

WHAT'S YOUR IDENTITY THEFT RISK?

FIGHTING FRAUD: STAY ONE STEP AHEAD



Identity thieves are always looking for opportunities to steal personal information. How well do you protect yourself? Read each statement below and checkmark it if it applies to you.

- My mailbox is secured with a lock or I use a P.O. box.
- I always drop outgoing mail in an official USPS collection box or at the post office, rather than leaving it in my home mailbox.
- I properly dispose of personal documents by shredding them before discarding.
- I only carry the credit and debit cards I need for the day, leaving unnecessary cards at home.
- I memorize my PINs rather than writing them down or storing them in my phone.
- When entering passwords, PINs, or payment details in public, I shield the keypad from view to prevent onlookers from seeing my information.
- I change my PINs and passwords often.
- My passwords are strong, at least 10-12 characters long, and include a mix of uppercase and lowercase letters, numbers, and special characters.
- I use a password manager to keep track of my login credentials securely.
- I only carry my Social Security card when absolutely necessary.
- I am selective about sharing my Social Security number and always ask why it's needed and how it will be protected before providing it.
- I do not give personal information over the phone to unfamiliar callers.
- I use a credit monitoring service to keep an eye on any suspicious activity.
- When using public Wi-Fi, I connect through a VPN to protect my data.
- I avoid clicking on links in pop-up windows.
- I do not click on links in emails or text messages from unknown sources.
- Before using ATMs or card readers, I inspect them for signs of skimming devices.
- I always take my receipts, store them securely, and shred them when they are no longer needed.
- I do not use the autofill feature to save my login credentials.
- I remain vigilant about security risks while traveling.
- My computer and devices are protected by security software and programs.
- I keep my operating system and all software updated to the latest versions.
- I confirm the authenticity of websites by typing the address directly into my browser rather than using email links.
- I only download apps, software, and email attachments from trusted sources.
- I review all terms and disclosures before installing new software.

- I am mindful of what personal details I share on social media.
- I recognize that people online may not always be who they claim to be and remain cautious in my interactions.
- My home Wi-Fi network is password-protected and secured against unauthorized access.
- I enable two-factor authentication on my online accounts for extra security.
- I adjust all security and privacy settings on my computer and online accounts to the highest level of protection.
- I take advantage of security features available on all my internet-connected devices.
- I ensure my mobile devices do not automatically connect to public or unknown Wi-Fi networks.
- I log out of accounts and close my browser when finished with an online transaction.
- Before entering personal information on a website, I check for signs that the site is legitimate and secure.
- I do not store personal data or log into personal accounts on workplace computers or devices.

How Did You Score?

If **you marked most of these statements as true**, congratulations! You're taking strong steps to protect yourself from identity theft. For those that are unchecked, consider how you may be putting yourself at risk and take action to strengthen your security.

#StayOneStepAhead | [EnvistaFraudDefense.com](https://envista.frauddefense.com)