Cybersecurity checklist

This checklist provides actionable steps to help protect yourself from online threats that can lead to financial fraud and/or identity theft.

The Trusted Advisor

- [ ] **Create online accounts for all financial or healthcare-related accounts and monitor them regularly.**
  You may think you're keeping yourself safe by not creating an online account, but you may be surprised to learn that the opposite is true. If you don't set up your own online accounts, someone else potentially can.

- [ ] **Use strong passwords and consider a password manager.**
  When creating strong, unique passwords, consider using a passphrase – a sentence-like string of words that's more complex and harder to guess – and don't reuse passwords for multiple accounts. Secure password manager programs can help keep track of your login information across accounts.

- [ ] **Enable multi-factor authentication when available.**
  Also known as two-factor and two-step authentication, this helps minimize risk by adding a step to verify your identity, rather than relying on your username and password alone.

- [ ] **Sign up for text, email, and phone alerts for online account activity.**
  This adds a layer of confirmation for any account activity. Not you? Contact the institution right away.

- [ ] **Use anti-virus and anti-spyware security software.**
  Regularly update all software to fix security vulnerabilities that could be exploited.

- [ ] **Avoid phishing scams.**
  Be vigilant about suspicious emails, links, and attachments, and never click on anything that seems too good to be true or from an unknown sender. Misspelled words and email addresses and unfamiliar logos may be signs that a communication is not legitimate.

- [ ] **Use caution when providing personally identifiable information (PII).**
  Scam artists may call or text you claiming to be from a financial institution and request PII like your Social Security number. Legitimate institutions will never request this information from you. Only provide PII in person or through secure messaging portals, and only when you're the one initiating the communication.

- [ ] **Be wise about Wi-Fi.**
  Use caution when connecting to public Wi-Fi networks as they are often not secure, and your information could be viewed by others. Consider using a VPN (Virtual Private Network) for extra protection.

- [ ] **Review your apps' and devices' privacy policies and location settings.**
  Yes, they can be long and complex, but they tell you how the site maintains accuracy, access, security, and control of the personal information it collects. Limit what PII you share publicly.

- [ ] **Consider using credit monitoring services.**
  Monitor your credit closely. If you receive alerts about unfamiliar credit applications, changes to your credit score or report, it could indicate that your personal data has been compromised.

- [ ] **Back up your data regularly.**
  Frequently back up important data to an external hard drive or cloud storage service to protect against data loss.

Transamerica℠

The Trusted Advisor

Additional resources

Fraud
reportfraud.ftc.gov

Identity theft
Identitytheft.gov

Credit bureaus
- Equifax, Experian, and Transunion
- AnnualCreditReport.com
- usa.gov/credit-reports

Help your clients make trusted and informed decisions, so they can live their best lives today and tomorrow.

Visit **transamerica.com/trusted-advisor**

4276339

Transamerica℠