States United DEMOCRACY CENTER

# Keeping Statewide Elected Officials Safe: Securing Online Activity

The security of statewide elected leaders is essential to maintaining peace, order, and trust in American democracy. This document addresses suggestions for safeguarding such officials' online activity; these suggestions will also be helpful to staff. Other documents in the series include: Reviewing Security Resources and Deploying the Security Team, Protecting Loved Ones and Hardening Home Security, Preparing for Events, Protecting Personal Identifiable Information, and Office and Staff Security Considerations.

---

### Use two-factor identification.

This provides an extra layer of account security for log-ins.

### Always require a password to access your phone, computer, and tablet.

### Passwords should be strong, unique to each account, and changed frequently.

A strong password includes capital and lower-case letters, numbers, and symbols. It should never include personal information, such as your name. Passwords should be changed every 30 days, should never be used for more than one site, nor reused, nor shared with others (including staff). A password manager/ vault (with encrypted storage) may help you keep track of each password.

### Keep software updated, especially your operating system, security software, and browser.

Software providers regularly issue updates to patch security holes.

### Create a secondary email account to log in to websites for personal purposes.

A secondary email account, not used for personal correspondence but for logging in to websites, will reduce spam and exposure to cyber criminals.

### Don't click on links or attachments in suspicious emails.

They may include viruses. Unless you know the sender and the contents of the attachment or link, do not click on it.

### Don't use unsecured or unknown wireless networks. Be wary of using free and/or public Wi-Fi.

These networks are frequently exploited by cybercriminals. Use only known networks, and use your mobile device's network, which tends to be more secure, for highly sensitive data, such as online banking. Consider using the data on your phone or carrying a hotspot with you.

## Enable remote tracking for wireless devices.

This allows you to find a lost device.

## Enable wiping for wireless devices with only personal information on them and discuss procedures with counsel about devices with work information on them.

In the event that a mobile device with only personal information on it is lost, ensure that deleting the contents remotely is possible. Consult with counsel about what to do in the event a work device is lost, as state laws and policies may impact the appropriate response.

## Download only trusted apps and keep them updated.

Mobile applications often gather large amounts of personal data, including location data and contacts. Be sure you know what an application is collecting before downloading it. Keep apps up to date to patch security issues.

## Log out of accounts when you're not using them.

This is especially true on a public computer.

## Determine the appropriate use of social media, which presents unique security concerns.

- Avoid posting about or tagging your real-time location in your private life and consult with security professionals before doing so in your official capacity.
- Consider deleting private social media accounts. If you use social media, use privacy settings to control who can find your profile and see your posts.
- Consult security professionals before posting images of your office or home.
- Ensure that the official's loved ones are instructed in social media hygiene.

## Exercise extra caution when making online purchases.

- Buy only from sellers with a non-P.O. Box physical address and phone number.
- Buy only from secure sites. Check a seller's security/encryption software before buying. Sites that begin with "https" tend to be more secure, as are ones with a padlock icon in the browser location field. Avoid buying from sellers outside the United States when possible.
- If you buy from someone directly, email them first to see if their email address is active.
- Double-check the domain name to make sure you are buying from the correct site. Cyber criminals set up fake sites that mimic legitimate sites and have similar URL addresses. Read reviews of the seller on other sites, ideally trusted third-party sites.

Updated March 2023

---

*The States United Democracy Center is a nonpartisan organization advancing free, fair, and secure elections. We focus on connecting state officials, law enforcement leaders, and pro-democracy partners across America with the tools and expertise they need to safeguard our democracy. For more information, visit [www.statesuniteddemocracy.org](http://www.statesuniteddemocracy.org) or follow us at @statesunited.*