Cyber Hygiene Guide

Politicians and Political Parties

facebook

Canadian Election Integrity Initiative

Design by **ccm.design**

Cover Image by **Songquan Deng**

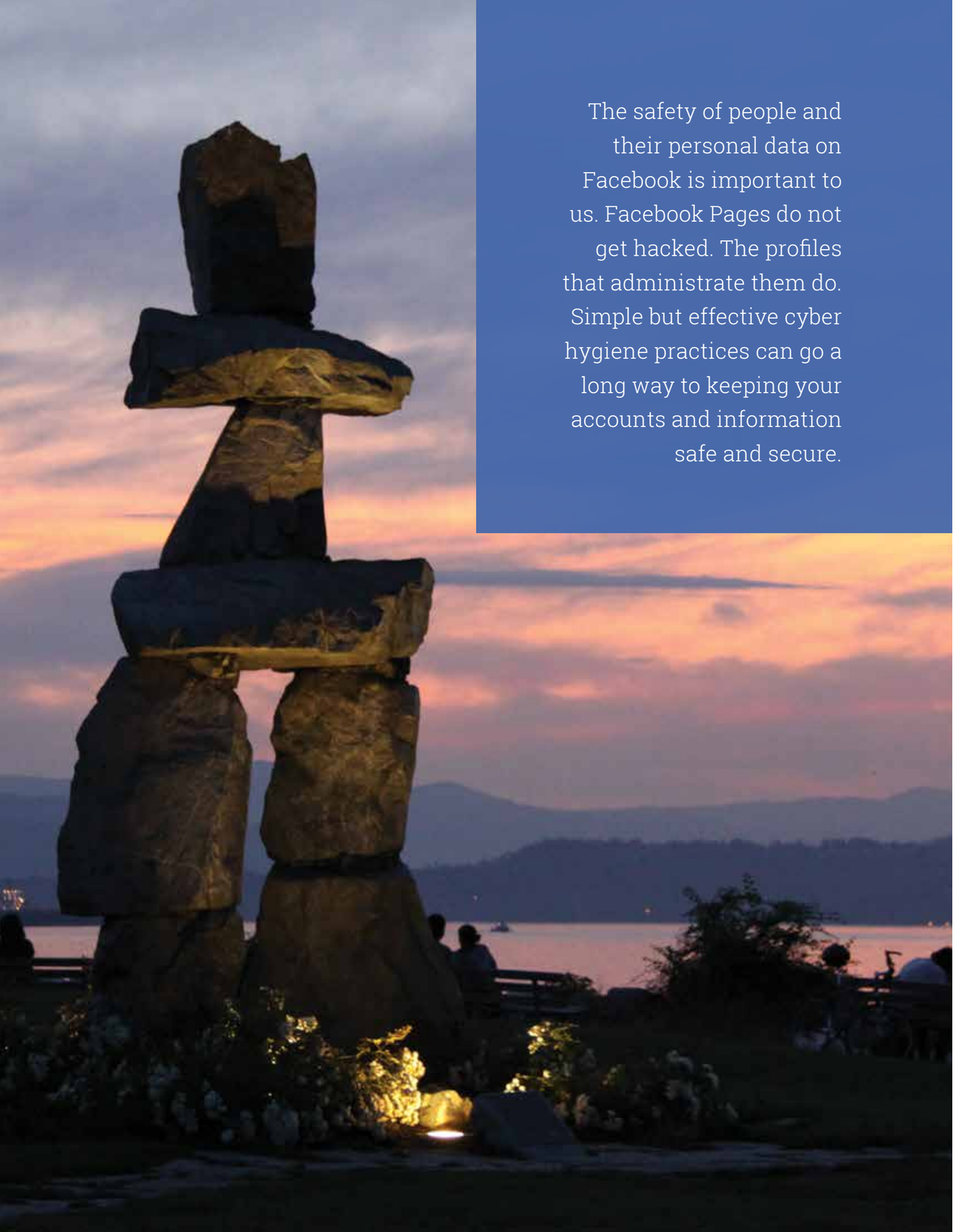
facebook

Helping to Safeguard the Integrity of the Electoral Process in Canada

In response to a request from the Minister of Democratic Institutions, the Communications Security Establishment (CSE) issued in June 2017 its *Cyber Threats to Canada's Democratic Process* report, which provided a rigorous cyber-threat assessment for various aspects of the democratic process. Facebook takes cyber threats very seriously, and is committed to doing our part to protect and safeguard the integrity of the electoral process in Canada.

This **Cyber Hygiene Guide** provides best practices for politicians and political parties on how to keep your Facebook Pages and Facebook accounts secure. We are also making available to politicians and political parties in Canada a special **Cyber Threats Crisis Email Line** for compromised Facebook Pages and accounts. These efforts are part of Facebook's broader Canadian Election Integrity Initiative.

Photo by Matt Thomason on Unsplash



The safety of people and their personal data on Facebook is important to us. Facebook Pages do not get hacked. The profiles that administrate them do. Simple but effective cyber hygiene practices can go a long way to keeping your accounts and information safe and secure.

The Important Safety Role of Page Admins

The following guide shares useful tips for protecting the Facebook Pages and accounts of political parties, politicians, official figures and the teams involved in managing their accounts.

Politicians and political parties can connect with citizens and voters on Facebook by creating a Facebook Page. Anyone with a Facebook account can create a Page or help manage one, as long as they have a role on the Page. People who like a Page can get updates about the Page, such as posts, photos or videos, in their News Feed.

The Pages belonging to political figures and institutions are often administrated by more than one person and therefore more than one Facebook account. That's why everyone involved should be aware of the importance of ensuring the security of their personal accounts. All security and privacy options should be activated for each administrator of a political account.

By Christina Chan

Protecting the Accounts of Page Admins

Protect Your Password and Account

Don't use your Facebook password anywhere else online, and never share your password. You should be the only one who knows it. Avoid using personally identifiable information that can be easily discovered such as your name, phone number, birthdate, mailing address, etc. **Your password should be difficult to guess.**

You will find login alerts in the Security section, under Settings. When you turn on login alerts, we'll send you an email or notification each time someone logs into your account from a new place.

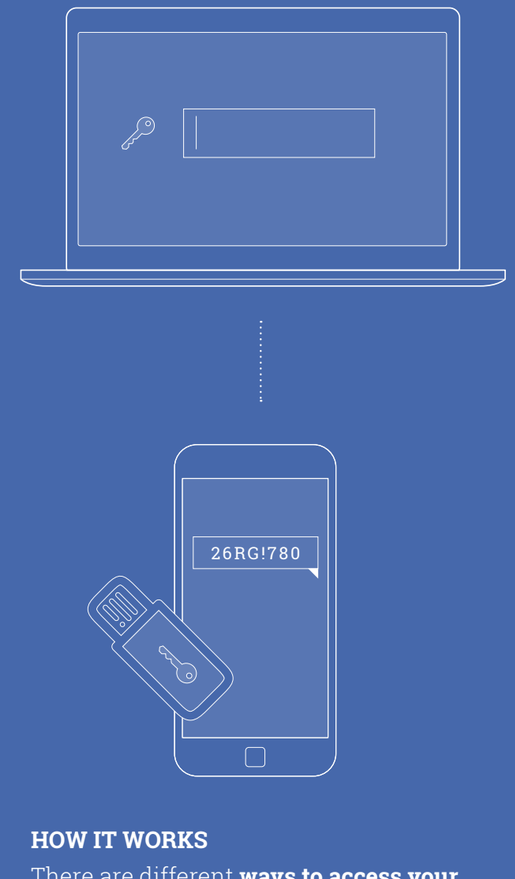
Use login alerts to get notifications if your account is being logged into from a new or different device.

Use login approvals as an extra security feature that can be used for two-factor authentication.

Logging Out of Your Account

The "Where You're Logged In" section of your "Security and Login" settings shows you a list of computers, phones and tablets that have been used recently to log in to your account.

To log out of Facebook on another computer, phone or tablet, go to your "Settings," then click on "Security and Login." In the "Where You're Logged In" section, find the session you want to end and click "Log Out."



Two-Factor Authentication

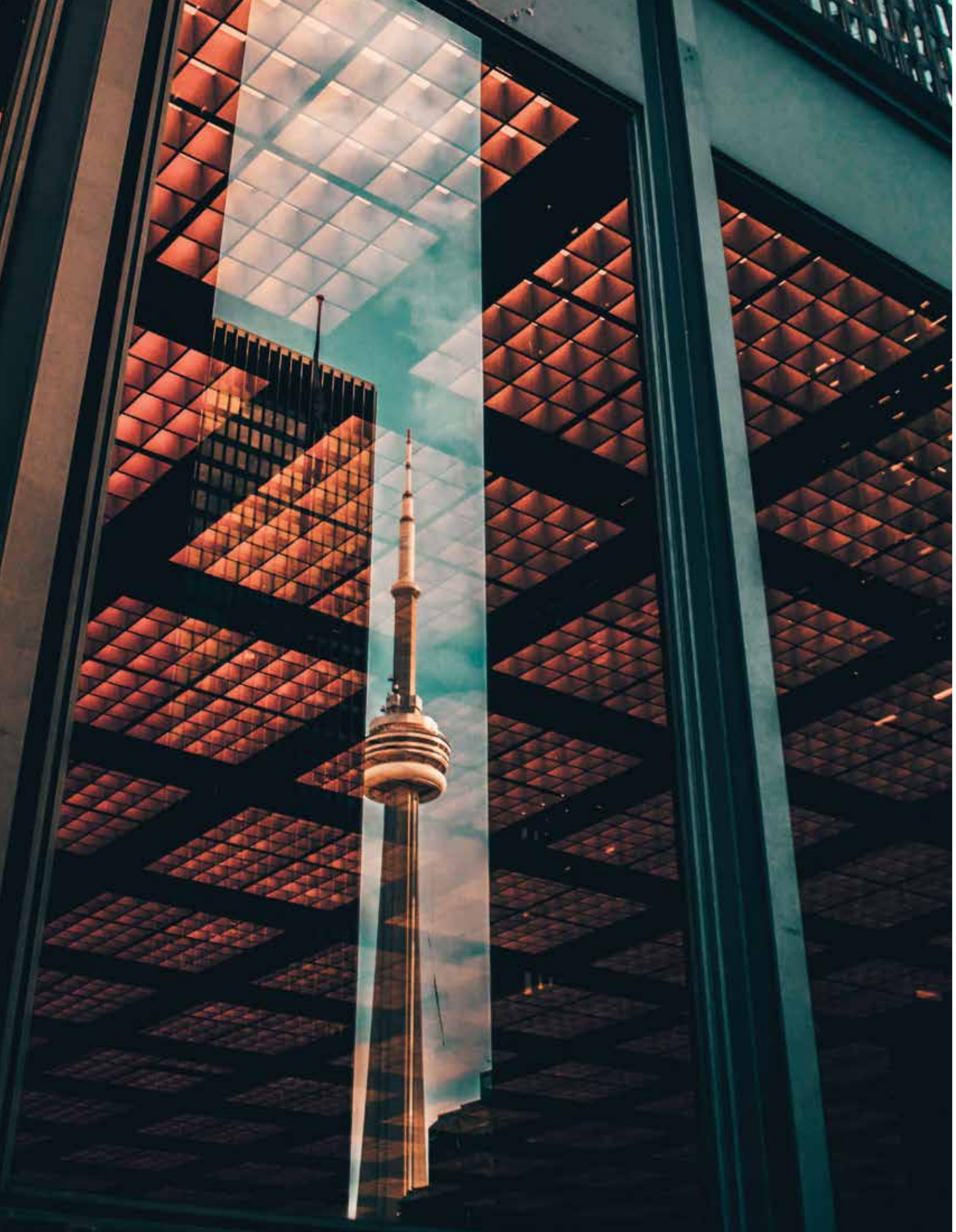
WHAT IS IT?
Two-factor authentication is a security feature that helps protect your Facebook account in addition to your password. If you set up two-factor authentication, you'll be asked to enter a special security code or confirm your login attempt each time someone tries accessing Facebook from a computer or mobile device we don't recognize. You can also get alerts when someone tries logging in from a computer we don't recognize.

To turn on or manage two-factor authentication:

1. Go to your Security and Login Settings by clicking in the top-right corner of Facebook and clicking **Settings > Security and Login.**
2. Scroll down to **Use two-factor authentication** and click **Edit**
3. Choose the authentication method you want to add and follow the on-screen instructions
4. Click **Enable** once you've selected and turned on an authentication method

HOW IT WORKS
There are different **ways to access your specific Security Code**:

1. Every time you need it, we send you an SMS with a login code;
2. You can ask for ten codes to print out, write down or save, so you have them when you need them;
3. You can use the Code Generator if you have the Facebook app installed on your smartphone or tablet.
4. You can use a Universal 2nd Factor **security key**



By Yeshi Kangrang on Unsplash

CYBER THREAT

TACTICS TO WATCH OUT FOR

t is helpful to familiarize yourself with the standard approaches generally used by those targeting elected officials, candidates and those associated with them. You can help protect your Facebook account by ensuring your email account and website are kept safe. Below are commonly used strategies and information to help minimize the risk of a compromised account.

Should your account be compromised, contact our Canadian Cyber Threats Crisis Email Line.

Spear Phishing

In spear phishing, bad actors send highly customized emails to specifically targeted individuals. These emails are intended to look like legitimate correspondence but often contain malicious links or documents. Examples of spear phishing include emails or messages indicating that a password reset is required for your email account. The email contains a shortened link which directs to a fake email login page. If you enter your information on this page, the hacker is able to acquire the information and access your account.

It's important to understand that your personal email, social media and other accounts are just as attractive as the accounts you use for your professional, government and official purposes. Exercise the same level of vigilance in protecting your personal accounts as you do with the accounts you use for official business.

Recommendation: If you receive an unexpected email or message prompting a password reset, don't click any links in the message. Instead, visit the sender's official website to check the legitimacy of the request.

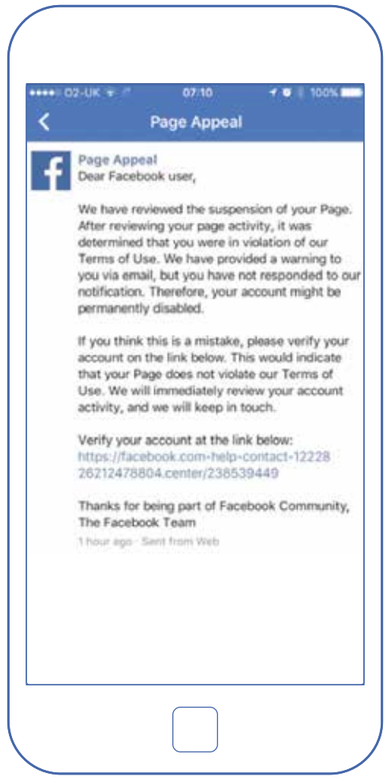
Facebook Branded Page Appeal Phishing

Sometimes phishing campaigns try to convince targeted users that their Facebook account or Page has been suspended, and the message may appear to be sent directly from Facebook. These campaigns are designed to collect your sensitive information with a link to a credential-harvesting domain. With access to your login credentials, hackers will be able to log in to your account and make changes to your settings that will ultimately prevent you from using the account altogether.

Facebook branded Page Appeal phishing attacks make illegitimate use of Facebook's branding to send messages— commonly via Messenger, increasing the impression that the notification is real and personalized.

Clicking the link in the message will compromise the account and locks users out of their accounts. Resolving this requires escalation to the Facebook Security team. Hackers using this method of phishing have developed ways to hide their activity from detection while retaining access to the targeted Facebook Page or account. These campaigns are financially motivated and tend to target influential Facebook Pages with high follower counts, making policymakers attractive targets.

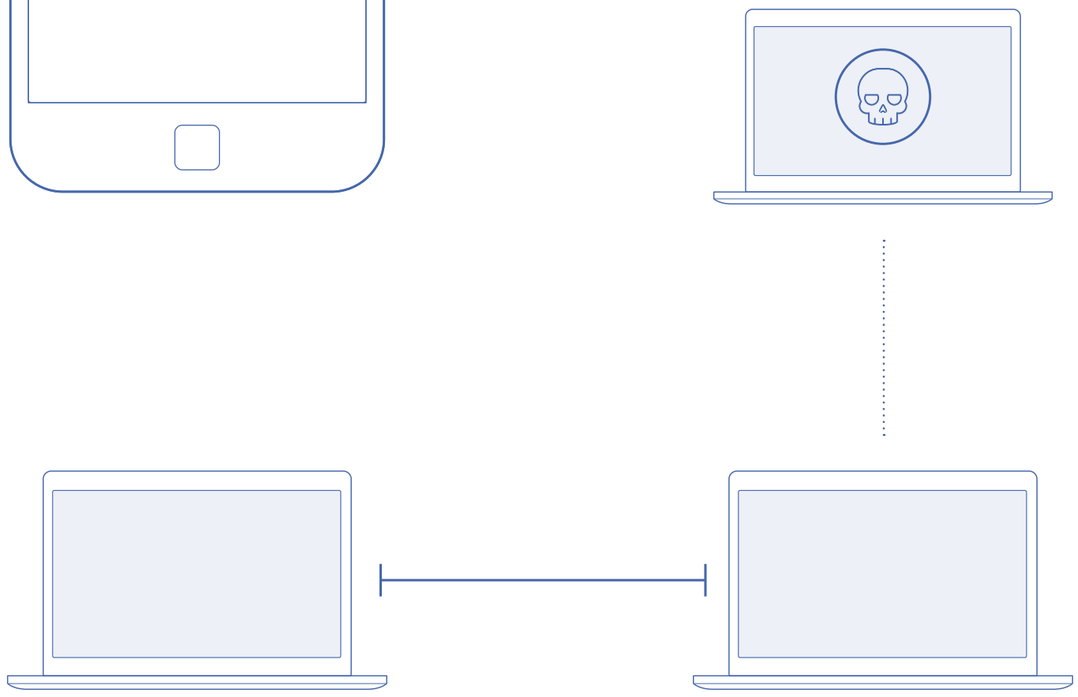
Recommendation: If you suspect that you have been targeted by a Facebook branded phishing campaign, please contact the Cyber Threats Crisis Email Line and/or your party's headquarters, and Facebook Security will assist in remediation.



Targeting of Professional Staff

Online security threats extend not only to you but also to your colleagues and staff. A common tactic is to use the same approach with the entire staff of the targeted victim in order to gather as much valuable information as possible.

Recommendation: Share security and best practices with your staff and colleagues. Internal security awareness training in your organization should emphasize the value of your information and the likelihood that dedicated malicious actors will try to acquire it.



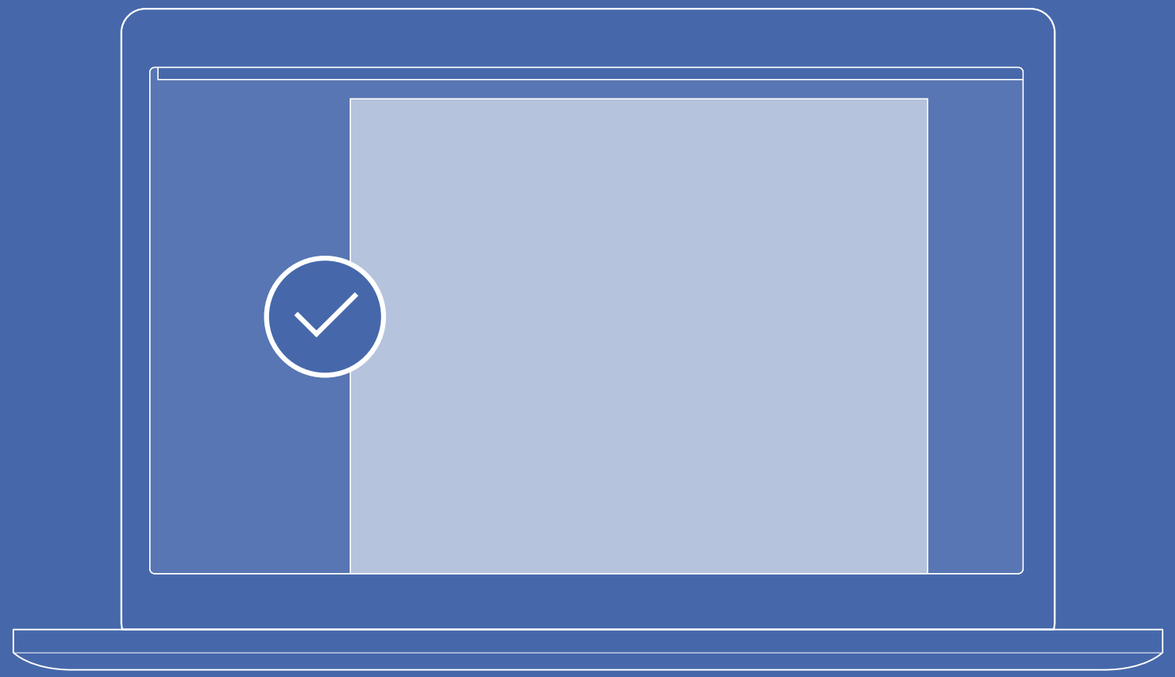
Website Compromise

Another approach bad actors have used is 'strategic web compromise', in which they infect specific websites that their targets are likely to visit. Navigating to one of these sites will lead to the automatic downloading of malicious code, often in the target's browser. This malicious code is then used to carry out further attacks, such as copying and sharing information accessed or browsed by the victim. Recently, this type of activity has focused on Ministries of Foreign Affairs and Embassy websites, which are likely to be visited by diplomats, politicians and their professional staffs.

Recommendation: Make use of web browsers only if they have built-in security protections, like Google Chrome, and regularly patch and update the web browsers and other software you use.

Authentic Identity of Page Admins

Facebook is based on the principle of authentic identity. When people stand behind their opinions and actions with their authentic identity and reputation, our community is more accountable. If we discover that people are not using their authentic identity, we will disable their accounts. When Page Admins do not use their authentic identity, they run the risk of having their accounts disabled and losing access to their Page.



Verified Pages

Pages and profiles can be verified by Facebook to let people know that they're authentic. A blue badge on a Page or profile indicates that Facebook has confirmed the authenticity of a Page or profile for a public figure or political party.

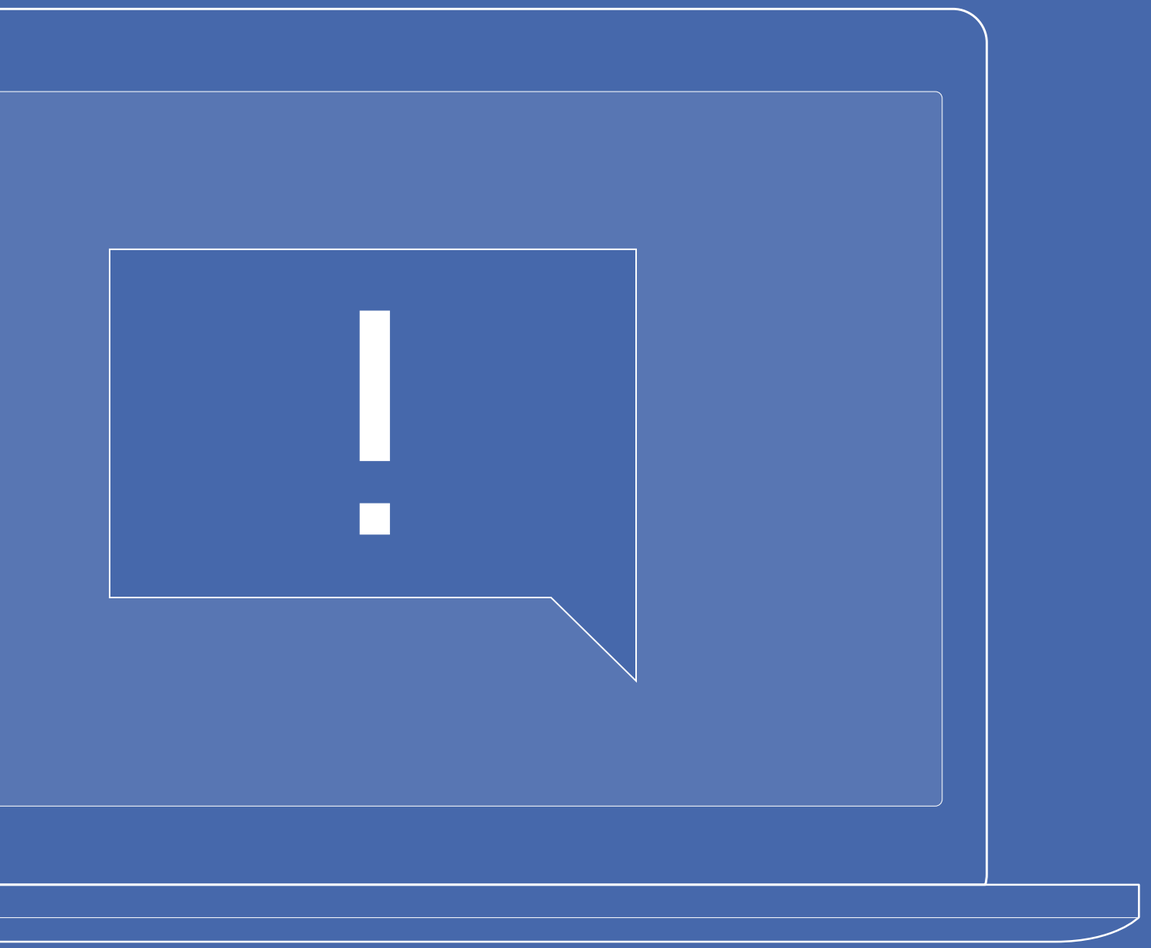
To request a blue verification badge, your Page or profile must comply with Facebook's terms of service and have the following:

1. A cover photo
2. A profile photo
3. A name that follows Facebook's guidelines
4. Content posted to the account
5. "Follow" enabled (profiles only)

Eligibility for the blue verification badge is based on a variety of factors, such as account completeness, policy compliance and public interest.

You can submit a request by filling out the **Blue Verification Badge Request Form**. We require a copy of your official government-issued photo identification (example: passport, driver's license, national identification card) to validate your request. We encourage you to include additional information to help us better review your request. Please include a few sentences explaining why the account should receive the blue verification badge and relevant URLs that help illustrate public interest for the account.

The **Blue Verification Badge Request Form** can be found in the Facebook Help Centre: **www.facebook.com/help**



Facebook Community Standards aim to find the right balance between a place where people can express themselves and an environment that is open and safe for everyone.

www.facebook.com/communitystandards

Reacting to Offensive Content

REPORTING OFFENSIVE CONTENT

The best way of reporting offensive content or spam on Facebook is to use the "Report" link next to the post. We look at the report and take suitable measures.

Here are some examples of how you can report content to us:

Report a comment on Facebook
Click "X" in the upper-right corner.
Select "Report"

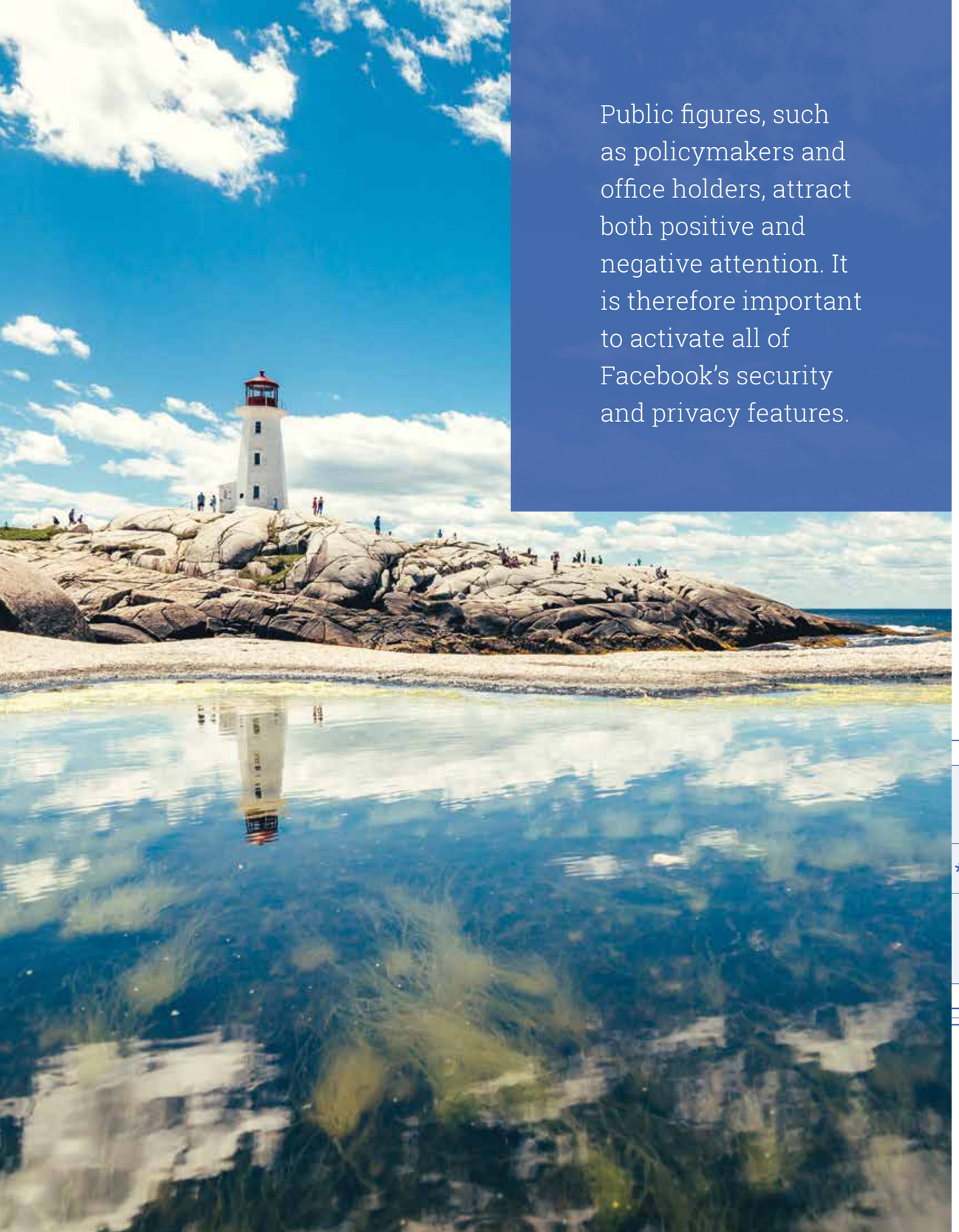
Report a message
Open the message that you want to report. Click the cogwheel in the top right.
Click "Report Spam or Abuse..."
and follow the instructions

You can find instructions for all content types at **www.facebook.com/report**.

DOCUMENT OFFENSIVE CONTENT

If you want to report illegal content to law enforcement agencies, it is a good idea to take screenshots of the undesirable activities.

If you ever feel like you or someone you know is in immediate danger, contact your local law enforcement.



Public figures, such as policymakers and office holders, attract both positive and negative attention. It is therefore important to activate all of Facebook's security and privacy features.

Top Safety Tips

Here are some safety tips to protect your account:

1. Protect your password
2. Use our **extra security features**: such as, two-factor authentication, login notifications, one-time passwords, app passwords and trusted contacts
3. Make sure your email account(s) are secure.
4. Log out of Facebook when you use a computer you share with other people. If you forget, you can log out remotely.
5. Run anti-virus software on your computer.
6. Think before you click or download anything.

Don't use your Facebook password anywhere else online.

Never share your password. You should be the only one who knows it.

Avoid including your name or common words. Your password should be difficult to guess.

You can find more safety tips in the Facebook Help Center: www.facebook.com/help

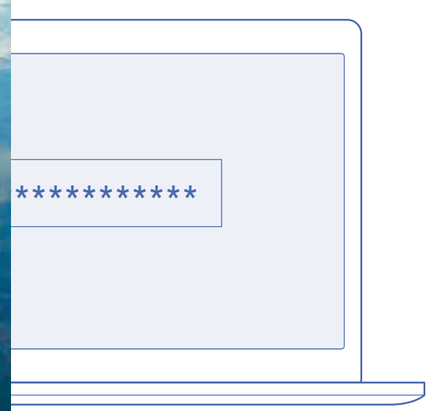


Photo by Justin Roy on Unsplash

Security Checkup

You can use Facebook's Security Checkup to review and add more security to your account. Security Checkup will help you:

1. Log out of Facebook from unused browsers and apps
2. Get alerts when someone tries logging into your account from an unrecognized computer or mobile device
3. Learn how to protect your password

You can find Security Checkup in the Facebook Help Center: www.facebook.com/help

Helping to Safeguard the Integrity of the Electoral Process in Canada

At Facebook, we take the safety of our platform and users very seriously. We are committed to doing our part to protect and safeguard the integrity of the electoral process in Canada.

Cyber Threats Crisis Email Line

We are making available to politicians and political parties in Canada a special **Cyber Threats Crisis Email Line** for compromised Pages and accounts in order to recover compromised accounts and address cyber threats as quickly as possible.

Further information and links

www.facebook.com/safety
www.facebook.com/help
www.facebook.com/about/basics

By Bernard Gagnon

Canadian Election Integrity Initiative

facebook

Canadian Election Integrity Initiative