Starter Cybersecurity Checklist

What you can do to improve your cybersecurity today.

1. **Set up two-factor authentication.** With two-factor authentication (“2FA”) enabled, a bad actor needs more than your password to compromise your data. This is one of the most effective cybersecurity measures today.
   - Most major online services now offer two-factor authentication
   - Read more at: https://eff.org/common2FA

2. **Never reuse passwords and consider using a password manager.** No matter how strong your password is, if a service you’ve used it for is compromised (which has happened too many times to count), an attacker can discover it and exploit it. Using a password manager is an easy way to create and manage a variety of strong passwords.
   - **You can check if your email has been involved in a publicly known data breach at:** https://haveibeenpwned.com/
   - Read more at: https://ssd.eff.org/en/module/creating-strong-passwords

3. **Make sure your software is up to date!** There’s a reason why you hear this all the time.
   - Remember WannaCry? The vulnerability at the heart of that ransomware is still reeking havoc because so many computers remain out-of-date

4. **Encrypt your communications.** Safeguard against interception of your communications by using applications that protect them with ‘end-to-end encryption.’ With end-to-end encryption, only the people (or devices) who are supposed to read your messages can decipher them.
   - Signal is one popular messaging application with end-to-end encryption
   - Read more at: https://ssd.eff.org/en/module/what-should-i-know-about-encryption

5. **Encrypt your data, too.** Encryption keeps your data secure even if an attacker obtains your device. While iPhones have full-disk encryption enabled by default when a passcode is set, one must activate it manually for Android phones as well as Mac and Windows computers. This can be done in their respective security settings.
   - Read more at: https://ssd.eff.org/en/module/keeping-your-data-safe

6. **Start planning for the future.** Lasting cybersecurity is a process, not a checklist. The following guides are both accessible and effective:
   - Electronic Frontier Foundation’s Surveillance Self-Defense guide, available at: https://ssd.eff.org/
About the Fourth Amendment Advisory Committee

The Fourth Amendment Advisory Committee is dedicated to supporting civil liberty and the work of the Congressional Fourth Amendment Caucus. We educate decision-makers on issues related to the Fourth Amendment, especially when law and technology intersect.

Since 2016, the Fourth Amendment Advisory Committee has hosted over a dozen events educating lawmakers and their staffs on pressing Fourth Amendment issues ranging from warrantless surveillance to encryption. Please sign up for invitations at https://www.fourthadvisory.org. You can also view recordings of our past events at https://www.fourthadvisory.org/news.

For more information about the Fourth Amendment Advisory Committee, please contact:

Sean Vitka
sean@fourthadvisory.org

For more information about the Fourth Amendment Caucus, please contact the caucus co-chairs:

Representative Lofgren
ZJ Hull
ZJ.Hull@mail.house.gov

Representative Amash
Carolyn Iodice
Carolyn.Iodice@mail.house.gov