mayors innovation project

Digital Defense Checklist

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.

Part 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 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.

Part 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.

Part 3: Clean up your digital presence

- [ ] Separate personal social media accounts from professional, city, and campaign accounts.
- [ ] Hide location information from social media posts by default. Delay social media posts that reveal an event's location until after you have left an event.
- [ ] Implement a password manager to help you use long, unique passwords for every account. Consider working with your IT department to make this city policy.
- [ ] Change your most important passwords to be unique and longer than 12 characters.
- [ ] Turn on 2-factor authentication for important accounts.
- [ ] Hide personal social media accounts from Google (each platform has its own instructions). Ensure that professional and campaign accounts are viewable on Google. If you are not on major platforms, consider making accounts to prevent impersonation.

Part 4: Plan for harassment, stalking, and protests

- [ ] Use a PO Box or Commercial Mail Receiving Agency box instead of home address. Remove address and phone listings from websites like Whitepages.
- [ ] Remove listings from Spokeo, Whitepages, and other data aggregator sites. Consider a paid service like DeleteMe or PrivacyDuck to help automate this task.
- [ ] Plan for threats. Create your plan seriously and enact it when you receive threats.

    - 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.
    - 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.

Part 5: 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.

We thank our partner, the **Digital Defense Fund,** for making this content possible. To learn more about their work, go to: https://digitaldefensefund.org/

digital defense fund