CYBERSECURITY BEST PRACTICES

Cybersecurity incidents and data breaches in the U.S. are at an all-time high. Transamerica is committed to safeguarding the privacy and personal information of all our customers. We take numerous precautionary steps to protect personal data, including routine security evaluations and enhanced security for certain systems.

You can play an important role in helping reduce the risk of a cyber-attack. Below, we've outlined a few simple principles of what we like to call "good cyber hygiene" that you can adopt to help keep financial information secure.

CREATE COMPLEX PASSWORDS AND CHANGE THEM FREQUENTLY.

If you have not done so already, it is important that you establish login credentials for your online accounts. Wherever possible, use complex passwords that are at least eight (8) characters long and mix numbers, upper and lowercase letters, and symbols. Make your passwords unpredictable. Change passwords often and avoid using the same password on other websites. Do not use names, dates or words related to you. Remember not to share your passwords with anyone else – passwords should be 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, TEXT 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, but also expose personal data and 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 https://www.identitytheft.gov/steps.

For additional information on how you can protect your networks and personal computing devices, visit the federal government's website www.OnGuardOnline.gov.

TRANSAMERICA®