What Every Election Staffer Should Know About Cybersecurity

1. **Everyone is a security official**
   Take cybersecurity seriously. Take responsibility for reducing risk, training your staff, and setting the example. Human error is the number one cause of breaches. Spear-phishing attacks and other attempts at interference can be thwarted with cybersecurity vigilance.

2. **Use two-factor authentication (2FA)**
   Use two-factor authentication for everything: official work accounts, personal email accounts, social media accounts, and any data storage services. Use a mobile app (such as Google Authenticator, Duo, or Authy) or a physical key (such as Yubikey or other U2F devices) for your second factor, not text messaging. 2FA is an extra step, but is very effective at preventing unauthorized access.

3. **Create long, strong passwords**
   Current computing capabilities can crack a seven-character password in milliseconds. For your passwords, create **`SomethingReallyLongLikeThisString`**, not something really short like **`Th1$`**. Contrary to popular belief, a long string of random words without symbols is more difficult to break than something short, with lots of **`$ymB01$`**.

4. **Keep credentials secure**
   When collaborating with others, resist the temptation to share credentials to systems with them, regardless of who they are.

5. **Practice cyber hygiene**
   Follow all applicable guidance for patching and software updates. Ensure that your systems have the most updated antivirus software.