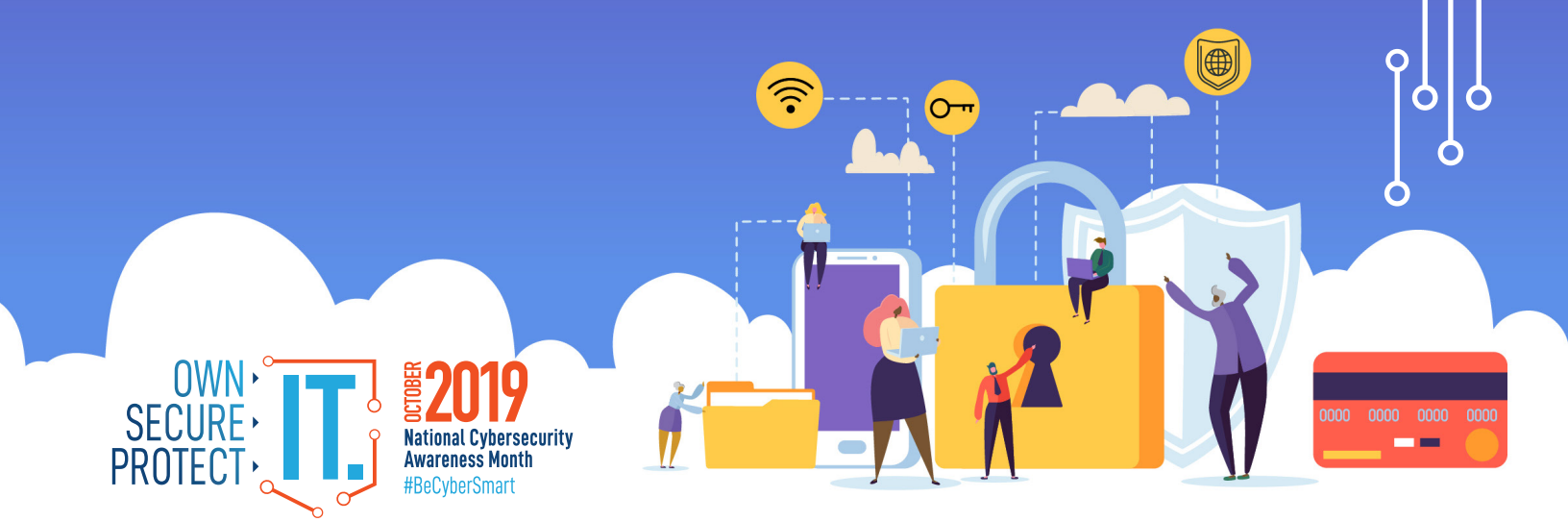

OWN IT. SECURE IT. PROTECT IT.

OCTOBER 2019
National Cybersecurity Awareness Month
#BeCyberSmart

5 WAYS TO BE CYBER SECURE AT WORK

Businesses face significant financial loss when a cyber attack occurs. In 2018, the U.S. business sector had the largest number of data breaches ever recorded: 571 breaches.[1] Cybercriminals often rely on human error—employees failing to install software patches or clicking on malicious links—to gain access to systems. From the top leadership to the newest employee, cybersecurity requires the vigilance of everyone to keep data, customers, and capital safe and secure. #BeCyberSmart to connect with confidence and support a culture of cybersecurity at your organization.

SIMPLE TIPS TO SECURE IT.

- **Treat business information as personal information.** Business information typically includes a mix of personal and proprietary data. While you may think of trade secrets and company credit accounts, it also includes employee personally identifiable information (PII) through tax forms and payroll accounts. Do not share PII with unknown parties or over unsecured networks.
- **Technology has its limits.** As "smart" or data-driven technology evolves, it is important to remember that security measures only work if used correctly by employees. Smart technology runs on data, meaning devices such as smartphones, laptop computers, wireless printers, and other devices are constantly exchanging data to complete tasks. Take proper security precautions and ensure correct configuration to wireless devices in order to prevent data breaches. For more information about smart technology see the Internet of Things Tip Card. Read the Internet of Things 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.
- **Social media is part of the fraud toolset.** By searching Google and scanning your organization's social media sites, cybercriminals can gather information about your partners and vendors, as well as human resources and financial departments. Employees should avoid oversharing on social media and should not conduct official business, exchange payment, or share PII on social media platforms. Read the Social Media Cybersecurity Tip Sheet for more information.
- **It only takes one time.** Data breaches do not typically happen when a cybercriminal has hacked into an organization's infrastructure. Many data breaches can be traced back to a single security vulnerability, phishing attempt, or instance of accidental exposure. Be wary of unusual sources, do not click on unknown links, and delete suspicious messages immediately. For more information about email and phishing scams see the Phishing Tip Sheet.

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

[1] Identity Theft Resource Center, "2018 End-of-Year Data Breach Report", 2018.

CISA | NATIONAL CYBERSECURITY ALLIANCE | CyberAware