BETTER SAFE THAN SORRY

CYBERSECURITY BEST PRACTICES

Identity fraud losses in 2021 amounted to $24 billion and affected 15 million U.S. consumers.[1]

As part of Transamerica's commitment to safeguarding the privacy and personal information of our customers, we take many precautionary steps to protect sensitive data. Those measures include routine security evaluations and additional security for certain systems.

You can play an important role in helping reduce the risk of a cyberattack. We've outlined a few simple principles you can adopt to practice "good cyber hygiene" that can help keep your financial information secure.

CREATE COMPLEX PASSWORDS AND CHANGE THEM FREQUENTLY

First things first: If you haven't done so already, create login credentials for your online accounts. Wherever possible, use complex passwords of at least eight (8) characters long and mix numbers, upper and lower case letters, and symbols. Make your passwords unpredictable. Change passwords often and avoid using the same password on other websites. Don't use names, dates, or words related to you. Passwords aren't for sharing; they're for your eyes only.

MAKE SURE YOU HAVE UP-TO-DATE SECURITY SOFTWARE AND REGULARLY RUN VIRUS CHECKS ON YOUR COMPUTER

Good protection software provides 24/7 online safety against malicious software by preventing harmful malware from coming into contact with your computer system. Outdated software makes you vulnerable to attack, so keep your software — including your operating system, web browsers, and apps — up to date to protect against the latest threats. Use a firewall — a software program or piece of hardware that helps protect your computer.

BEWARE OF PHISHING SCAMS THAT ASK YOU TO PROVIDE PERSONAL INFORMATION IN EMAILS, TEXTS, AND POP-UPS

Reputable companies won't request confidential information or ask you to reset a password over email. These requests are key indicators of likely phishing scams. Be cautious about opening attachments or clicking on links in emails. These links could not only harm your computer and expose personal data, but also any other information stored on your computer. Instead, verify the URL of the company's website, open a new browser window, and type the verified URL directly into the address bar.

REMAIN VIGILANT AND REGULARLY REVIEW ACCOUNTS AND CREDIT REPORTS FOR ANY UNAUTHORIZED ACTIVITY

Review all account statements on a regular basis. Use available confirmations and alerts to catch anything suspicious in real time. Unusual or unauthorized activity could indicate that someone has stolen personal details or committed fraud. That's why it's important to monitor your credit profile. For more information about identity theft, visit **identitytheft.gov/steps.**

For more information, visit the federal government's website.

Visit: OnGuardOnline.gov

[1] "2022 Identity Fraud Study: The Virtual Battleground," Javelin Strategy & Research, March 2022

117773R3

TRANSAMERICA®