



# CYBER SECURITY & YOU

FEBRUARY 2021

## 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.

### 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 emails, 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.

- **Shake Up Your Password Protocol.** 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.
- **Be up to date.** Keep your software updated to the latest version available. Maintain your security settings to keeping 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 FRAUD

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.
- 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. ■