Online (and Offline) Security Checklist

PROTECT YOUR DATA AND DOLLARS

Today online security is more important than ever, with millions of Americans having been affected by identity theft. Knowing how to guard your personal information is the first line of defense.

How to Protect Yourself

ONLINE

Use strong passwords; change them often.

- Use different passwords so a data breach doesn't expose other accounts.

Be wary of Wi-Fi.

- Put a password on your home Wi-Fi.
- Avoid logging in to personal accounts through public Wi-Fi.

Know what you're clicking on (emails, websites, ads, popups).

- Beware of commands to act urgently, threats of consequences, bad grammar and misspelled words.
- If you're unsure about an email link, type in the web address (don't click).

Use social media privacy settings.

- Think before you post personal specifics like birthdays, hometown, kids' names, trip pictures, or current location.

OFFLINE

Keep important documents safe.

- Lock Social Security cards, birth certificates, and insurance, financial and tax records in a safe or file cabinet.

Shred documents with personal info.

- Safely discard bills, bank statements deposit receipts and credit card offers.

Check mail daily.

- Stop delivery if you're away from home.
- Sign up for Informed Delivery (a digital preview of your mail) at USPS.com.

Keep track of your wallet or purse.

- Consider what you really need to carry: driver's license, debit/credit cards, work ID and health insurance card.

ON YOUR PHONE

Don't give out personal or financial information during an unsolicited call.

- If the caller claims to be from a company and you're unsure, hang up and call the company's publicly available number directly.
- Never reply to text messages asking for personal information.

Lock your smart phone; choose a strong passcode.

- Consider using fingerprint or face recognition scans.
- Get track-and-wipe software in case of theft.

How to Protect Those You Care About

CHILDREN

Identity thieves target children for their clean credit histories. Children's data also can be exposed through online gaming or social media.

Warning Signs

- The child is turned down for government benefits.
- IRS sends notice that the child didn't pay income taxes, or that their Social Security number was used on another tax return.
- You receive collection calls or bills for products or services you didn't receive.

PARENTS AND ELDERLY

Seniors' regular income and accumulated assets put them at greater risk for financial exploitation.

Warning Signs

- The individual is unwilling to discuss or seems confused about financial or estate plans.
- You notice unusual bills, collection notices, payments, withdrawals, new accounts or sudden account closures.
- Expected checks are missing or never deposited.
- Relationships seem to influence financial decisions.

American Century Investments®

What to Do If You Suspect Identity Theft

- Contact financial institutions.
- Change passwords.
- Close fraudulent accounts.
- Place a fraud alert on credit reports.
- File a report at IdentityTheft.gov.
- Order copies of credit reports.
- Capture everything in writing.

STAY AWARE

LIMIT ACCESS

MONITOR ACCOUNTS

Resources

CREDIT REPORTING AGENCIES

Experian
1-888-397-3742
www.experian.com

Equifax
1-800-685-1111
www.equifax.com

TransUnion
1-800-916-8800
www.transunion.com

FEDERAL TRADE COMMISSION RESOURCES

Get Free Annual Credit Reports
www.annualcreditreport.com

Report Identity Theft
www.identitytheft.gov

Opt Out of Pre-Approved Credit Offers
1-888-567-8688
www.optoutprescreen.com

Sign Up Your Phone With the National Do Not Call Registry
1-888-382-1222
www.donotcall.gov

American Century Investments®