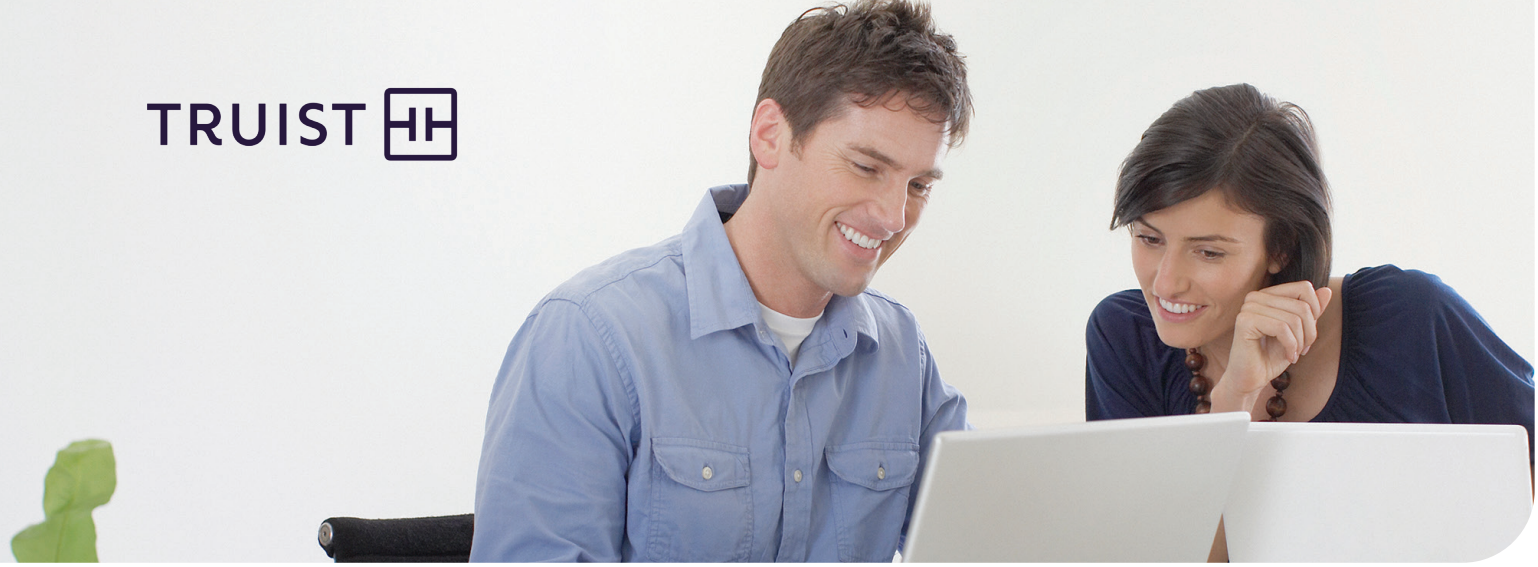

Cybersecurity Checklist: Working Together to Prevent Fraud and Protect Your Data

We use a multi-layered strategy of technology and dedicated teams to help **protect you and your finances from fraud** and other security threats. Even with tremendous investments in fraudsters can gain access to your information through social engineering, identity theft, and malware.

Supplement our security measures by using the checklist below.

1. Use unique passwords for each account and protect them

- Create long passwords that contain symbols, numbers, and uppercase and lowercase letters
- Don't reuse or recycle your passwords
- Don't share your passwords with anyone
- Change your passwords using a randomly generated schedule
- Ensure that your passwords bear no resemblance to former passwords
- Consider using a secure password manager to help with creating unique passwords across multiple sites

2. Enable multifactor authentication where available

Multifactor authentication requires additional verifying information to grant access to an account. This gives your accounts an added layer of security. Multifactor authentication can include:

- SMS or email notifications
- Biometric identification
- Tokens

3. Avoid links from unknown sources in text, email, instant message, social media and websites

- Be suspicious of any message that asks you to provide personal information. Truist never uses emails or text message to solicit your personal information
- Hover your mouse over hyperlinks to inspect their true destination
- Make sure you're on the right site before entering personal information - such as your name, address, birth date, Social Security number, phone number or credit card number

4. Limit what you share on social media and who can view your profile

You should protect the following information in particular:

- Your birthdate
- Your street address
- Geotagged photos
- The time you're away on vacation

5. Secure your devices

- Always keep your device's software updated (use the latest operating system and browser versions available)
- Install security software and keep it up to date
- Download apps from trusted app stores
- Turnoff Wi-Fi/file sharing/ AirDrop options when not in use
- Avoid working with personal or sensitive data when you're using unsecured, public Wi-Fi
- Lock your devices and use biometric authentication (like face or fingerprint recognition)

6. Secure your important documents

Protect your Social Security cards, passports and birth certificates by storing them in a secure place such as a safe deposit box, and only carry them when you need them for a specific purpose.

This information can be used by an identity thief to commit fraud like taking over your financial accounts, opening new loans and credit cards, and establishing utility services in your name.

7. Shred documents containing personal/financial information

When you're done reviewing your paper documents like your receipts, financial statements, or credit card bills, put them in the shredder instead of the trash. Or choose paperless statements for easy, safe record keeping.

8. Order your credit report annually from each credit bureau

Read your credit report regularly. Make sure it's accurate, and if you spot an inaccuracy, follow up. Check reports from Experian, Equifax, and Transunion.

9. Keep your contact information up to date

Update your email, mobile phone and mailing address to ensure Truist can contact you in case of suspicious activity.

10. Download the Truist app and enable alerts and card controls

Protect your peace of mind: Get notifications about important account activity and lock your credit or debit card instantly.