

SECURITY & PRIVACY CHECKLIST FOR MAYORS



mayors
innovation
project



WOMEN MAYORS
NETWORK

Mayors, elected officials, and city staff face unique risks when it comes to privacy. As public figures, they must maintain a public profile online. This attracts heightened interest from opponents, trolls, and cybercriminals targeting cities.

The checklist below covers essential elements of safety and security. Remember that security is a continuous practice, and everyone should make time to monitor their security protocols routinely. Trusted staff can help support in setting up these steps, but you should be involved in the process. Consider working with IT and related departments to make these steps part of a comprehensive municipal policy to protect yourself, staff, and city systems. Remember: check city, business, and personal accounts.

These steps are framed as personal actions for individuals, relevant to both leaders and staff.

1



Take stock of your online presence

- ✓ Check haveibeenpwned.com to see if your account logins have been included in any past breaches. Prioritize changing these credentials in part 3.
- ✓ Open an incognito browser window and Google yourself.
 - Take note of anything you want to be removed from your search results.
 - Do your social media accounts appear in Google searches, and if so, which ones?
 - Are your social media profiles public? If so, which ones?
 - The slide deck covers essential elements of safety and security. Remember that security is a continuous practice, and everyone should make time to monitor their security protocols routinely. Trusted staff can help support in setting up these steps, but you should be involved in the process. Consider working with IT and related departments to make these steps part of a comprehensive municipal policy to protect yourself, staff, and city systems.

2



Review your rules and laws

- ✓ If you qualify, remove your address from public [voter registration lists](#).
- ✓ Know your lawyer: determine if your city's legal resources are available to you in the case of security or harassment threats. If not, find a lawyer now, before a situation occurs.
- ✓ Review your state's rules and public information laws regarding social media accounts. For some general guidelines published after the 2024 Lindke v. Freed case, see [Social Media 2.0](#).

3



Digital defense and social media

- ✓ Keep personal social media accounts separate from professional, city, and campaign accounts, and hide personal social media accounts from Google (each platform has its own instructions).
- ✓ Ensure professional and campaign accounts are viewable on Google. If you are not on major platforms, consider making accounts to prevent impersonation.
- ✓ Use strong, unique, long passwords for important accounts. Use 2-factor authentication or a password manager and consider working with your IT department to make this city policy.
- ✓ Remove location information from social media posts by default; turn off geotagging and refrain from posting about an event until you have left the location. If posting live, be aware of recognizable signage or landmarks in your posts. When possible, close relatives of the official are advised to take similar measures to protect privacy and location information.

4



Plan for threats and harassment

- ✓ If you can, use a PO Box or Commercial Mail Receiving Agency box instead of a home address to file candidacy or updates to information.
- ✓ Find and remove personal contact info in Google using their free “[Results about you](#)” feature, and then file a detailed removal request form.
- ✓ Remove address and phone listings from people finder websites like Whitepages, Spokeo, and Radaris. There are hundreds of these sites. Find a full list with instructions for opting out [here](#), or consider a paid service like [Optery](#) or [DeleteMe](#) to help automate this task.

5



Define and be ready to act on threats

- ✓ Make a plan and have criteria for what constitutes a credible threat. The police in your area may not be familiar with serious online harassment; make sure you [document the threats clearly](#), and consider talking to law enforcement about online harassment before an issue arises. If possible, work with local law enforcement to create a shared definition of a credible or actionable threat so that when such a situation arises, you are already on the same page.
- ✓ Key safety plan elements include: where to go when your home does not feel safe; talking to a few trusted friends and family about the plan and how they can avoid scams and threats; distinguishing between protests and threats, and knowing when the former becomes the latter; and who you will bring in to help with challenges like harassing emails so that you may better protect your mental health.

6



Assess your city's security culture

- ✓ Identify who is responsible for policies around social media, security, and harassment, and empower them to institutionalize best practices.
- ✓ Implement trainings for city staff, including more creative learnings, such as your IT department sending fake phishing emails and reporting back on how many staff clicked links. Security is an abstract concept - do not wait until it is too late to make it 'real.'
- ✓ Remember: this issue impacts you personally, but it is also a major issue for your constituents. Consider using blogs, social media, and more to talk to your constituents about the work you are doing around security and encourage them to do the same.

THANKS TO THE FOLLOWING PARTNERS FOR MAKING THIS CONTENT POSSIBLE OVER THE YEARS.



Looking for more?

[A Digital Resilience Toolkit for Women in Politics](#) by Kristina Wilfore, ShePersisted, 2022

[Protests and Public Safety: A Guide for Cities & Citizens](#) by Institute for Constitutional Advocacy and Protection at Georgetown Law, 2022

[Keeping Statewide Elected Officials Safe](#) by States United Democracy Center, 2023