive.

Establish Strict Access Control

- Perform a stock take of all digital assets owned and used by the election campaign. For example, there should be clear awareness of what, where and how data is stored in each device.

- Institute strict control over administrator and remote access privileges to digital assets. The principle of least privileges should be followed as much as possible.

- Establish a whitelist of applications that are allowed to run on device(s) used for campaign purposes especially those containing or processing sensitive data. All other applications should be disallowed.

Enforce Strong Password Management

- Institute minimum password lengths and complexities for campaign and campaign-related accounts. A strong password would generally comprise at least 12 characters with a mix of upper- and lower-case letters, numbers, and special characters.

- Implement multi-factor authentication (MFA) to further secure online accounts.

- Raise awareness amongst account holders on safeguarding account credentials (e.g. do not share the credentials with anyone and do not write the password down on paper).

Perform Regular Software Updates

- Firmware and software should always be updated promptly to protect campaign devices from known vulnerabilities.

- Set automatic updates where feasible.

Regularly Backup Important Data

- Regularly backup important data on devices to ensure data integrity and availability in the event of a cybersecurity incident such as ransomware. Backups should be stored disconnected from the organisation's network and kept offline, so as to prevent threat actors from being able to compromise both the primary system as well as the backup system in the same attack.

Raise Cybersecurity Awareness Amongst Campaign Staff

- Educate campaign staff on common cybersecurity threats such as phishing.

- Remind them that they should practice good cyber hygiene and implement preventive measures.

- Establish clear lines of communication for incident reporting. Campaign staff should also be encouraged to report near-miss incidents.

- Train campaign staff to spot signs of compromise (e.g. not able to login using original password, receiving a ransom message, sudden presence of unknown applications installed in device, or inexplicable activities detected on their device(s)).

Develop Cybersecurity Monitoring and Incident Response Capabilities

- Establish cybersecurity monitoring capabilities to detect breaches or breach attempts. Such capabilities can take the form of installed technologies such as Endpoint Detection and Response (EDR).

- Perform regular security assessments on election campaign related websites using reputable tools such as SSL Labs, MxToolbox, or the Cyber Security Agency of Singapore's Internet Hygiene Portal to identify possible flaws for remediation.

- Enable loggings of network traffic and security events. Logs should be retained for a suitable period (e.g. 6 months) to facilitate any investigations in the event of a cybersecurity incident.

- Develop an incident response and management plan to ensure that all stakeholders know their role. The following checklist developed by SingCERT may be useful when developing an incident response plan for your campaign: https://www.csa.gov.sg/Tips-Resources/Resources/singcert/Incident-Response-Checklist.

Steps to Take in the Event of a (Suspected) Cybersecurity Incident

If election candidates, political parties or campaign staff suspect that a cybersecurity incident may have occurred, they should:

- Lodge a police report immediately, and keep the Elections Department (ELD) informed.

To respond to the incident:

- Contact the relevant email and social media platform providers for issues related to your email or social media accounts. For immediate self-help, please refer to the section Useful Links for Email Providers and Social Media Platforms.

Contact your appointed cybersecurity vendor if there is a compromise in your IT system. A non-exhaustive list of cybersecurity vendors is provided under the section Cybersecurity Service Providers. For immediate self-help, you may also wish to visit https://www.csa.gov.sg/cyber-aid.

Additional Resources

For additional information on the potential cyber threats mentioned in this advisory and other references on cybersecurity tips and good practices, please refer to section Useful References.

For clarifications on the advisory, please send an email to SingCERT at singcert@csa.gov.sg

Useful Links for Email Providers and Social Media Platforms

The following table provides account retrieval details for popular email providers:

Email Provider	Email Contact
Gmail	**Compromised Account** https://support.google.com/accounts/answer/6294825
Outlook or Hotmail	**Compromised Account** https://support.microsoft.com/en-hk/help/10494/microsoft-account-how-to-access-a-compromised-account

The following table provides details for account verification, and account retrieval and impersonation profile reporting for popular social media platforms:

Social Media Platform	Contact Information
Facebook	**Verify Account** https://www.facebook.com/help/1288173394636262 **Compromised Account** https://www.facebook.com/hacked **Impersonation Account** https://www.facebook.com/help/174210519303259/
Twitter	**Verify Account** https://help.twitter.com/en/managing-your-account/about-twitter-verified-accounts **Compromised Account** https://help.twitter.com/en/safety-and-security/twitter-account-compromised **Impersonation Account** https://help.twitter.com/forms/impersonation
Instagram	**Verify Account** https://help.instagram.com/854227311295302 **Compromised Account** https://help.instagram.com/368191326593075 **Impersonation Account** https://help.instagram.com/446663175382270
YouTube	**Verify Account** https://support.google.com/youtube/answer/3046484?hl=en **Compromised Account** https://support.google.com/youtube/answer/76187?hl=en **Impersonation Account** https://support.google.com/youtube/answer/2801947?hl=en
LinkedIn	**Compromised Account** https://www.linkedin.com/help/linkedin/answer/56363/reporting-a-hacked-account?lang=en **Impersonation Account** https://safety.linkedin.com/identifying-abuse#profiles
Snapchat	**Compromised Account** https://support.snapchat.com/en-US/a/hacked-howto

	Impersonation Account https://support.snapchat.com/en-US/i-need-help
TikTok	**Verify Account** https://support.tiktok.com/en/using-tiktok/growing-your-audience/how-to-tell-if-an-account-is-verified-on-tiktok **Compromised Account** https://support.tiktok.com/en/log-in-troubleshoot/log-in/my-account-has-been-hacked **Impersonation Account** https://support.tiktok.com/en/safety-hc/report-a-problem/report-a-user
WhatsApp	**Compromised Account** https://faq.whatsapp.com/1131652977717250

Cybersecurity Service Providers

To review and manage your campaign's cybersecurity posture or to seek incident response services, you can refer to the following link for CREST-accredited incident response companies with a presence in Singapore:

https://www.crest-approved.org/members/?filter_accredited_services_10717=Cyber%20Security%20Incident%20Response&filter_offices_10717=Singapore

Useful References

For more information on potential cyber threats to your campaign and possible preventive measures you can take to secure your IT systems, please visit the following websites:

Data Theft / Breach

- https://www.csa.gov.sg/alerts-advisories/Advisories/2020/AD-2020-009
- https://www.csa.gov.sg/Tips-Resources/publications/cybersense/2022/data-breaches

Social Engineering

- https://www.csa.gov.sg/Tips-Resources/publications/cybersense/2021/social-engineering-attacks
- https://www.csa.gov.sg/Tips-Resources/gosafeonline/2021/spot-signs-of-phishing
- https://www.cisa.gov/phishing-infographic

- https://www.ncsc.gov.uk/guidance/phishing

Exploitation of Vulnerabilities

- https://owasp.org/www-community/vulnerabilities/
- https://www.malwarebytes.com/blog/business/2022/09/6-patch-management-best-practices-for-businesses

Website Defacement

- https://www.csa.gov.sg/alerts-advisories/Advisories/2022/AD-2022-007
- https://www.cisa.gov/tips/st18-006
- https://www.cisa.gov/uscert/ncas/tips/ST18-006
- https://cyberexperts.com/website-security-practices/

Distributed Denial of Service (DDoS)

- https://www.csa.gov.sg/Tips-Resources/gosafeonline/2014/Distributed-Denial-of-Service-Attack
- https://www.csa.gov.sg/docs/default-source/publications/singcert/pdfs/playbook-for-ddos.pdf?sfvrsn=71bdb38d_1
- https://www.cisa.gov/uscert/ncas/current-activity/2022/10/28/joint-cisa-fbi-ms-isac-guide-responding-ddos-attacks-and-ddos
- https://blogs.blackberry.com/en/2022/11/ddos-attack-8-simple-prevention-and-mitigation-strategies

Ransomware

- https://www.csa.gov.sg/alerts-advisories/Advisories/2021/AD-2021-006
- https://www.csa.gov.sg/alerts-advisories/Advisories/2021/AD-2021-009
- https://www.csa.gov.sg/docs/default-source/publications/singcert/pdfs/ransomware-response-checklist.pdf?sfvrsn=6c852e82_1
- https://www.cisa.gov/publication/protecting-sensitive-and-personal-information

- https://www.nomoreransom.org/en/index.html

Insider Threats

- https://www.ncsc.gov.uk/guidance/reducing-data-exfiltration-by-malicious-insiders

- https://www.cisa.gov/defining-insider-threats

- https://securityintelligence.com/posts/what-are-insider-threats-and-how-can-you-mitigate-them

Incident Response

- https://www.csa.gov.sg/Tips-Resources/Resources/singcert/Incident-Response-Checklist

- https://www.csa.gov.sg/Tips-Resources/Resources/singcert/incident-response-playooks

- https://ihp.csa.gov.sg

- https://www.ncsc.gov.uk/collection/incident-management

ISSUED BY

CYBER SECURITY AGENCY OF SINGAPORE

ELECTIONS DEPARTMENT SINGAPORE

31 JUL 2023