2025 Canada Elections

Helping high-risk users stay safe online

Helping people stay safe online is our top priority and we recognize that this is especially important when it comes to our democratic institutions and processes. That's why we design our products with built-in protections and invest in global teams and operations to prevent abuse on our platforms.

In recent years, there has been a significant increase in cybersecurity threats, especially for individuals and groups that tend to be at higher risk for online attacks, such as candidates, journalists, campaign staff, and people working in public life.

To help anyone at risk, we're making our strongest security protections easily accessible and sharing more details about the best tools, tips, and resources people can use to protect themselves online.

1. Google provides several free tools focused on account security

Security Checkup provides personalized security recommendations for your Google account including recovery options, 2 step verification, screen locks, and more.

Password Manager makes it simple to use a strong, unique password for all your online accounts. When you use Google Password Manager, you can save passwords in your Google Account or on your device. To learn more and sign up, please visit **support.google.com/accounts**.

Follow the QR Code to learn more.

2. Google is also focused on online threats to high-risk users in election-related roles

The **Advanced Protection Program** is Google's strongest form of account security for those at highest risk of targeted attacks, recommended for anyone in the elections space. APP protects from phishing, by requiring passkey or security keys when logging in. It also provides protections from harmful downloads, blocking files that may be harmful.

It also keeps your personal information secure by only allowing Google apps and verified third-party apps to access your Google Account data, and only with your permission. New protections are automatically added to defend against today's wide range of threats, and you can now enroll with the seamless, secure authentication of passkeys.

Sign up today at no cost by visiting **google.com/advancedprotection** or by scanning the QR code.

Project Shield mitigates the risk of a distributed denial of service (DDoS) attack, a common tactic for malicious actors to disrupt online services by flooding them with massive traffic – making them inaccessible to legitimate users. Project Shield acts as a layer of defense to block traffic from these attackers, and increase the stability of a website. Project Shield is freely available for news, human rights, election-related websites (including political candidates), non-profit arts & sciences, and for governments experiencing exigent circumstances. Learn more about protecting your site at projectshield.google.

3. Passkeys: One step closer to a passwordless future

With the dramatic rise of state-sponsored cyberattacks and malicious actors online, we're more focused than ever on protecting people, businesses and governments by sharing our expertise, empowering society and continuously working to advance the state of the art in cybersecurity to help build a safer world for everyone.

Challenge

Passwords have been used with computers for over 60 years, but, today, they're simply no longer sufficient in keeping users' and organizations' data safe. Phishing attacks continue to grow in their scale and sophistication by taking advantage of security weaknesses in passwords.

Solution

Partnering with the FIDO Alliance, we enabled support for passkeys - a simpler and more secure alternative to passwords, bringing phishing-resistant technology to billions of people worldwide. With passkeys, you can skip your password for an easier and more secure sign-in experience, using your fingerprint, face scan or screen lock to sign in to your Google Account. Find out more by visiting **safety.google/authentication/passkey/.**

4. Helping you control your online presence

On Google Search, we offer a set of policies and tools to help people take more control over how their sensitive, personally-identifiable information can be found.

You can request to remove select personally identifiable information (PII) from Google Search results. This information includes Address, phone number, and/or email address and more.

Scan the QR code for more information regarding Google's **Personally-Identifiable Information removal tools**.

The **Google Civics Training Center** offers tools and resources to help you establish an online presence, including setting up your YouTube channel and ensuring your information appears accurately on Search.

Learn more at **civicsresources.withgoogle.com**.

5. Other safety considerations to keep in mind

Keep your devices secure

If your phone is ever lost or stolen, you can visit your Google Account and select "Find your phone" to protect your data in a few quick steps. Whether you have an Android or iOS device, you can remotely locate and lock your phone so that no one else can use your phone or access your personal information.

Browse the web safely

Be careful using public or free Wifi even if it requires a password. These networks may not be encrypted, so when you connect to a public network, anyone in the vicinity may be able to monitor your internet activity, such as the websites you visit and the information you type into sites. If public or free wifi is your only option, the Chrome browser will let you know in the address bar if your connection to a site is NOT secure.

Avoid online scams and phishing attempts

Phishing is an attempt to trick you into revealing critical personal or financial information, like a password or bank details. It can take many forms, such as a fake login page. To avoid getting phished, never click on questionable links; double-check the URL — by hovering over the link or long-pressing the text on mobile — to make sure the website or app is legitimate; and make sure the URL begins with "https."

For more information or questions, please contact ca-elxn-esc@google.com

Google