

Twenty-first century technology evolves at a breakneck pace that unfortunately limits our ability to fend off digital hacks and malware. The best defense against digital intrusion is knowledge. Here are the best practices for securing your information online:

1. **Keep your passwords safe.** Don't use the names of your children, pets, favorite sports teams or dates of birth, as this information can be easily found on social media profiles. Don't use the same password in multiple online accounts. Change your passwords regularly. Consider using a Password Manager program such as Norton Identity Safe.
2. **If in doubt, don't click on it.** Be skeptical. Cyber criminals send fake emails or texts that can look authentic. This is called "phishing," and these links contain malicious software ("malware") that can mine your device for personal information. Be wary of any emails and messages that seem to be from a company you do business with, especially if they contain spelling mistakes, poor grammar or use a different tone of voice compared to previous communication you've received from the company. Also remember that most businesses will never send you emails or texts, or even call you, asking for secure information. If you do receive a message fitting this description, delete it immediately.
3. **Use two-factor authentication (TFA).** Adding an extra layer of security will significantly increase protection. This could involve adding a personal question, using biometric scanning, voice recognition, a secret username, or using your email and phone to confirm new login and transaction requests.
4. **Use a comprehensive, integrated security solution.** Using lots of different security software can leave gaps in your defense, so consumers are usually better off using a single comprehensive security solution that covers all their connected devices and protects against all the different types of threats - from spyware and viruses to financial Trojans. Program examples include Norton 360, AVG Ultimate, or Avast Premium, to name a few.
5. **Stay vigilant and responsive.** Regularly check your bank and credit statements to spot any transactions you didn't make. If you see anything that looks odd, alert your financial institution and change your credit or debit card. If

a company that you use has experienced a breach, change your passwords immediately.

6. **Use VPNs, especially on public Wi-Fi.** Many public Wi-Fi connections are unencrypted, offering the chance to intercept data being sent and received by your device. Using a virtual private network (VPN) – available by subscription – makes it much harder for your data to be intercepted.

If you follow these six security habits and remain vigilant, you will significantly decrease your exposure to potential digital security threats in 2020 and beyond.