Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

CYBER SECURITY GUIDE
FOR CAMPAIGN TEAMS

CAMPAIGN TEAMS

Canada

TABLE OF CONTENTS

INTRODUCTION: WHY THIS GUIDE IS IMPORTANT TO YOUR CAMPAIGN PLANNING

Welcome to the Cyber Security Guide for Campaign Teams.

The Canadian Centre for Cyber Security prepared this guide to assist campaign teams across Canada in the lead up to elections at the federal, provincial, territorial, and municipal levels.

In 2017, and again in 2019, the Canadian Centre for Cyber Security advised Canadians that foreign actors are likely to try to interfere in Canadian election processes using cyber systems to target political candidates and campaigns.

So **if you're involved in politics – as a volunteer, paid staffer or candidate – you are more likely to be a target,** particularly in the lead-up to an election.

Consider the information it takes to run a campaign. You start with a campaign strategy and a plan. Your team will also have lists of donors, supporters, and registered voters, as well as research you may have commissioned.

The bottom line is that, as a member of a campaign team, **you hold valuable, strategic data that others want to access and that you need to protect**. The information systems and devices you use and run as part of your political campaign are an important part of the election process. For that reason, **you have to prioritize cyber security before, during, and after your campaign.**

The decision of where and how to invest in cyber security is based on your campaign's requirements. However, if you focus on these decisions before the heat of a campaign, you won't have to worry about it midway through when time is scarce and the pressure is on.

With this Cyber Security Guide for Campaign Teams, we've outlined practical advice and guidance about cyber security that is applicable to all campaigns. It will help your campaign team's thinking about cyber security related to your candidate, your strategies, your data, and your technology. By following this guide, you will help protect your campaign from cyber security compromises and the accompanying consequences.

The Cyber Centre is pleased to work with you, through this Campaign Guide, to help you have a cyber safe campaign.

BEFORE WE START… SOMETHING FOR EVERYONE

As a kickstart to your cyber security planning, here are important, practical measures you and every member of your campaign team can take right now on any device to make your campaign more secure. Read more about these measures later in this guide or visit **www.cyber.gc.ca** for more on any of these steps.

Practice good password etiquette (page 9)

- Use unique passphrases or complex passwords.
- Don't share passwords. Don't use the same password for multiple accounts, websites, or devices.
- Use two-factor authentication (2FA) when available. (page 10)

Apply updates to your mobile devices, computers, and applications.

- Those updates are crucial to your security: they contain what we call security "patches". Don't ignore them.
- Be sure to apply updates to your mobile applications in addition to your device operating systems and get them to automatically update.
- Schedule a mandatory training session in which all campaign members update their devices and applications.

Secure your social media accounts (page 12)

- Use as many security options (settings) as you can for each social media platform.
- Know your options for delegating authority (what to do when you need multiple users to access one account).

Be on guard for phishing and spear-phishing messages (page 14)

- Know how to spot phishing and spear-phishing messages.
- Be wary of suspicious links – don't click on them.
- Use anti-virus or anti-malware software on computers.

Store your data securely and know your back-up procedures (page 16)

- Use only new USB memory sticks purchased by the campaign team. Use them for campaign-related work only. Do not use them on untrusted computers. (page 16)
- Secure data stored in the cloud or online by turning on the available security features. Consider storage solutions with restricted access. (page 14)
- Backup your vital campaign information and know where you have it backed up.
- Practice recovering your data at least once. This way you'll know what to do if you become a ransomware victim.

STEP 1: ASSESS WHAT CYBER SECURITY MEANS FOR YOUR CAMPAIGN

The data your campaign team holds and the technology you use during the campaign are unique to your campaign, so you need to have a strong understanding of what you're protecting. The planning chart on page 6 shows you how to take the next steps. But we'll start with the creation of three important lists.

DATA: First, create a list of the data your team will be relying on during the campaign. Email? Strategies? Plans? Lists? Photos? Videos? Research? It's important to itemize each data set or document, because you need to know what to do with it and how to protect it.

TECHNOLOGY: Next, consider what technology and devices your team will use during the campaign. Will the candidate have his or her own device? Who on the campaign gets a smart phone? Are volunteers using their own devices? Do you have to consider laptops, desktops or tablets?

PLATFORMS: Now, think about the communication platforms your team will use. It's likely your team will establish email addresses for the campaign. You will also likely use social media during the campaign, so make sure you itemize which social media platforms you've chosen. Identify the applications (apps) you expect to use, such as chat apps or messaging apps. Consider file sharing networks and video or photo databases. Make sure you list them all.

With these three lists, you're ready to move on.

Next, think about how your team will share—or won't share—your campaign data. For instance, you will not share your campaign budget with every volunteer, but communications volunteers might require access to your social media plan.

- Decide on and communicate about whom on your campaign team needs access to what information. In order to make your campaign secure, be clear on the access privileges that an individual will have.
- Determine what happens when you add to or change those lists during the campaign. What new information or technology do you expect to obtain, create or receive during the campaign? A new stump speech? New video clips? New polling data? A brand new laptop or mini-recorder? Adding items during a campaign will be easier if you've thought about them at the start. It will also be clear to the campaign team who should have access to new information or technology if you've established that up front.
- Establish and communicate policies and standards. For example, your volunteers will be eager to help, but if you don't make it clear to them that they aren't permitted to copy voter lists to their devices, your campaign risks a security breach.
- Consider how your campaign team will receive training on cyber security. You may have specific messages for team members to use as they knock on doors, but do they know what to do if they want to use a thumb drive on a laptop in the campaign office? Is it clear to them what to do if they receive links in emails?

As you establish your campaign team, you should also establish a culture of cyber security. Set clear expectations at the start, and you reduce the risks of cyber breaches throughout the campaign.

If you'd like to read more about the cyber threats within Canada and have a broader contextual knowledge of the cyber threats you could face, take a look at the Communications Security Establishment's ***Cyber Threats to Canada's Democratic Processes*** report from 2017 and the **update from 2019**, as well as the Canadian Centre for Cyber Security's ***National Cyber Threat Assessment*** released in late 2018.

EXAMPLE OF A PLANNING CHART

DATA OR TECH	PERMITTED ACCESS	STORAGE	SECURITY	DISPOSE/ARCHIVE
Campaign Strategy	• Candidate • Campaign Manager • Finance Officer	• Cloud provider	• Create access control lists for individuals in permitted access column	• Send to riding association office • Delete from all other storage
Social Media Plan	• Candidate • Campaign Manager • Communications Manager • Social Media Lead • Social Media Volunteers	• Network folder • Dedicated Communications device	• Create access control lists for individuals in permitted access column	• Send to riding association office • Delete from all other devices
Donor List	• Candidate • Campaign Manager • Donor Coordinator • Finance Officer	• Campaign leadership devices	• Create access control lists for individuals in permitted access column	• Send to riding association office • Delete from all other devices
Voter List	• Campaign Manager • Voter Coordinator	• Network folder	• Create access control lists for individuals in permitted access column	• Return to Party Headquarters • Destroy local copies
Campaign devices	• As designated by the campaign leadership	• With designated volunteers • In campaign office	• Control access to devices, configure security settings, and apply all required updates	• Remove all content • Wipe Devices
Volunteers devices (BYOD situation)	• Volunteer, allowed by campaign leadership	• Kept with volunteers • Not stored in campaign office	• Configure security settings on device and update during training sessions.	• Encourage the removal of all campaign documents. • Change access permissions for volunteers (change passwords, remove access to networks etc.)

STEP 2: UNDERSTAND WHERE YOUR DATA LIVES

In order to protect your data and documents, you need to know where you're storing them. You'll want to keep a few things in mind as you consider this.

We recommend applying security based on your risk tolerance and budget. You may choose to hire an IT service professional or company to manage the set-up of your IT networks. For some campaigns, this could mean contracting with a managed service provider to **store your data in a cloud solution.** Cloud storage solutions specifically designed for election campaign use are available in Canada. **We recommend this option.** They move some of the data-protection risk from your campaign team to professional services. But not all cloud services are equal. Take a look at page 14 for advice on how to evaluate and choose cloud services.

For campaigns that do not choose to use a cloud solution, other IT set-ups are available. You might elect to establish a server or network file-sharing option. Or have all files saved on a limited number of devices. You may choose a combination of both cloud and local file sharing. No matter what storage solution you chose, you will use the same cyber security principles for determining access to, and protection of, your campaign information.

The decision about how you access your information when you need it will likely play into how you conduct your campaign. Consider how access to the documents you've identified as critical for the campaign will meet the objectives of the campaign. How will you conduct your day-to-day business? Do you need to share the latest party messages on a daily basis? With whom? Should they be stored on a shared drive or on one specific communications device? Will you share updated strategies often and should you store them in the cloud?

To complete this assessment of where to store your data, you need to have a clear understanding of who has responsibility for what function on your team. Does this affect where your data is stored?

RISK TOLERANCE

As we mentioned earlier in this document, each campaign's needs are unique, as is your risk tolerance. Understanding your risk tolerance can help you make decisions about how you will secure your data and technology.

Risk tolerance is about making reasonable judgements about what could happen and what the result might be. What are you willing to lose, and what cannot be lost, at any cost? Determining risk tolerance should begin with a risk management meeting with your campaign team to review potential risk scenarios for your IT security and other elements of your campaign.

Take a look at lessons learned from previous campaigns and consider how issues have changed since that time. Consider the evolution in technology and the communications practices that exist today.

STEP 3: SECURE YOUR DATA AND TECHNOLOGY

The best approach to cyber security is to think about layers. Each cyber security action you take adds a layer of protection to your campaign.

The next pages walk you through specific cyber security tools and actions you should be using now, both in a campaign office and out on the campaign trail, because any piece of technology can be an attractive target during a campaign. The advice is grouped in four sections: **Devices, Social Media and Messaging, Data and Networks, and Physical Spaces.**

DEVICES

Your campaign team and candidate will certainly use mobile devices extensively, and these are attractive targets to threat actors. Lost, stolen, or compromised devices give threat actors unauthorized access to your network, and put work-related and personal information at risk. Secure the devices you use with the following measures:

- Lock all mobile devices with a strong password, PIN, or biometric (see password section, page 9).
- Apply operating system and application updates as they become available. This includes third-party apps as they may provide a conduit into social media accounts such as Twitter and Facebook. Always accept the updates when prompted because they often provide important security patches.
- Use an anti-virus application on your desktops, laptops and mobile devices.
- Do not use “Remember Me” features which store your ID and password on websites and mobile applications.
- Back-up your mobile device regularly.
- Turn off or disable features such as location services, Bluetooth, or Wi-Fi when you’re not using them.
- Be wary of connecting your devices to unsecured or free Wi-Fi networks. Use a data plan with a reputable carrier instead of using free Wi-Fi. (see the Wi-Fi Security section, page 15).
- Use a power receptacle, like a portable battery pack, to charge your device instead of a USB port on a computer or in a free charging station. Using unknown USB power charging stations is not recommended because, not only can they charge your device, information can be transmitted to and from the device.
- Do not connect devices that you suspect are compromised to your PC or any other networked computer, especially if you only need to charge the device. Connecting compromised devices can infect the entire network. If you suspect your device is compromised, give it to your campaign team or IT professional for review.
- Do not leave your devices unattended in public places.
- Restrict others—even family members—from using your mobile devices.
- Avoid jailbreaking (modifying the phone to install unauthorized software) or trying to remove the security measures imposed by the device manufacturer.
- Do not install applications on your work devices without understanding the relevant campaign policies.
- Review the privacy policies and the access requirements (e.g. access to camera, microphone, calendar, location services) of approved applications before installing them on your mobile devices.
- Be aware of your surroundings when using devices, especially when entering passwords or sharing sensitive information.
- Take note of any odd device behaviour (e.g. rapid battery drainage or strange texts/emails) as it may indicate a compromise.

PASSWORDS AND PASSPHRASES

Passwords control access to your mobile devices, social media accounts, and email accounts. A weak or compromised password could lead to stolen campaign data. We recommend that you **use passphrases** that are longer and easier to remember than passwords. However, websites, applications, and services are all set up differently. You may have to follow the password creation rules of the website, application, or service that you're using. If you're able to use a passphrase, do so—otherwise be sure to use a strong password.

PASSPHRASES	PASSWORDS	PASSCODE
A memorized phrase consisting of a sequence of mixed words or other text. Use passphrases whenever you are able. (e.g. "closet lamp bathroom painting")	A string of characters used to gain access to sensitive data or devices. (e.g. Mj#wlpcsw27!)	Short codes made up of numbers. (e.g.385462).

For either passwords or passphrases, consider the following:

- Do not include common expressions, song titles or lyrics, movie titles, quotes etc. Keep the words random.
- Consider including words from different languages.
- Change only when there is a good reason to do so (e.g. a suspected or a known compromise).
- Do not use the same password on multiple accounts or devices.
- Do not change a password or passphrase by simply changing the number at the end of it (e.g. falsehousebookspeed1 to falsehousebookspeed2).

For passphrases:

- Choose four random words to create a passphrase that is at least 15 lowercase letters long.
- Use association techniques like scanning a room in your home, such as your bedroom and select "closet lamp bathroom painting".
- Do not use the names of your kids or members of your favourite sports teams. These could be easily guessed by a threat actor watching your social media.

For passwords:

- Use a minimum of 12 characters for complex passwords (if the creation rules allow for that length).
- Use a memorable phrase to help you remember a complex password (e.g. the phrase: "My jersey number when I played competitive soccer was 27!" could help you remember the password: "Mj#wlpcsw27!").
- Do not use something simple, like Password01, as a password.
  Do not simply substitute letters for numbers or symbols like Pa$$w0rd01.

For passcodes:

- Use passcodes only when you are specifically required to do so; otherwise use passphrases or passwords.
- Use randomly generated PINs where available.
- Avoid easily guessed combinations when choosing your PIN. (e.g. 1111, your birthday, your phone number).

TWO-FACTOR AUTHENTICATION (2FA)

Two-factor authentication (2FA) involves adding an additional factor beyond a username and password when you access an account to make it more secure. 2FA uses a combination of two different factors including something you know (e.g. a password), something you have (e.g. a token or a phone), or something you are (e.g. a biometric, like a fingerprint).

Because of the widespread nature of phishing attacks and password theft, many services, including most social media platforms, have added 2FA options. **We strongly recommend the use of 2FA** for these platforms, especially for important public-facing campaign accounts. Check with the service provider on how you can turn 2FA on.

For campaign office infrastructure that may allow remote access Virtual Private Networks (VPNs) and email services that give access to or contain sensitive campaign materials, campaigns should consider investing in 2FA infrastructure to provide the appropriate authentication to secure them. For systems containing sensitive campaign information, we recommend any 2FA solution over a password alone. Not all 2FA solutions are equal – but all 2FA solutions will improve your campaign's overall cyber security posture.

ENCRYPTION

Encryption converts readable information into unreadable cipher text to hide its content and prevent unauthorized access. Encryption can take place when your data is in transit (such as HTTPS web traffic) or at rest (such as the encrypted contents of a phone, laptop or computer hard drive). Encryption is the key mechanism to protect the security and privacy of campaign information in transit over the internet. It is also one of the primary ways to protect the contents of devices that may be lost or stolen during the campaign.

Most modern devices have options to encrypt your data. **We recommend turning encryption on where you can.** For example, on most mobile devices, setting a passcode to lock the device also encrypts the data it contains. Consult an IT professional to determine when you should encrypt memory cards, USB sticks, web sites, or any other means you use to store or transmit your campaign information.

CAMERA LENS COVERS

If you allow an app access to your camera and microphone, and threat actors access the app, they can access both the front and the back cameras, record you at any time an authorized app is in use, take pictures and videos without permission and upload them online instantly, and even livestream the camera to the internet.

- Consider using a camera lens cover on your phone and denying apps access to your phone camera. A camera lens cover is a thin mechanical privacy cover that you put over your device's camera. These covers can be purchased at electronic shops and allow easier access than covering with tape or other material.

SECURING DEVICES IN A BRING YOUR OWN DEVICE (BYOD) SCENARIO

If your campaign allows personal devices for official business use, remember that campaign staff and volunteers who leave the campaign may have sensitive information stored on their devices. Their personal devices may not have up-to-date software and security updates installed, which would leave sensitive information vulnerable. The sensitive information may not be encrypted on personal devices. Anyone using a personal device should:

- Follow BYOD policies to address expected behaviours and manage associated risks.
- Participate in cyber security training offered by the campaign. Campaigns should use training sessions to have all members update their cyber security measures.
- Request the installation of anti-virus software on their device, if they have not already been using it.

PHONE SPECIFIC THREATS

Most mobile and landline phone calls are not secure. Phones are susceptible to intrusion, and threat actors are able to monitor them with communication interception devices that mimic cell towers. **Consider having sensitive conversations in a private space away from electronic devices.** If this is not possible, be mindful of your phone's potential lack of security the next time you place a call.

If your campaign team holds or participates in regular teleconferences, consider changing the conference identification number on a scheduled basis. Consider who needs to have the call-in numbers and how those numbers are shared.

Bluetooth vulnerabilities

Threat actors can use Bluetooth vulnerabilities to steal your information. Hackers can exploit Bluetooth to gain complete control of your devices.

KNOWN BLUETOOTH ATTACKS

- **Bluejacking**—A threat actor sends unsolicited messages to your Bluetooth-enabled mobile devices. If you respond to the message or add the contact to your address book, you give the threat actor the opportunity to connect to your devices because you are establishing them as a known contact. Threat actors can then control your device remotely.
- **Bluebugging**—A threat actor poses as a device you're looking to connect to (e.g. headphones). You may not even realize that you are connecting to a spoofed device. Once connected, your device and your data are accessible as long as the spoofed device is in your list of paired devices.
- **Car Whisperer**—Car Whisperer software allows a threat actor to send or receive audio from the car kit installed in your vehicle. If exploited, threat actors could eavesdrop on your conversations by receiving audio from the car microphone.
- **Crackle**—A threat actor exploits flaws in the pairing process that allows key recovery so that your devices can be accessed.
- **GATTack**—An attacker creates a man-in-the-middle attack (i.e. secretly relays and can alter communications between sender and recipient) to intercept, clone, block, or change messages.

Bluetooth technology is continuing to evolve. New versions of Bluetooth have increased ranges and speeds, making data transfers easier and more convenient. The technology is changing, but you can protect your data and devices with a few simple actions:

- Turn off Bluetooth when you're not using it. On many devices you can find the option to turn off Bluetooth by swiping down on your home screen.
- Turn off discovery mode when you're not connecting devices.
- Avoid pairing devices in public spaces.
- Pair only with devices that you know and trust.
- Never transfer sensitive information over Bluetooth.
- Avoid using Bluetooth-enabled keyboards to enter sensitive information or passwords.
- Remove lost or stolen devices from your list of paired devices.
- Delete all stored data and devices from Bluetooth-enabled cars.

Voicemail

Threat actors can gain access to your voicemail and compromise your campaign. Since many voicemail PINs are only four digits long, intruders can easily guess or crack them. Use a voicemail PIN that is different from the factory setting default, and change it regularly. If possible, use a PIN longer than four digits for added security.

SOCIAL MEDIA AND MESSAGING

Activity on your campaign team's social media accounts impacts the public's perception of your campaign. If threat actors access your accounts, they can post sensitive or false information that discredits or embarrasses your candidate and puts your campaign at risk.

- Use strong and unique passwords (see password section on page 9) for each of your social media accounts to prevent all your accounts from being compromised in a single hack.
- Use two-factor authentication (2FA) when possible. (see 2FA section on page 10)
- Restrict access to social media platforms. Allow a limited number of campaign staff access to post or edit on social media channels.
- Know your options for delegating authority and approving content (what to do when you need multiple users accessing one account).

INSTANT MESSAGING AND TEXTING APPS

Instant messaging and chat apps are great for communicating quickly. Many use end-to-end encryption to secure conversations and offer features, like disappearing messages and identity confirmation, to maintain confidentiality. Be aware that conversations you assume are private can still be exposed. Exposure doesn't always come from a compromise of your application or the systems running the app. Despite a device's security settings or app encryption, an untrustworthy recipient can still take a screenshot of a conversation and post online. Take a moment to consider the sensitivities of your messages before you send them, regardless of your device's security.

SOCIAL ENGINEERING

Keep in mind that there's a human element to cyber security that could put you and your campaign at risk, even if you've taken all the technical steps to secure your networks and devices.

Social engineering relies on a threat actor's ability to exploit using technology. Rather than hacking into a system or account through technical means, a threat actor will try to manipulate the prospective victim. For example, a threat actor may claim to have a legitimate connection to you by pretending to be a constituent in your riding, a potential donor to your campaign, or a journalist. Threat actors may ask you to provide information (e.g. phone numbers or account information), open emails with attachments or visit specific websites – all for malicious purposes.

Social engineering tactics have a high success rate.

- Be suspicious of phone calls, visits, or emails from individuals asking about you, whom you know, and what you know.
- Verify who people are before giving them any information online. For example, if someone claims to be from a community organization or a media outlet, ask them to provide you with official identification.
- Never click on links. Instead, manually search for the web page in your browser.

MALWARE

Malicious software is designed to infiltrate or damage a computer system, without the owner's consent. Malware can come from software, email attachments, website downloads, links in texts, or infected media shared between users.

MALICIOUS MESSAGES INCLUDING EMAILS

Email may be your most common form of communication, and is therefore a highly attractive cyber target. Be aware that malicious emails, such as spam, phishing, and spear-phishing emails, could put you, your devices, and your information at risk. Malicious messages can also come through texts or apps.

Your campaign will likely receive messages, many by email, from organizations and members of the public that you may not know or have never worked with. Your campaign team needs to know how to sift out legitimate messages from malicious ones. At first glance, malicious messages may appear to be legitimate.

We recommend that you set up, with your email service provider, a DMARC (Domain-based Message Authentication, Reporting & Conformance) service. For example, DMARC services let you know if the emails you receive from Canada Revenue Agency (CRA) are actually sent from a CRA email account. This type of service effectively verifies that the domain, in this case CRA, is real.

Spam messages

Spam messages are any unsolicited electronic messages. Spam messages are often a source of scams or offensive content, and may contain malicious links that redirect you to an unsafe or fake website that contains malware or asks you to enter sensitive information (e.g. passwords). Spam may also contain malicious attachments that could infect your devices with malware.

Phishing and Spear Phishing

Phishing messages target a group of people by simulating a legitimate message from a trusted sender, such as an email or SMS (text message) from your political party or a community group in your riding. Phishing messages can include good news (e.g. someone is donating to your campaign) or include a threat (e.g. someone has information about you that they will release to the media). Either way, the aim of these messages is to get you to give up personal information or click on malicious links and attachments.

Spear-phishing messages are like phishing messages, but they are tailored to you based on your line of work, your interests, or personal characteristics. As someone openly working on a campaign, threat actors can easily gather information about you so that they can create a personalized spear-phishing message.

Phishing and spear-phishing messages target people like you. These messages appear to be legitimate; they may use real logos or familiar colours, layouts, and fonts, which make it difficult for you to see the threat. **Email phishing is the most common method that attackers use to spread ransomware and malware.**

See page 19 for advice on how to identify and handle malicious messages.

RANSOMWARE

Ransomware is a type of malware that threat actors use to deny a user's access to a system or data until a sum of money is paid. Even if the victim pays the ransom, the threat actors may continue to demand more money. If you are a victim, we recommend that you don't pay but your decision should be based on the assessment of your risk tolerance.

DATA AND NETWORKS

CLOUD SERVICES

Cloud services offer software, file storage, email services, remote access to documents and other services which may make your campaign team more productive. **We recommend that your campaign team work with a cloud service provider to set up the IT networks** that suit your specific needs.

Choose a reputable cloud service provider. Read reviews and get recommendations on reputable cloud service providers.

- Ask your cloud service provider where your data and backups physically reside. Cloud service providers frequently use facilities outside of Canada. These facilities are subject to the laws of their host country and may be subject to additional scrutiny by that country's security services.
- Confirm that the service provider uses anti-malware protection, software patching, encryption, and redundant (backup) power.
- Encrypt sensitive files in the cloud. Many cloud service providers offer file encryption by default.

WI-FI IN THE CAMPAIGN OFFICE

If your campaign chooses to establish a Wi-Fi network, use these technical measures to strengthen your Wi-Fi network.

- Change the default Wi-Fi network name and the router access password on your network router. The network name is the Service Set Identifier or SSID. You can usually make changes online by following the router manufacturer's instructions.
- Install software or hardware firewalls on your network and its devices (e.g. software firewall on laptops).
- Use Wi-Fi Protected Access 2 (WPA2-Enterprise) on your wireless router.
- Create a guest Wi-Fi access point to ensure your sensitive information cannot be accessed.
  To create the Wi-Fi access point there are two options:
  - Subscribe to a separate data line with your provider. This preferred option keeps your guest network and campaign network completely separate.
  - Use a router that has a separate guest network. This alternate option requires regular maintenanc, and does not totally remove the threat of a compromise from the guest account.
- Ensure that router firmware is up-to-date.
- Use hardware that is currently supported by a vendor and make sure to apply all security updates.
- Set up a VPN to allow staff to access campaign networks and systems remotely.

WI-FI OUTSIDE THE CAMPAIGN OFFICE

Instruct all staff and volunteers to **avoid using unsecured or free Wi-Fi**.

Unsecured or free Wi-Fi may be convenient, but it is relatively easy for anyone else on the network to eavesdrop (i.e. intercept communications or data). For instance, you may receive a common password at a local coffee shop, but that does not make the Wi-Fi network secure. It is very hard to protect phones or devices when they are connecting to an unsecured or free Wi-Fi hotspot. Threat actors can create “Sign-in for free Wi-Fi” fake web pages on the local network and add malware to that page. The malware will then spread easily and threat actors can gain complete control over your device, even with a password provided by a coffee shop.

- Ensure that all staff and volunteers use a data plan with a reputable carrier, especially when doing sensitive work. They should not connect to unsecured or free Wi-Fi networks.
- Make sure the Wi-Fi settings on your device do not automatically connect you to a network. Turn the “automatic connection” function off.
- Do not allow staff and volunteers to connect devices that connect to unsecured or free Wi-Fi to the sensitive IT resources used by your campaign. They should use a different device that has not connected to unsecured or free Wi-Fi.

If your staff or volunteers need to use unsecure or free Wi-Fi on their personal or campaign devices, they should not type any sensitive information while connected to that network. This includes passwords to social media accounts or login information for special sites.

You can use your own campaign-specific Virtual Private Networks (VPN) and anti-malware services to lessen the risk associated with using unsecure or free Wi-Fi. A VPN is a private communications network created over an often less-secure shared or public network. Organizations use VPNs as closed, restricted networks, allowing only authorized users access. VPN communications are typically encrypted or encoded to keep non-authorized users from accessing all data flowing over the public network. However, you should assume the devices and any data communicated over VPNs may be compromised.

- When looking to create or use a VPN, choose a commercial VPN appliance or cloud product that is purposely installed on your network. Be aware some commercial “VPN services” simply mask identities to increase privacy but do not enhance the security of your data.

BACKUPS AND RECOVERY OF DATA

You should have a plan for recovering from successful cyber attacks (e.g. ransomware, denial of service, defacing websites). Maintain backups of your information so you can recover from an attack or a lost or stolen device.

Steps 1 and 2 of this guide should have helped you identify the information and data that is critical to your campaign. An IT service provider or cloud service provider can help you ensure that the right information is backed up frequently and that you can quickly recover the backed up information in a timely manner.

PORTABLE DATA STORAGE DEVICES

You might store copies of your files on portable data storage devices, such as USB memory sticks (thumb drives), so that you can work from anywhere. If you don't protect portable storage devices and information properly, a threat actor can access and copy that information.

- Use only new USB memory sticks purchased by the campaign team.
- Use USB memory sticks for campaign-related work only. Do not use a campaign USB on a personal device, as malware may jump from one device to another.
- Do not connect untrusted USB memory sticks to your devices, as they may have preinstalled malware on them.
- Report a lost or stolen portable data storage device to your campaign team.
- Consider encrypting your portable data storage devices.

An untrusted USB memory stick may be one you receive at a conference or from someone else. Remember, if your campaign did not purchase it new, you should either throw it out or have it scanned for viruses and malware.

PHYSICAL SPACES

Not all volunteers or campaign staff need the same access to your office or devices. Set restrictions on who has physical access to equipment and facilities. Physical theft and equipment tampering should be a real concern as it relates to cyber security. You should consider the following security protocols for your physical spaces:

- Determine who has access to servers, laptops, or teleconference equipment.
- Limit knowledge of any physical combination locks your campaign uses.
- Keep a list of who needs and who possesses a key to the office, and determine who locks up at the end of the day.
- Decide how you lock or secure essential equipment so it doesn't go missing.

Establish device-free physical spaces to hold private discussions and forbid the use of devices in those spaces. If a device has been compromised, the microphone or camera may be turned on remotely and without your knowledge**. Keeping devices out of certain discussions is the only way to ensure those discussions stay private**.

STEP 4: PROVIDE CYBER SECURITY TRAINING

Most of the people on your campaign team will be familiar with technology, but they will likely not all have the same appreciation for cyber security and how their actions on their devices could affect the campaign.

Despite the best cyber security tools and measures, breaches still happen, and people are often the weak link. It is human nature to be curious about a document or link, but clicking on the link or opening the document could mean you get compromised.

Once you have a strong understanding of what data and technology you are working with, **you need to train everyone on proper cyber security awareness. Do not underestimate the value of good training.**

First, understand what volunteers need to know. You should have a clear idea of what role each person or group is taking on. This will determine what devices you permit individuals to use. Campaign members should know what you require of them.

Next, using this guide, establish procedures and policies for handling campaign data and technology. If you expect team leads to be the only ones to access files, you should make this clear. If only certain people can save or edit documents, that should also be clear.

A culture of cyber security can help keep your campaign secure. Campaign team members should reinforce the established procedures and policies established by living them. Shortcuts may seem easier, but they leave your campaign vulnerable. **Establish a practice that allows all campaign team members to admit when they have made a security error.** You want them to identify potential cyber security problems as soon as they occur so you can work to fix them before your campaign is compromised. If campaign members see something suspicious, they should report it.

Finally, run cyber security training sessions for all campaign team members. They should understand the impact of reusing passwords, clicking on unknown links, or using free Wi-Fi. Plan to present specific scenarios during the training and discuss the mitigating steps volunteers need to take if something goes wrong or they make a mistake.

STEP 5: KNOW WHAT TO DISPOSE OF OR ARCHIVE

The process of understanding what data and technology you will work with during a campaign (steps 1-3) leads you to this final step: What do you do after the campaign with the documents you've created and the devices you've used? Step 5 in this process shouldn't be too tough if you know what you're working with, hence the reasons steps 1-3 are important.

In terms of cyber security, **cleaning up after a campaign is as important as the start of a campaign.** Your campaign and candidate risk their reputations if you merely abandon documents in a cloud service or on a network server. Likewise, leaving files on a laptop makes you vulnerable to unauthorized access, depending on where the laptop goes after the campaign. Disposing of or archiving your data ensures you know who has control of it and eliminates the risk you face.

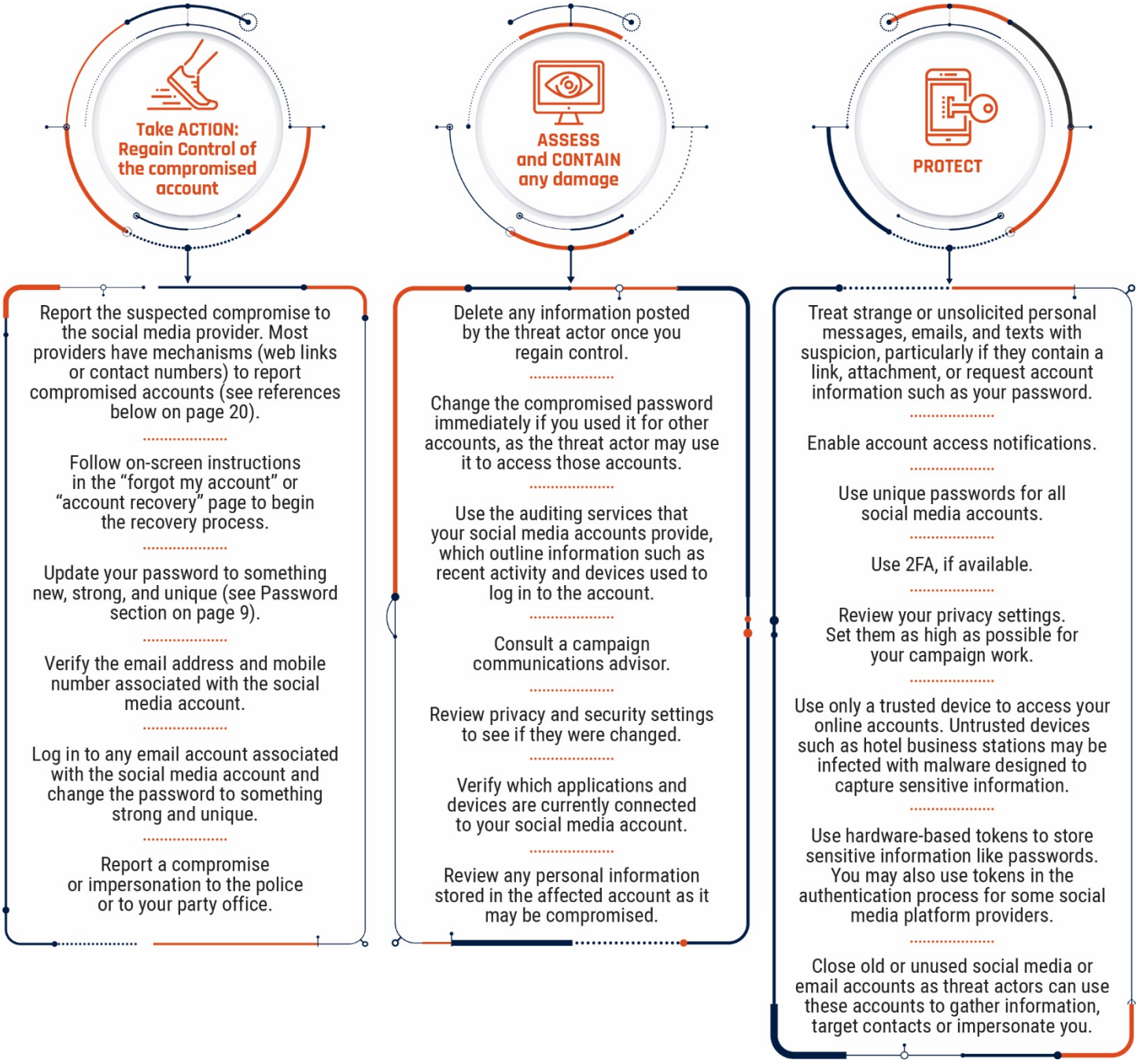
As you determine what you need to keep or dispose, you'll need to consider a few things. Your party or riding office may have directives about where campaign information goes, and the elections authority, such as Elections Canada, has requirements for the types of information that you must submit. You may also have legal requirements to keep or dispose of certain information. The requirements will be different for each level of election (municipal, provincial, territorial, federal).

Finally, keep in mind what data you or your party are going to need for the next election. At the end of a campaign it may not seem like a problem, but with a few planning steps, your secure data and information will be ready for you when you decide to jump back into the democratic process.

WHAT TO DO WHEN THINGS GO WRONG

LOSS OF CONTROL OF SOCIAL MEDIA CHANNELS

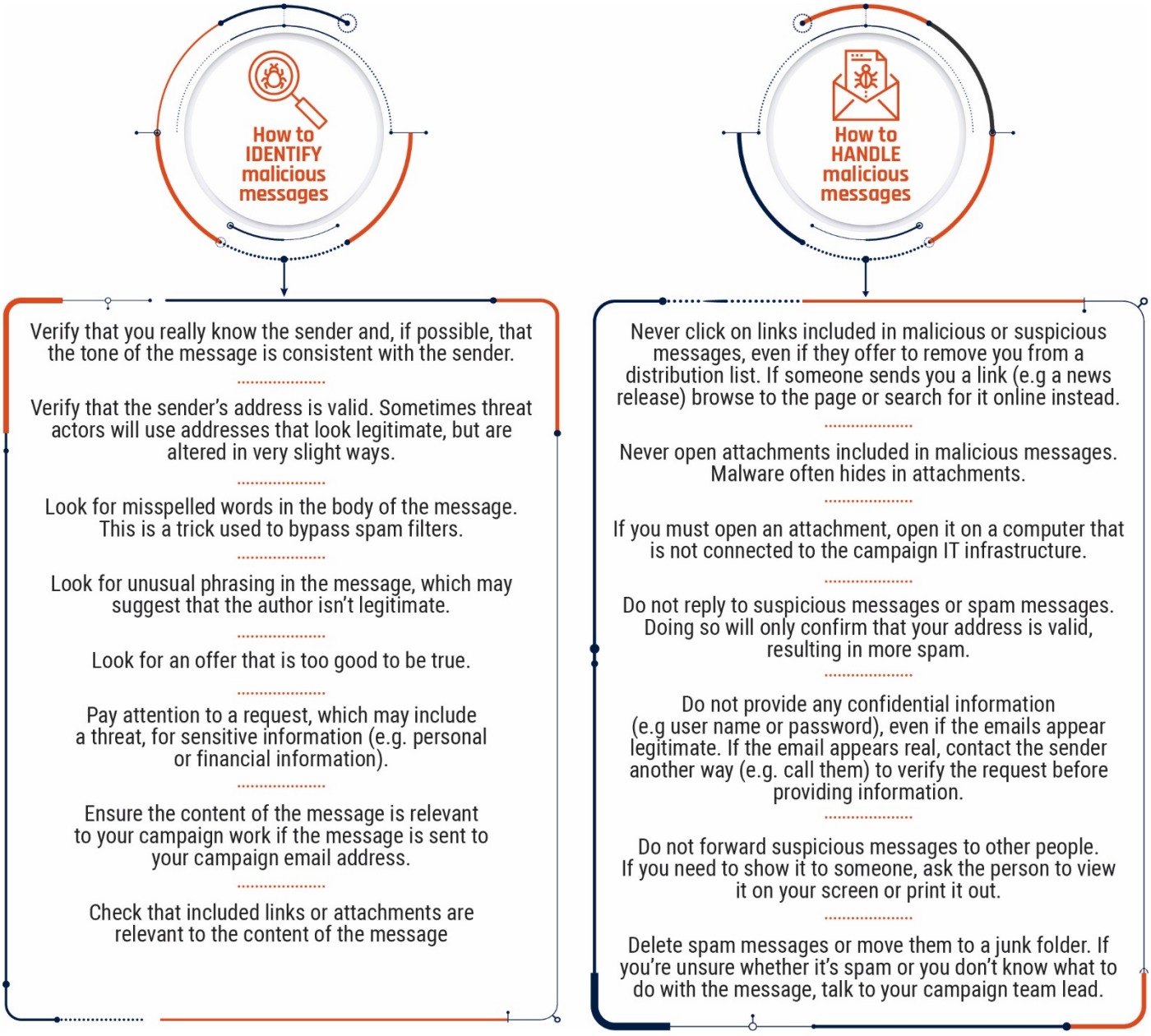
The results of an account compromise can be devastating. If one of your social media accounts are compromised: **take action, assess and contain, and protect.**



If you need to recover access to your social media, be aware that threat actors often use the recovery method to hijack account access. Any secondary account used for recovery, such as email, should be secured by a password that is not shared, and should be protected by 2FA. If the account recovery method uses personal questions, do not have answers that your social media pages easily provide.

IDENTIFY AND HANDLE MALICIOUS MESSAGES

All members of a campaign team should know how to identify malicious messages and how to handle them.



HOW TO HANDLE POTENTIALLY CRIMINAL MESSAGES OR CYBERCRIME

The Royal Canadian Mounted Police (RCMP) generally interprets cybercrime to be any crime where the internet and information technologies (such as computers, tablets, personal digital assistants, or mobile devices), have a substantial role in the commission of a criminal offence. It includes technically-advanced crimes that exploit vulnerabilities found in digital technologies. It also includes more traditional crimes that take on new shapes in cyberspace. If you receive an offensive, abusive, or potentially criminal message, whether it seems to be spam, phishing or something else, or if you think criminals are asking you for confidential information, inform your local police and the RCMP. Save the message, as authorities may ask you to provide a copy to help with any subsequent investigations. Do not send the message to others.

ADDITIONAL RESOURCES

Recovering Access to Social Media Accounts:

The following table provides some quick reference links to help you should your social media account be compromised.

Platform vendor	Compromised account resources	Impersonation account resources
Facebook	https://www.facebook.com/hacked	https://www.facebook.com/help/174210519303259/
Twitter	https://help.twitter.com/en/safety-and-security/twitter-account-hacked https://help.twitter.com/en/safety-and-security/twitter-account-compromised	https://help.twitter.com/forms/impersonation
Instagram	https://help.instagram.com/368191326593075	https://help.instagram.com/446663175382270
Youtube	https://support.google.com/youtube/answer/76187?hl=en	https://support.google.com/youtube/answer/2801947?hl=en
LinkedIn	https://www.linkedin.com/help/linkedin/answer/56363/reporting-a-hacked-account?lang=en	https://safety.linkedin.com/identifying-abuse#profiles
Snapchat	https://support.snapchat.com/en-US/a/hacked-howto https://support.snapchat.com/en-US/article/locked	https://support.snapchat.com/en-US/i-need-help

We all play a role in protecting Canada's cyber landscape. The following reports provide additional information on some of the cyber threats facing Canada today.

- **Cyber Threats to Canada's Democratic Process report 2017**
- **Update of the Cyber Threats to Canada's Democratic Process report 2019**
- **National Cyber Threat Assessment 2018**
- **An Introduction to the Cyber Threat Environment 2018**

NOTES