# Identity Theft and Internet Scams

Today’s technology allows us to connect around the world, from banks and shopping online, to controlling 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 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. All Americans should 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 cybercriminals 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.

www.icscomplete.com