BE CYBER SMART
#CyberMonth

CYBERSECURITY AWARENESS
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 2020 was $8.84 million[1]. That's an increase from the 2019 figure of $8.64 million.
- 7-10% of the U.S. population are victims of identity fraud each year, and 21% of those experience multiple incidents of identity fraud[2].
- In 2020, 47% of people living in the US experienced identity theft[3].

COMMON INTERNET SCAMS

As technology continues to evolve, cybercriminals will use more sophisticated techniques to exploit systems, accounts, and devices 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.

- **SHAKE UP YOUR PASSWORD PROTOCOL.** According to (National Institute of Standards and Technology (NIST) guidance, you should consider using the longest password or passphrase permissible. Get creative and customize your standard password for different sites, which can prevent cyber criminals from gaining access to these accounts and protect you in the event of a breach. Use password managers to generate and remember different, complex passwords for each of your accounts. Read the Creating a Password Tip Sheet for more information.
- **STAY UP TO DATE.** Keep your software updated with the latest version available. Maintain your security settings to keep your information safe by turning on automatic updates so you don't have to think about it, and set your security software to run regular scans

PROTECT YOURSELF FROM ONLINE FRUAD

STAY PROTECTED WHILE CONNECTED: The bottom line is that whenever you're online, you're vulnerable. If devices on your network are compromised for any reason, or if hackers break through an encrypted firewall, someone could be eavesdropping on you—even in your own home on encrypted Wi-Fi.

- Practice safe web surfing wherever you are by checking for the "green lock" or padlock icon in your browser bar—this signifies a secure connection.
- When you find yourself out in the great "wild Wi-Fi West," avoid free Internet access with no encryption.
- If you do use an unsecured public access point, practice good Internet hygiene by avoiding sensitive activities (e.g., banking) that require passwords or credit cards. Your personal hotspot is often a safer alternative to free Wi-Fi.
- Don't reveal personally identifiable information such as your bank account number, SSN, or date of birth to unknown sources.
- Type website URLs directly into the address bar instead of clicking on links or cutting and pasting from the email.

RESOURCES AVAILABLE TO YOU

If you discover that you have become a victim of cybercrime, immediately notify authorities to file a complaint. Keep and record all evidence of the incident and its suspected source. The list below outlines the government organizations that you can file a complaint with if you are a victim of cybercrime.

- **FTC.gov**: The FTC's free, one-stop resource, www.identitytheft.gov/can help you report and recover from identity theft. Report fraud to the FTC at ftc.gov/OnGuardOnline or www.ftccomplaintassistant.gov.
- **US-CERT.gov**: Report computer or network vulnerabilities to US-CERT via the hotline: 1-888-282-0870 or us-cert.cisa.gov. Forward phishing emails or websites to US-CERT at phishing-report@us-cert.gov.
- **IC3.gov**: If you are a victim of online crime, file a complaint with the Internet Crime Complaint Center (IC3) at www.IC3.gov.
- **SSA.gov**: If you believe someone is using your SSN, contact the Social Security Administration's fraud hotline at 1-800-269-0271.

CONTACT THE CISA CYBERSECURITY AWARENESS MONTH TEAM

Thank you for your continued support and commitment to Cybersecurity Awareness Month and helping all Americans stay safe and secure online. Please email our team at CyberAwareness@cisa.dhs.gov or visit http://www.cisa.gov/cybersecurity-awareness-month or staysafeonline.org/cybersecurity-awareness-month/ to learn more.

RESOURCES

1. Brook, Chris. (2020, August 18). *What Does a Data Breach Cost in 2020?* Digital Guardian. https://digitalguardian.com/blog/what-does-data-breach-cost-2020
2. Ricks, A, Irvin-Erickson, Y, PhD (2021). *Research Brief: Identity Theft and Fraud.* Center for Victim Research. https://ncvc.dspacedirect.org/bitstream/item/1228/CVR Research Syntheses_Identity Theft and Fraud_Brief.pdf
3. GIACT. (2021). *U.S. Identity Theft: The Stark Reality*. GIACT Systems, LLC.https://www.giact.com/aite-report-us-identity-theft-the-stark-reality/