What Every Candidate Should Know About Cybersecurity

Unfortunately, candidates—and their families—are potential cyber targets.

All candidates and their family members should take a few simple steps to make sure their accounts are not easy targets for hackers.

1. Set the Tone

a. **Talk with your family about digital security.**
Human choices are the most important factor in any cyber security strategy. Your family should be aware that hackers may try to target them. They should follow the security steps below and be vigilant. Most importantly, they should be careful about what information they put in email and on social media. It's especially important to have a conversation with children and teenagers about securing their social media accounts and setting ground rules about what is appropriate to post. When possible, keep conversations in person or on the phone and always assume anything written in email or posted on social media could become public.

b. **Cultivate a security culture in your campaign**
Reinforce to staff how important security is to the success of your campaign. Model security best practices, so staff can follow your example.

2. Keep campaign business off personal accounts

By keeping your personal and campaign email accounts separate, it's less likely that hackers will steal your personal emails if they target your campaign.

3. Use encrypted messaging and don't keep what you don't need

Use an encrypted messaging app like Signal or Wickr to chat with family or staff. They're much harder to hack and you can set them to auto-delete messages. Also set your email to auto-delete messages more than a month old. This will leave less data for hackers to steal.

(Continued on back)

4. **Activate Two-Factor Authentication**

   You and your family members should add two-factor authentication to your personal and work email, file storage, and social media accounts. Your campaign will tell you which two-factor method to use. Two-factor authentication makes it a lot harder for the bad guys to get into your account even if they steal your password.

5. **Create Strong Passwords**

   You and your families should create passwords that are as long as possible. Less than 8 characters is too short. 12 or longer is much better. Contrary to popular belief, it should not include requirements for numbers, special characters, or capitalization. `SOMETHINGLIKETHISPASSWORDHERE` is actually harder to hack than `s0m3TH!n6L1k$`. String a set of words together that are easy for you to remember.

   Don't write your password down where someone can find it. If you have even a faint suspicion that someone might know your password, change it immediately.

6. **Secure your devices**

   Work with your campaign staff to make sure your computer and phone are secure as possible. You'll want to be sure all your devices automatically lock and require a password. You'll also want to be able to wipe your devices remotely in case they get lost.