NATIONAL CYBERSECURITY AWARENESS MONTH

DO YOUR PART.
#BECYBERSMART

IDENTITY THEFT AND INTERNET SCAMS

Today's technology allows us to connect around the world, to bank and shop online, and to control our televisions, homes, and cars from our smartphones. With this added convenience comes an increased risk of identity theft and Internet scams. #BeCyberSmart on the Internet—at home, at school, at work, on mobile devices, and on the go.

DID YOU KNOW?

- The average cost of a data breach for a US company in 2019 was $8.19 million? That's an increase of 130% since 2006!
- 7-10% of the U.S. population are victims of identity fraud each year, and 21% of those experience multiple incidents of identity fraud.

COMMON INTERNET SCAMS

As technology continues to evolve, cybercriminals will use more sophisticated techniques to exploit technology to steal your identity, personal information, and money. To protect yourself from online threats, you must know what to look for. Some of the most common Internet scams include:

- **COVID-19 Scams** take the form of emails with malicious attachments or links to fraudulent websites to trick victims into revealing sensitive information or donating to fraudulent charities or causes. Exercise caution in handling any email with a COVID-19-related subject line, attachment, or hyperlink, and be wary of social media pleas, texts, or calls related to COVID-19.
- **Imposter Scams** occur when you receive an email or call from a person claiming to be a government official, family member, or friend requesting personal or financial information. For example, an imposter may contact you from the Social Security Administration informing you that your Social Security number (SSN) has been suspended, in hopes you will reveal your SSN or pay to have it reactivated.
- **COVID-19 Economic Payments scams** target Americans' stimulus payments. CISA urges all Americans to be on the lookout for criminal fraud related to COVID-19 economic impact payments—particularly fraud using coronavirus lures to steal personal and financial information, as well as the economic impact payments themselves—and for adversaries seeking to disrupt payment efforts.

SIMPLE TIPS

- **Double your login protection.** Enable multi-factor authentication (MFA) to ensure that the only person who has access to your account is you. Use it for email, banking, social media, and any other service that requires logging in. If MFA is an option, enable it by using a trusted mobile device, such as your smartphone, an authenticator app, or a secure token—a small physical device that can hook onto your key ring.

For more information about how you can Do Your Part. #BeCyberSmart, visit **www.cisa.gov/ncsam**

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY CISA

TIA Transportation Intermediaries Association