Six ways to protect yourself and your company online

1. **Create strong passwords**
   - Pick complex passwords. Change them often.
   - Consider using fake answers to security questions to make it more difficult for criminals to access your accounts.
   - People still fail to create strong passwords—1 in 5 employees’ credentials could be easily compromised.

2. **Check your computer for personally identifiable information**
   - This includes your Social Security, driver’s license, and passport numbers.
   - Who’s behind company breaches? 73% Outsiders
     - 50% Organized criminal groups
     - 12% State-affiliated actors
     - 12% Organized criminal groups
     - 2% Multiple parties
     - 2% Partners

3. **Keep software up to date**
   - Before downloading an update, visit the company’s website to confirm it’s legitimate. Upgrade as soon as possible.
   - 200,000+ people in 150+ countries affected by ransomware WannaCry.

4. **Avoid public Wi-Fi**
   - Don’t connect to hotspots or networks before verifying they’re secure.
   - 73% of Americans don’t use a virtual private network to secure their Wi-Fi connection, even though it could help protect their personal data.

5. **Stay vigilant on email**
   - If you don’t recognize a sender’s email address, don’t click on a link. Be wary of any email asking for confidential information.
   - Business email compromise (BEC) scams, relying on spear-phishing emails, targeted 7,710 organizations each month and have exposed victims to $12.5 billion in losses.

6. **Pay attention to URLs**
   - 73% of Americans don’t use a virtual private network (VPN) to secure their Wi-Fi connection, even though it could help protect their personal data.

---

Data sources:
6. Domestic and international exposed dollar loss, reported by the FBI, Internet Crime Complaint Center (IC3), July 12, 2018.

© 2018 Wells Fargo Bank, N.A. All rights reserved.