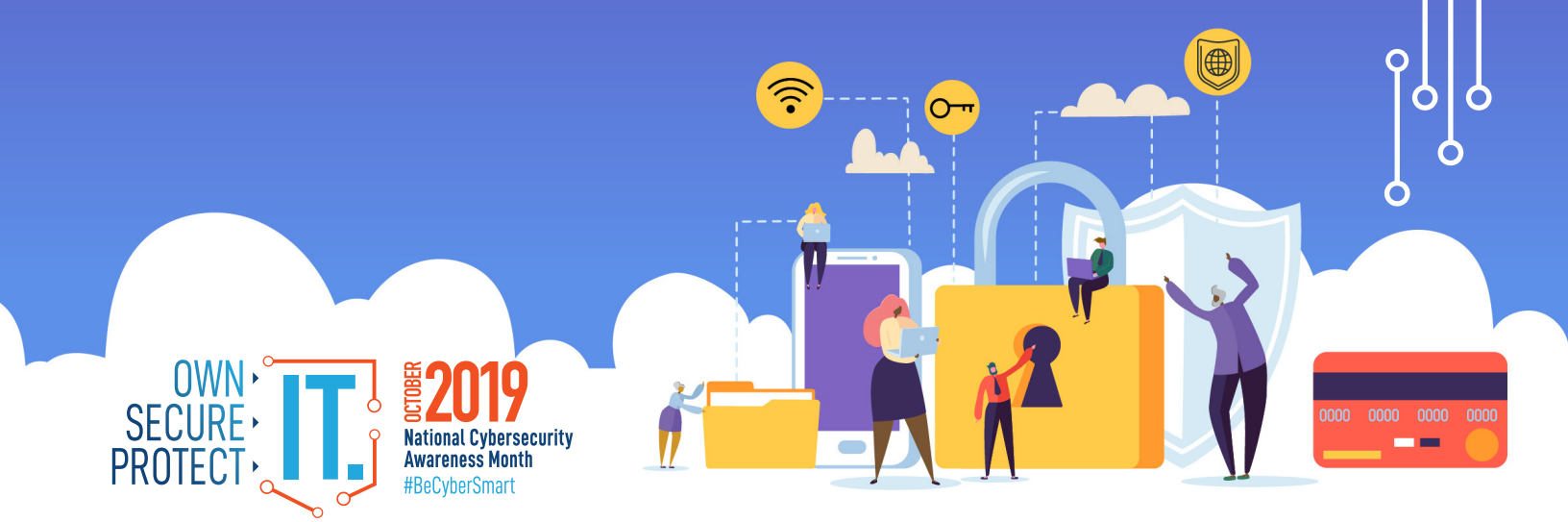


OWN IT. SECURE IT. PROTECT IT.

OCTOBER 2019
National Cybersecurity Awareness Month
#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 total number of data breaches reported in 2018 decreased 23% from the total number of breaches reported in 2017, but the reported number of consumer records containing sensitive personally identifiable information (PII) exposed increased 126%.[1]
- Credit card fraud tops the list of identity theft reports in 2018. The Federal Trade Commission (FTC) received more than 167,000 reports from people who said their information was misused on an existing account or to open a new credit card account.[2]
- Consumers reported $905 million in total fraud losses in 2017, a 21.6% increase over 2016.[3]

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. According to the FTC, these are the top three kinds of threats reported in 2018:

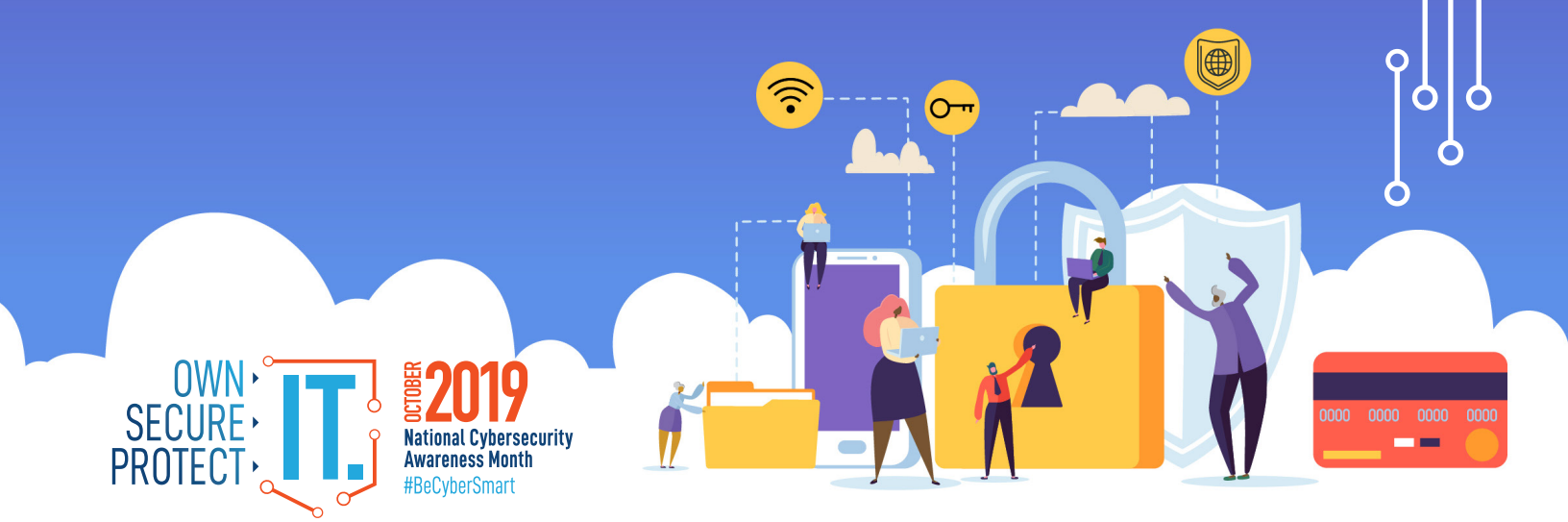
- **Identity theft** is the illegal acquisition and use of someone else's personal information to obtain money or credit. Signs of identity theft include bills for products or services you did not purchase, suspicious charges on your credit cards, or new accounts opened in your name that you did not authorize.
- **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.
- **Debt Collection scams** occur when criminals attempt to collect on a fraudulent debt. Signs the "debt collector" may be a scammer are requests to be paid by wire transfers or credit cards. In 2018 there was a spike in requests for gift cards and reloadable cards as well.

SIMPLE TIPS TO PROTECT IT.

- **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. Read the Multi-Factor Authentication (MFA) How-to-Guide for more information.

For more information about connecting with confidence visit: **https://niccs.us-cert.gov/national-cybersecurity-awareness-month-2019**

CISA | NATIONAL CYBERSECURITY ALLIANCE | CyberAware



- **Shake up your password protocol.** According to 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.
- **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

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.ftc.gov/complaint
- **US-CERT.gov:** Report computer or network vulnerabilities to US-CERT via the hotline: 1-888-282-0870 or www.us-cert.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 http://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.

[1] Identity Theft Resource Center, "2018 End-of-Year Data Breach Report", 2018.
[2] Federal Trade Commission, "Consumer Sentinel Network Data Book 2018", 2019.
[3] Experian, "Identify Theft Statistics", 2019.