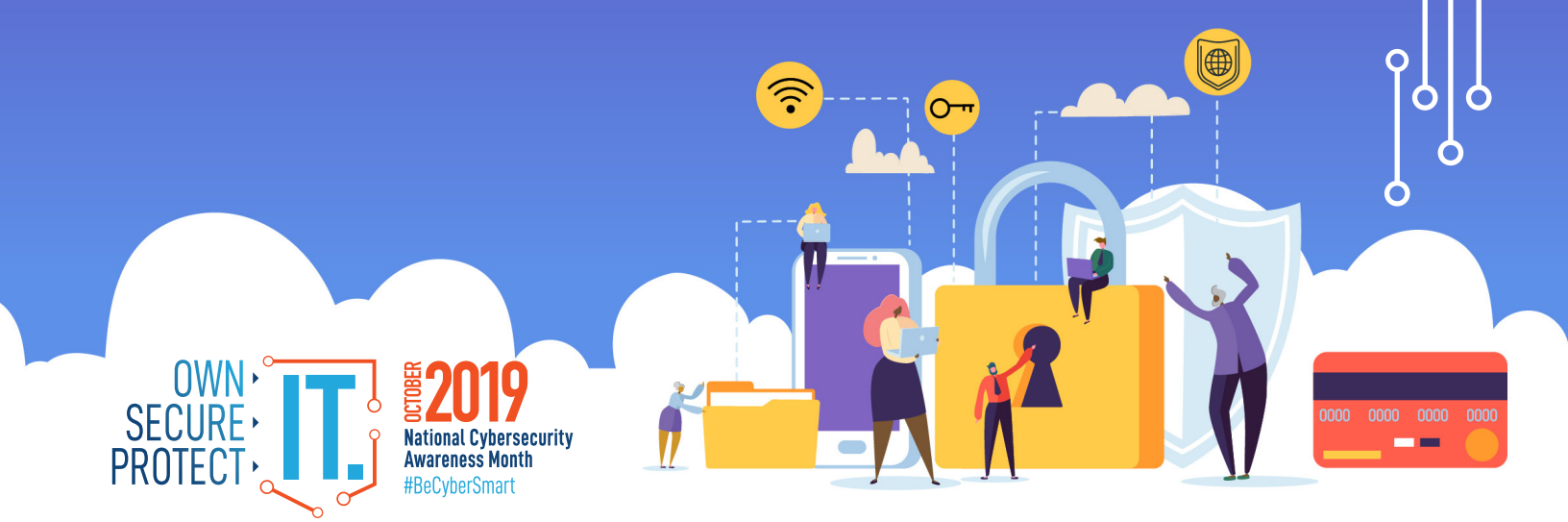


5 STEPS TO PROTECTING YOUR DIGITAL HOME

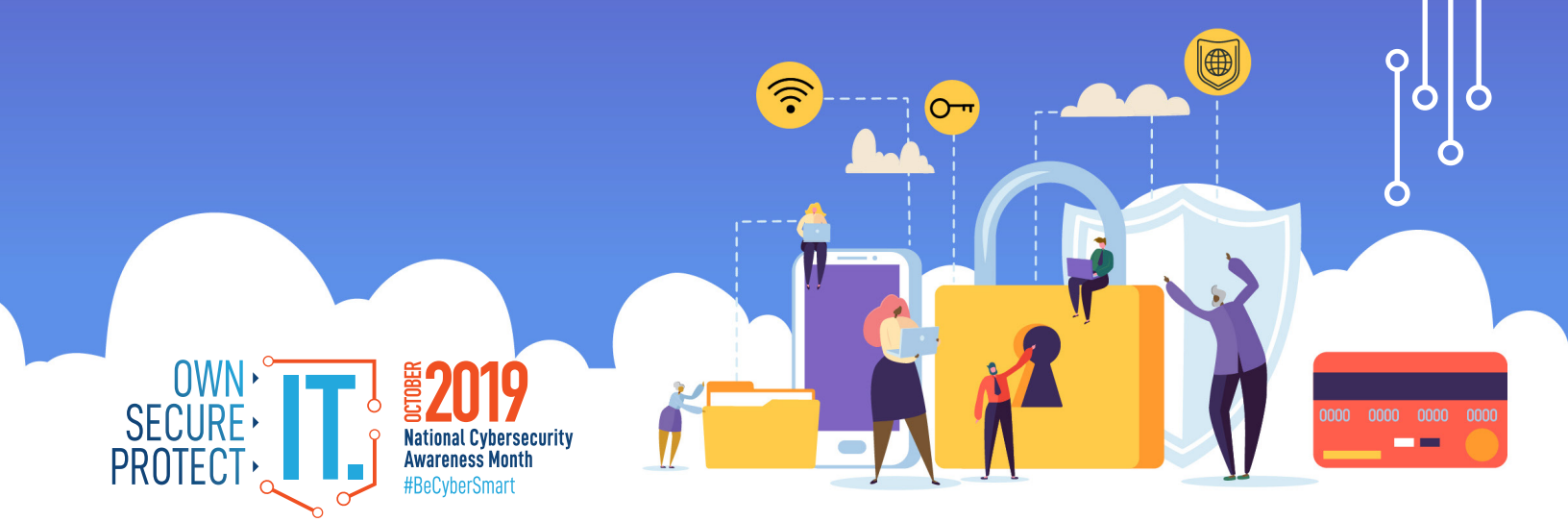
More and more of our home devices— including thermostats, door locks, coffee machines, and smoke alarms—are now connected to the Internet. This enables us to control our devices on our smartphones, no matter our location, which in turn can save us time and money while providing convenience and even safety. These advances in technology are innovative and intriguing, however they also pose a new set of security risks. #BeCyberSmart to connect with confidence and protect your digital home.

SIMPLE TIPS TO PROTECT IT.

- **Secure your Wi-Fi network.** Your home's wireless router is the primary entrance for cybercriminals to access all of your connected devices. Secure your Wi-Fi network and your digital devices by changing the factory-set default password and username. For more information about protecting your home network, check out the National Security Agency's Cybersecurity Information page.
- **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.
- **If you connect, you must protect.** Whether it's your computer, smartphone, game device, or other network devices, the best defense is to stay on top of things by updating to the latest security software, web browser, and operating systems. If you have the option to enable automatic updates to defend against the latest risks, turn it on. And, if you're putting something into your device, such as a USB for an external hard drive, make sure your device's security software scans for viruses and malware. Finally, protect your devices with antivirus software and be sure to periodically back up any data that cannot be recreated such as photos or personal documents.
- **Keep tabs on your apps.** Most connected appliances, toys, and devices are supported by a mobile application. Your mobile device could be filled with suspicious apps running in the background or using default permissions you never realized you approved—gathering your personal information without your knowledge while also putting your identity and privacy at risk. Check your app permissions and use the "rule of least privilege" to delete what you don't need or no longer use. Learn to just say "no" to privilege requests that don't make sense. Only download apps from trusted vendors and sources.
- **Never click and tell.** Limit what information you post on social media—from personal addresses to where you like to grab coffee. What many people don't realize is that these seemingly random details are all that criminals need to know to target you, your loved ones, and your physical belongings—online and in the real world. Keep Social Security numbers, account numbers, and passwords private, as well as specific information about yourself, such as your full name, address, birthday, and even vacation plans. Disable location services that allow anyone to see where you are— and where you aren't —at any given time. Read the Social Media Cybersecurity Tip Sheet 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



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

OWN IT. SECURE IT. PROTECT IT.

OCTOBER 2019
National Cybersecurity Awareness Month
#BeCyberSmart

CREATING A PASSWORD

Creating a strong password is an essential step to protecting yourself online. Using long and complex passwords is one of the easiest ways to defend yourself from cybercrime. No citizen is immune to cyber risk, but #BeCyberSmart and you can minimize your chances of an incident.

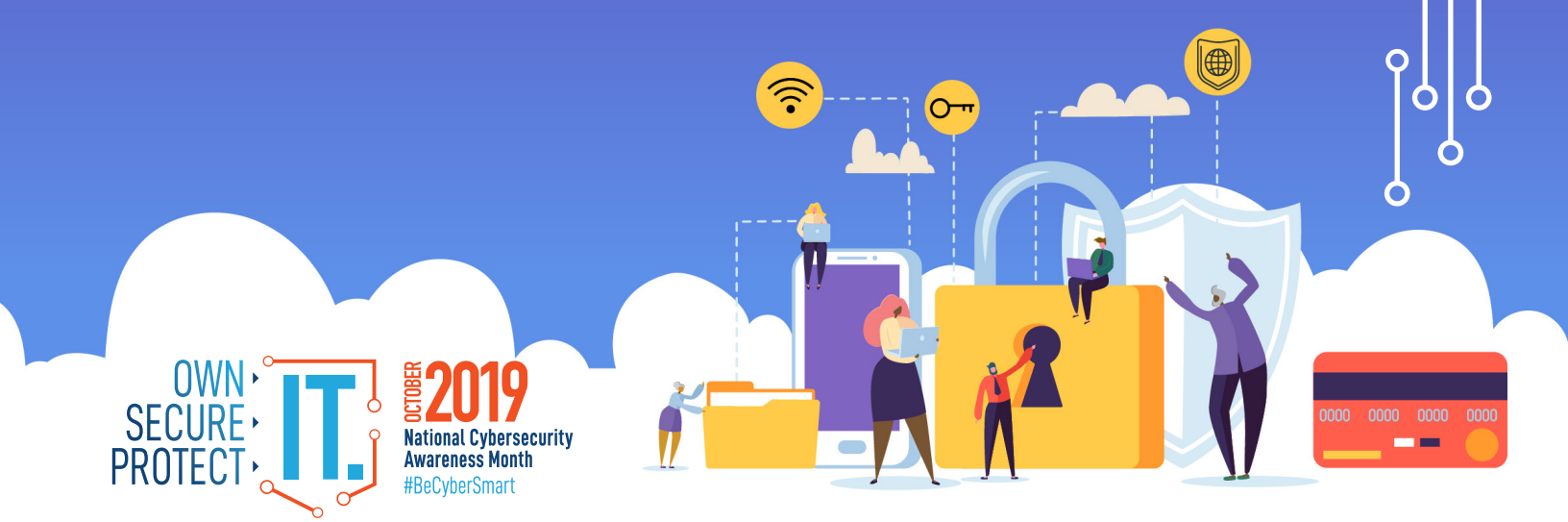
SIMPLE TIPS TO SECURE IT.

Creating a strong password is easier than you think. Follow these simple tips to shake up your password protocol:

- **Use a long passphrase**. According to NIST guidance, you should consider using the longest password or passphrase permissible. For example, you can use a passphrase such as a news headline or even the title of the last book you read. Then add in some punctuation and capitalization.
- **Don't make passwords easy to guess.** Do not include personal information in your password such as your name or pets' names. This information is often easy to find on social media, making it easier for cybercriminals to hack your accounts.
- **Avoid using common words in your password.** Substitute letters with numbers and punctuation marks or symbols. For example, @ can replace the letter "A" and an exclamation point (!) can replace the letters "I" or "L."
- **Get creative.** Use phonetic replacements, such as "PH" instead of "F". Or make deliberate, but obvious misspellings, such as "enjin" instead of "engine."
- **Keep your passwords on the down-low.** Don't tell anyone your passwords and watch for attackers trying to trick you into revealing your passwords through email or calls. Every time you share or reuse a password, it chips away at your security by opening up more avenues in which it could be misused or stolen.
- **Unique account, unique password.** Having different passwords for various accounts helps prevent cyber criminals from gaining access to these accounts and protect you in the event of a breach. It's important to mix things up—find easy-to-remember ways to customize your standard password for different sites.
- **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.
- **Utilize a password manager to remember all your long passwords.** The most secure way to store all of your unique passwords is by using a password manager. With just one master password, a computer can generate and retrieve passwords for every account that you have – protecting your online information, including credit card numbers and their three-digit Card Verification Value (CVV) codes, answers to security questions, and more.

For more tips on password creation and other ways to stay secure online visit the National Security Agency's Cybersecurity Information page.

CISA | NATIONAL CYBERSECURITY ALLIANCE | CyberAware



OWN IT. SECURE IT. PROTECT IT.

OCTOBER 2019
National Cybersecurity Awareness Month
#BeCyberSmart

CYBERSECURITY WHILE TRAVELING

In a world where we are constantly connected, cybersecurity cannot be limited to the home or office. When you're traveling—whether domestic or international—it is always important to practice safe online behavior and take proactive steps to secure Internet-enabled devices. The more we travel, the more we are at risk for cyberattacks. #BeCyberSmart and use these tips to connect with confidence while on the go.

SIMPLE TIPS TO OWN IT.

Before You Go

- **If you connect, you must protect.** Whether it's your computer, smartphone, game device, or other network devices, the best defense against viruses and malware is to update to the latest security software, web browser, and operating systems. Sign up for automatic updates, if you can, and protect your devices with anti-virus software. Read the Phishing Tip Sheet for more information.
- **Back up your information.** Back up your contacts, financial data, photos, videos, and other mobile device data to another device or cloud service in case your device is compromised and you have to reset it to factory settings.
- **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.
- **Keep it locked.** Lock your device when you are not using it. Even if you only step away for a few minutes, that is enough time for someone to steal or misuse your information. Set your devices to lock after a short time and use strong PINs and passwords. Read the Creating a Password Tip Sheet for more information.
- **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.

During Your Trip

- **Stop auto connecting.** Some devices will automatically seek and connect to available wireless networks or Bluetooth devices. This instant connection opens the door for cyber criminals to remotely access your devices. Disable these features so that you actively choose when to connect to a safe network.

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

CISA | NATIONAL CYBERSECURITY ALLIANCE | CyberAware

- **Stay protected while connected.** Before you connect to any public wireless hotspot—such as at an airport, hotel, or café—be sure to confirm the name of the network and exact login procedures with appropriate staff to ensure that the network is legitimate. 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. Only use sites that begin with "https://" when online shopping or banking.
- **Play hard to get with strangers.** Cyber criminals use phishing tactics, hoping to fool their victims. If you're unsure who an email is from—even if the details appear accurate—or if the email looks "phishy," do not respond and do not click on any links or attachments found in that email. When available use the "junk" or "block" option to no longer receive messages from a particular sender. Read the Phishing Tip Sheet for more information.
- **Never click and tell.** Limit what information you post on social media—from personal addresses to where you like to grab coffee. What many people don't realize is that these seemingly random details are all that criminals need to know to target you, your loved ones, and your physical belongings—online and in the real world. Keep Social Security numbers, account numbers, and passwords private, as well as specific information about yourself, such as your full name, address, birthday, and even vacation plans. Disable location services that allow anyone to see where you are—and where you aren't— at any given time. Read the Social Media Cybersecurity Tip Sheet for more information.
- **Guard your mobile device.** To prevent theft and unauthorized access or loss of sensitive information, never leave your equipment—including any USB or external storage devices—unattended in a public place. Keep your devices secured in taxis, at airports, on airplanes, and in your hotel room.

OWN IT. SECURE IT. PROTECT IT.

OCTOBER 2019
National Cybersecurity Awareness Month
#BeCyberSmart

A HOW-TO-GUIDE FOR MULTI-FACTOR AUTHENTICATION

SIMPLE TIPS TO SECURE IT.

Have you noticed how often security breaches, stolen data, and identity theft are consistently front-page news these days? Perhaps you, or someone you know, are a victim of cyber criminals who stole personal information, banking credentials, or more. As these incidents become more prevalent, you should consider using multi-factor authentication, also called strong authentication, or two-factor authentication. This technology may already be familiar to you, as many banking and financial institutions require both a password and one of the following to log in: a call, email, or text containing a code. By applying these principles of verification to more of your personal accounts, such as email, social media, and more, you can better secure your information and identity online!

What it is

Multifactor authentication (MFA) is defined as a security process that requires more than one method of authentication from independent sources to verify the user's identity. In other words, a person wishing to use the system is given access only after providing two or more pieces of information which uniquely identifies that person.

How it works

There are three categories of credentials: something you either know, have, or are. Here are some examples in each category.

In order to gain access, your credentials must come from at least two different categories. One of the most common methods is to login using your user name and password. Then a unique one-time code will be generated and sent to your phone or email, which you would then enter within the allotted amount of time. This unique code is the second factor.

SOMETHING YOU KNOW

- Password/Passphrase
- PIN Number

SOMETHING YOU HAVE

- Security Token or App
- Verification Text, Call, Email
- Smart Card

SOMETHING YOU ARE

- Fingerprint
- Facial Recognition
- Voice Recognition

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

CISA | NATIONAL CYBERSECURITY ALLIANCE | CyberAware

OWN SECURE PROTECT IT. OCTOBER 2019
National Cybersecurity Awareness Month
#BeCyberSmart

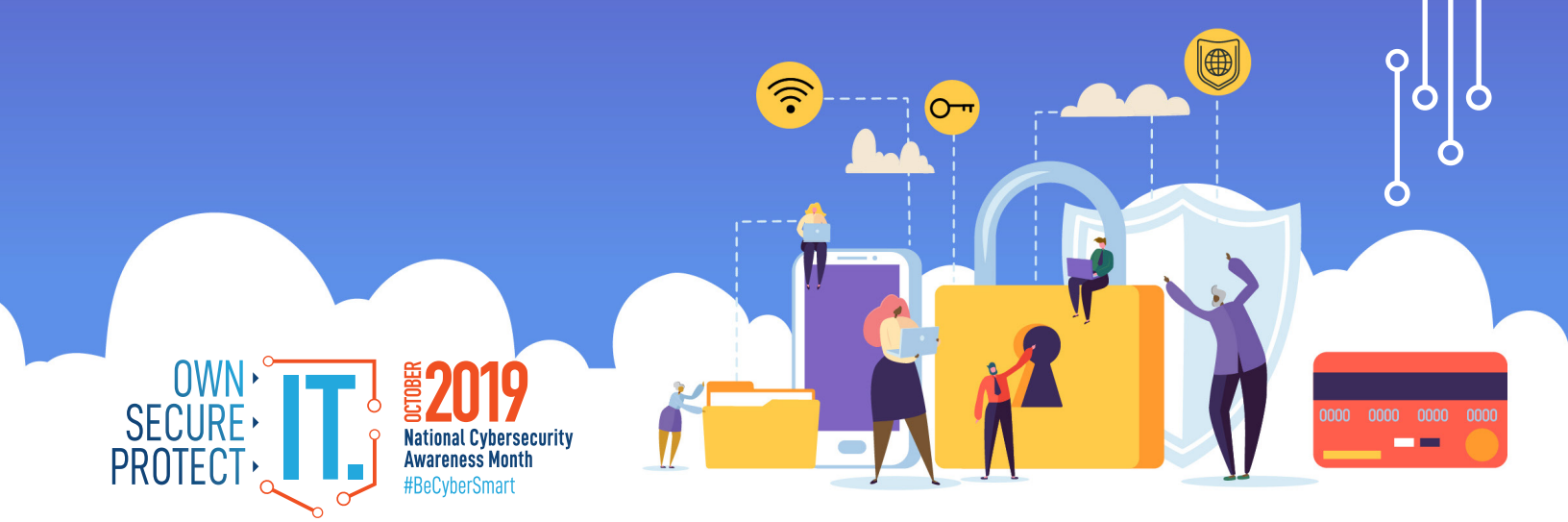
When should it be used?

MFA should be used to add an additional layer of security around sites containing sensitive information, or whenever enhanced security is desirable. MFA makes it more difficult for unauthorized people to log in as the account holder. According to the National Institute of Standards and Technology (NIST) MFA should be used whenever possible, especially when it comes to your most sensitive data—like your primary email, financial accounts, and health records. Some organizations will require you to use MFA; with others it is optional. If you have the option to enable it, you should take the initiative to do so to protect your data and your identity.

Activate MFA on your accounts right away!

To learn how to activate MFA on your accounts, head to the Lock Down Your Login site, which provides instructions on how to apply this stronger form of security to many common websites and software products you may use. If any of your accounts are not listed on that resource site, look at your account settings or user profile and check whether MFA is an available option. If you see it there, consider implementing it right away!

User names and passwords are no longer sufficient to protect accounts with sensitive information. By using multifactor authentication, you can protect these accounts and reduce the risk of online fraud and identify theft. Consider also activating this feature on your social media accounts!



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:

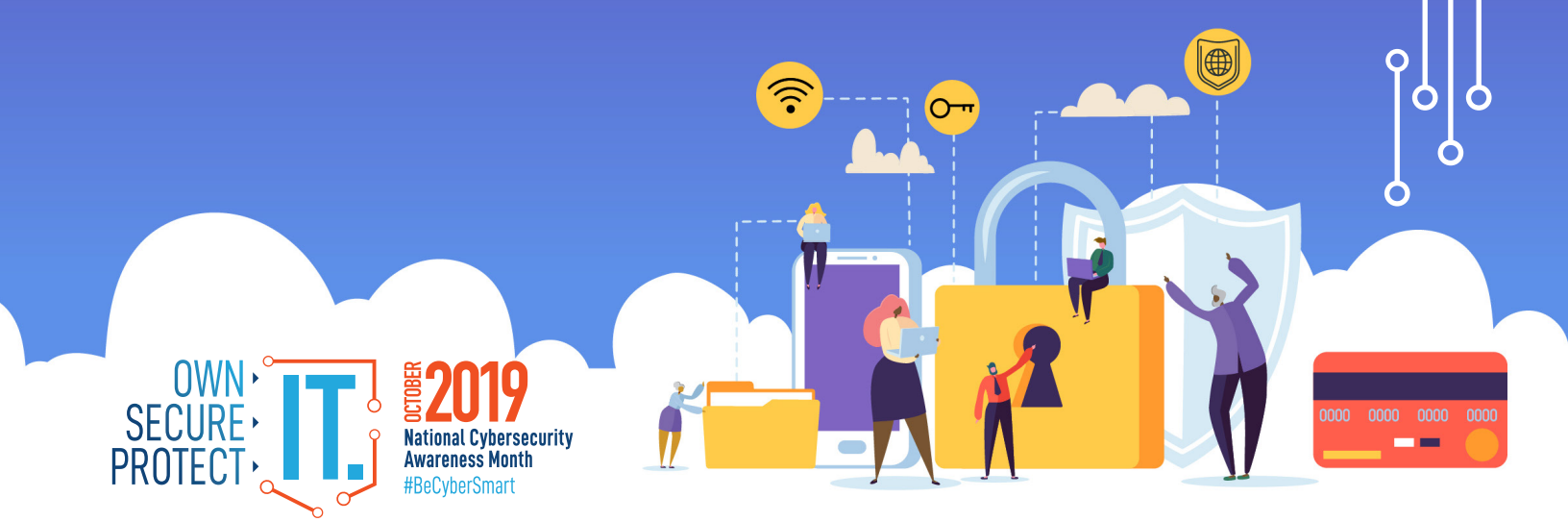
- **Identity theft** is the illegal acquisition and use of someone else's personal information to obtain money or credit. Signs of identity theft include bills for products or services you did not purchase, suspicious charges on your credit cards, or new accounts opened in your name that you did not 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.

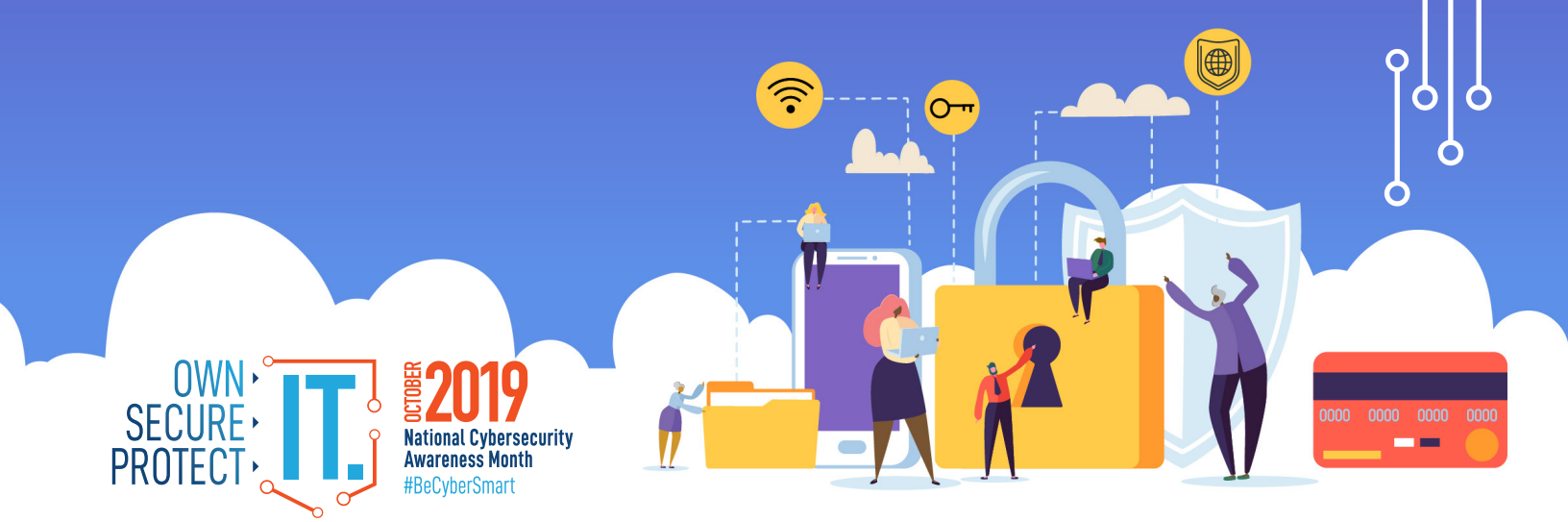
- Practice safe web surfing wherever you are by checking for the "green lock" or padlock icon in your browser bar—this signifies a secure connection.
- When you find yourself out in the great "wild Wi-Fi West," avoid free Internet access with no encryption.
- If you do use an unsecured public access 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.



OWN IT. SECURE IT. PROTECT IT.

OCTOBER 2019
National Cybersecurity Awareness Month
#BeCyberSmart

INTERNET OF THINGS

Internet of Things (IoT) or smart devices refers to any object or device that is connected to the Internet. This rapidly expanding set of "things," which can send and receive data, includes cars, appliances, smart watches, lighting, home assistants, home security, and more. #BeCyberSmart to connect with confidence and protect your interconnected world.

WHY SHOULD WE CARE?

- Cars, appliances, wearables, lighting, healthcare, and home security all contain sensing devices that can talk to another machine and trigger other actions. Examples include devices that direct your car to an open spot in a parking lot; mechanisms that control energy use in your home; and tools that track eating, sleeping, and exercise habits.
- New Internet-connected devices provide a level of convenience in our lives, but they require that we share more information than ever.
- The security of this information, and the security of these devices, is not always guaranteed. Once your device connects to the Internet, you and your device could potentially be vulnerable to all sorts of risks.
- With more connected "things" entering our homes and our workplaces each day, it is important that everyone knows how to secure their digital lives.

SIMPLE TIPS TO OWN IT.

- **Shake up your password protocol.** Change your device's factory security settings from the default password. This is one of the most important steps to take in the protection of IoT devices. According to NIST guidance, you should consider using the longest password or passphrase permissible. Get creative and create a unique password for your IoT devices. Read the Creating a Password Tip Sheet for more information.
- **Keep tabs on your apps.** Many connected appliances, toys, and devices are supported by a mobile application. Your mobile device could be filled with apps running in the background or using default permissions you never realized you approved—gathering your personal information without your knowledge while also putting your identity and privacy at risk. Check your app permissions and learn to just say "no" to privilege requests that don't make sense. Only download apps from trusted vendors and sources.
- **Secure your network.** Properly secure the wireless network you use to connect Internet-enabled devices. Consider placing these devices on a separate and dedicated network. For more information on how you can secure your network, view the National Security Agency's Cybersecurity Information page.
- **If you connect, you must protect.** Whether it's your computer, smartphone, game device, or other network devices, the best defense is to stay on top of things by updating to the latest security software, web browser, and operating systems. If you have the option to enable automatic updates to defend against the latest risks, turn it on.

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

CISA | NATIONAL CYBERSECURITY ALLIANCE | CyberAware

OWN IT. SECURE IT. PROTECT IT.

OCTOBER 2019
National Cybersecurity Awareness Month
#BeCyberSmart

ONLINE PRIVACY

The Internet touches almost all aspects of our daily lives. We are able to shop, bank, connect with family and friends, and handle our medical records all online. These activities require you to provide personally identifiable information (PII) such as your name, date of birth, account numbers, passwords, and location information. #BeCyberSmart when sharing personal information online to reduce the risk of becoming a cybercrimes victim.

DID YOU KNOW?

- 64% of U.S. adults have noticed or been notified of a major data breach affecting their sensitive accounts or personal data.[1]
- Roughly half of Americans (49%) feel that their personal information is less secure than it was five years ago.[2]
- 58% of Americans age 50 and older are more likely to feel that their personal information has become less safe in recent years: 58% of Americans in this age group express this opinion.[3]
- 69% of consumers believe companies are vulnerable to hacks and cyberattacks.[4]

SIMPLE TIPS TO OWN 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.
- **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.
- **If you connect, you must protect.** Whether it's your computer, smartphone, game device, or other network devices, the best defense against viruses and malware is to update to the latest security software, web browser, and operating systems. Sign up for automatic updates, if you can, and protect your devices with anti-virus software. Read the Phishing Tip Sheet 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

- **Play hard to get with strangers.** Cyber criminals use phishing tactics, hoping to fool their victims. If you're unsure who an email is from—even if the details appear accurate— or if the email looks "phishy," do not respond and do not click on any links or attachments found in that email. When available use the "junk" or "block" option to no longer receive messages from a particular sender.
- **Never click and tell.** Limit what information you post on social media—from personal addresses to where you like to grab coffee. What many people don't realize is that these seemingly random details are all that criminals need to know to target you, your loved ones, and your physical belongings—online and in the real world. Keep Social Security numbers, account numbers, and passwords private, as well as specific information about yourself, such as your full name, address, birthday, and even vacation plans. Disable location services that allow anyone to see where you are—and where you aren't—at any given time. Read the Social Media Cybersecurity Tip Sheet for more information.
- **Keep tabs on your apps.** Most connected appliances, toys, and devices are supported by a mobile application. Your mobile device could be filled with suspicious apps running in the background or using default permissions you never realized you approved—gathering your personal information without your knowledge while also putting your identity and privacy at risk. Check your app permissions and use the "rule of least privilege" to delete what you don't need or no longer use. Learn to just say "no" to privilege requests that don't make sense. Only download apps from trusted vendors and sources.
- **Stay protected while connected.** Before you connect to any public wireless hotspot—such as at an airport, hotel, or café—be sure to confirm the name of the network and exact login procedures with appropriate staff to ensure that the network is legitimate. 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. Only use sites that begin with "https://" when online shopping or banking.

[1] Smith, Aaron. "Americans and Cybersecurity." Pew Research Center: Internet, Science & Tech. April 27, 2017. https://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/.

[2] Ibid.

[3] Ibid.

[4] PricewaterhouseCoopers. "Consumer Intelligence Series: Protect.me." PwC. 2017. https://www.pwc.com/us/en/services/consulting/library/consumer-intelligence-series/cybersecurity-protect-me.html.

OWN IT.
SECURE IT.
PROTECT IT.

OCTOBER 2019
National Cybersecurity Awareness Month
#BeCyberSmart

PHISHING

Phishing attacks use email or malicious websites to infect your machine with malware and viruses in order to collect personal and financial information. Cybercriminals attempt to lure users to click on a link or open an attachment that infects their computers, creating vulnerability to attacks. Phishing emails may appear to come from a real financial institution, e-commerce site, government agency, or any other service, business, or individual. The email may also request personal information such as account numbers, passwords, or Social Security numbers. When users respond with the information or click on a link, attackers use it to access users' accounts.

HOW CRIMINALS LURE YOU IN

The following messages from the Federal Trade Commission's OnGuardOnline are examples of what attackers may email or text when phishing for sensitive information:

- "We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below, and confirm your identity."
- "During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."
- "Our records indicate that your account was overcharged. You must call us within 7 days to receive your refund."
- To see examples of actual phishing emails, and steps to take if you believe you received a phishing email, please visit "

SIMPLE TIPS TO SECURE IT.

- **Play hard to get with strangers.** Links in email and online posts are often the way cybercriminals compromise your computer. If you're unsure who an email is from—even if the details appear accurate—do not respond, and do not click on any links or attachments found in that email. Be cautious of generic greetings such as "Hello Bank Customer," as these are often signs of phishing attempts. If you are concerned about the legitimacy of an email, call the company directly.
- **Think before you act.** Be wary of communications that implore you to act immediately. Many phishing emails attempt to create a sense of urgency, causing the recipient to fear their account or information is in jeopardy. If you receive a suspicious email that appears to be from someone you know, reach out to that person directly on a separate secure platform. If the email comes from an organization but still looks "phishy," reach out to them via customer service to verify the communication.
- **Protect your personal information.** If people contacting you have key details from your life—your job title, multiple email addresses, full name, and more that you may have published online somewhere—they can attempt a direct spear-phishing attack on you. Cyber criminals can also use social engineering with these details to try to manipulate you into skipping normal security protocols.

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

CISA | NATIONAL CYBERSECURITY ALLIANCE | CyberAware

- **Be wary of hyperlinks.** Avoid clicking on hyperlinks in emails and hover over links to verify authenticity. Also ensure that URLs begin with “https.” The “s” indicates encryption is enabled to protect users’ information.
- **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.
- **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.
- **Install and update anti-virus software.** Make sure all of your computers, Internet of Things devices, phones, and tablets are equipped with regularly updated antivirus software, firewalls, email filters, and anti-spyware.

For more information on ways you can safeguard your information, visit the National Security Agency’s Cybersecurity Information page.

Homeland Security

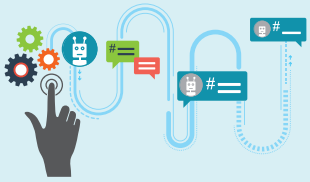
NATIONAL PROTECTION AND PROGRAMS DIRECTORATE
Office of Cyber and Infrastructure Analysis
May 2018

SOCIAL MEDIA BOTS OVERVIEW

Social Media Bot programs are common and adaptable to various social media platforms across multiple venues and areas of interest. Social Media Bot usage continues to increase on various social media platforms within the United States. As Social Media Bots increase in usage and utility, malicious behavior via Social Media Bots is also likely to increase. Recent elections in 2016 and 2017, in the United States, United Kingdom, France, and Germany, have drawn a spotlight on the nefarious activity of Social Media Bots.

OCIA defines Social Media Bots as programs that vary in size depending on their function, capability, and design; and can be used on social media platforms to do various useful and malicious tasks while simulating human behavior. These programs use artificial intelligence, big data analytics, and other programs or databases to imitate legitimate users posting content.

Automated Social Media Bots allow the user to establish a set of parameters using programming language within an application or program (e.g., retweet a specific hashtag every time it is posted, but not when the bot itself retweets it), which the Social Media Bot then executes without human interaction.



Semi-automated Social Media Bots allow a user to program a set of parameters, but may have or require additional user interaction or a greater degree of management. These types of Social Media Bots are typically fake accounts with fake personalities and are run at least partially by humans or click farms, rather than programming language.

Common Attack Methods of Social Media Bots

- **Click Farming or Like Farming** inflate fame or popularity on a website through liking or reposting of content via Click Farms, which provide fake user accounts (typically semi-automated Social Media Bots) and management of the Social Media Bots (e.g., bot herder) for purchase.
- **Hashtag Highjacking** use hashtags to focus an attack (e.g., spam, malicious links) on a specific audience using the same hashtag.
- **Repost Storm** use a parent Social Media Bot account, or martyr Social Media Bot, to initiate an attack by reposting something, which an associated group of Social Media Bots (aka botnet) instantly reposts.
- **Sleeper Bots** remain dormant for long periods of time, wake up to launch their attack of thousands of posts or retweets in a short period of time (perhaps as a Retweet Storm, or spam attack), then return to a dormant state.
- **Trend Jacking and Watering Hole Attack** use top trending topics to focus on an intended audience for targeting purposes.

Social Media Bot Uses

(Below examples are fictitious)

Commercial Activity

Social Media Bots facilitate company-to-customer relations, including selling of products or services.

ShoeTown/All

RedShoeHelp @ShoeTown
How may I help you?

Jane
I need black flats, size 7M

Counterterrorism and Terrorism

Social Media Bots allow for faster searching and detection of online activity by using foreign language search terms.

Found #più caramelle al cioccolato al latte

#più caramelle al cioccolato al latte

Search for #Besiegen

Entertainment

Social Media Bots are used on social media specifically to find, add, or create, the illusion of online fame or popularity.

Social Beats Top/All

MusicMojo@TopTunes
#LoveXYZ'sNewSong!

Sam@Mazin'O@SnapTune
#LoveXYZ'sNewSong!

Harassment

Social Media Bots can be used to overwhelm the user's account to the point of deactivation.

SRit@sueritbot #Greatreportha!

JDoe@jondoebot #Greatreportha!

JLee@janleebot #Greatreportha!

JSmith@josmithbot #Greatreportha!

Your account has been deactivated due to high volume usage.

Hate Speech

Social Media Bots can propagate hate speech on social media platforms, making the subject matter appear to gain mainstream popularity.

#Hate

#Hate

#Hate

#Hate

Information Operations

The intentional spread of propaganda to sway public opinion, limit free speech, and manipulate democratic processes and elections.

#Propaganda

#Propaganda

#Propaganda

Notifications

Social Media Bots provide automated watching capabilities to capture breaking news, ideas, or events.

AAAlert@911-AACounty
#911 Emergency Alert!

Social and Civic Engagement

Social Media Bots post to encourage and heighten civic engagement and participation.

ParadeVolunteerNow/All

DCFunHelp@VolDCPSbot
#Volunteer Day of Service@ParadeSE!

JaneS@Helpinhandsmom
Thanks signing up now!

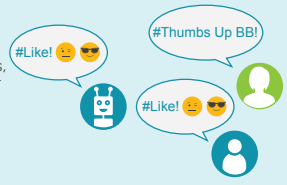
Social Media Bots Signature Behaviors

Congregation of Bots

Social Media Bots often congregate together, and act with randomness, making them easier to indentify.

Specific Content

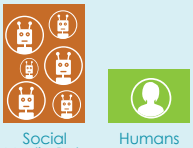
Social Media Bots tend to use emoticons, exclamation points, or other content in more regular patterns as compared to human users on social media.



Activity Levels

Social Media Bots often have higher levels of activity (typically automated Social Media Bots) as compared to human social media behavior.

Activity Level Comparison



Conclusion

Social Media Bots are becoming more prevalent and better at mimicking human behavior on social media platforms. As of 2017, technology companies are seeking investments and further incorporation of Social Media Bots into social media services and platforms, expanding "future digital communication" to provide a myriad of services as automated assistants. As Social Media Bots gain a greater foothold in social media and daily life, the potential uses, for good and malicious purposes, are ever expanding.

OWN IT. SECURE IT. PROTECT IT.

OCTOBER 2019
National Cybersecurity Awareness Month
#BeCyberSmart

SOCIAL MEDIA CYBERSECURITY

Now more than ever, consumers spend increasing amounts of time on the Internet. With every social media account you sign up for, every picture you post, and status you update, you are sharing information about yourself with the world. How can you be proactive to stay safe online and, "Own IT. Secure IT. Protect IT."? #BeCyberSmart and take these simple steps to connect with confidence and safely navigate the social media world.

DID YOU KNOW?

- 3.48 billion people worldwide now use social media worldwide. That's an increase of 9% from 2018. Put another way: 45% of the total world population are using social networks.[1]
- Digital consumers spend nearly 2.5 hours on social networks and social messaging every day.[2]
- 69% of U.S. adults use at least one social media site[3] and the average American has 7.1 social media accounts.[4]

SIMPLE TIPS TO OWN IT.

- **Remember, there is no 'Delete' button on the Internet.** Share with care, because even if you delete a post or picture from your profile seconds after posting it, chances are someone still saw it.
- **Update your privacy settings.** Set the privacy and security settings to your comfort level for information sharing. Disable geotagging, which allows anyone to see where you are—and where you aren't—at any given time.
- **Connect only with people you trust.** While some social networks might seem safer for connecting because of the limited personal information shared through them, keep your connections to people you know and trust.
- **Never click and tell.** Limit what information you post on social media—from personal addresses to where you like to grab coffee. What many people don't realize is that these seemingly random details are all that criminals need to know to target you, your loved ones, and your physical belongings—online and in the real world. Keep Social Security numbers, account numbers, and passwords private, as well as specific information about yourself, such as your full name, address, birthday, and even vacation plans. Disable location services that allow anyone to see where you are—and where you aren't—at any given time. Read the Social Media Cybersecurity Tip Sheet for more information.
- **Speak up if you're uncomfortable.** If a friend posts something about you that makes you uncomfortable or you think is inappropriate, let him or her know. Likewise, stay open-minded if a friend approaches you because something you've posted makes him or her uncomfortable. People have different tolerances for how much the world knows about them, and it is important to respect those differences. Don't hesitate to report any instance of cyberbullying you see.
- **Report suspicious or harassing activity.** Work with your social media platform to report and possibly block harassing users. Report an incident if you've been a victim of cybercrime. Local and national authorities are ready to assist you.

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

[1] Kemp, Simon. "Digital 2019: Global Digital Overview." DataReportal. January 30, 2019. https://datareportal.com/reports/digital-2019-global-digital-overview.

[2] Gwi. "Latest 2019 Social Media User Trends Report." GlobalWebIndex. 2019. https://www.globalwebindex.com/reports/social.

[3] Newberry, Christina. "130 Social Media Statistics That Matter to Marketers in 2019." Hootsuite Social Media Management. March 13, 2019. https://blog.hootsuite.com/social-media-statistics-for-social-media-managers/.

[4] Ibid.

CISA | NATIONAL CYBERSECURITY ALLIANCE | CyberAware

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY
July 2019

THE WAR ON PINEAPPLE: Understanding Foreign Interference in 5 Steps

To date, we have no evidence of Russia (or any nation) actively carrying out information operations against pizza toppings. This infographic is an ILLUSTRATION of how information operations have been carried out in the past to exploit divisions in the United States.

1. TARGETING DIVISIVE ISSUES

Foreign influencers are constantly on the lookout for opportunities to inflame hot button issues in the United States. **They don't do this to win arguments; they want to see us divided.**

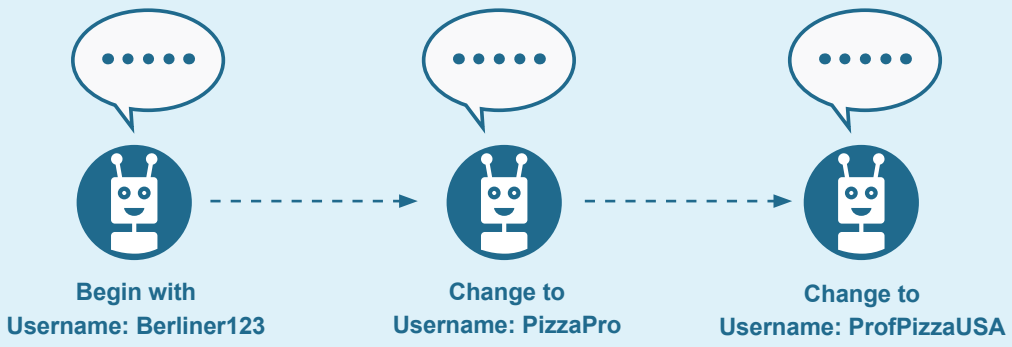
American Opinion is Split: Does Pineapple Belong on Pizza?

An A-list celebrity announced their dislike of pineapples on pizza, prompting a new survey. No matter how you slice it, Americans disagree on the fruit topping.

2. MOVING ACCOUNTS INTO PLACE

Building social media accounts with a large following takes time and resources, so accounts are often renamed and reused. Multiple accounts in a conversation are often controlled by the same user.

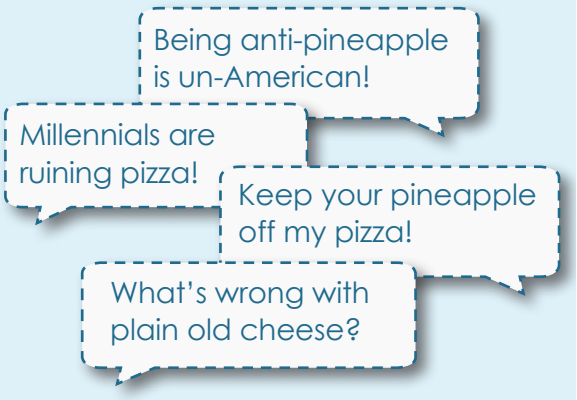
Pro Tip: Look at an account's activity history. **Genuine accounts usually have several interests and post content from a variety of sources.**



3. AMPLIFYING AND DISTORTING THE CONVERSATION

Americans often engage in healthy debate on any number of topics. Foreign influencers try to pollute those debates with bad information and make our positions more extreme by picking fights, or "trolling" people online.

Pro Tip: Trolls try to make people mad, that's it. **If it seems like an account is only aiming to raise tensions, think about whether it's worth engaging.**



4. MAKING THE MAINSTREAM

Foreign influencers "fan the flames" by creating controversy, amplifying the most extreme version of arguments on both sides of an issue. These are shared online as legitimate information sources.

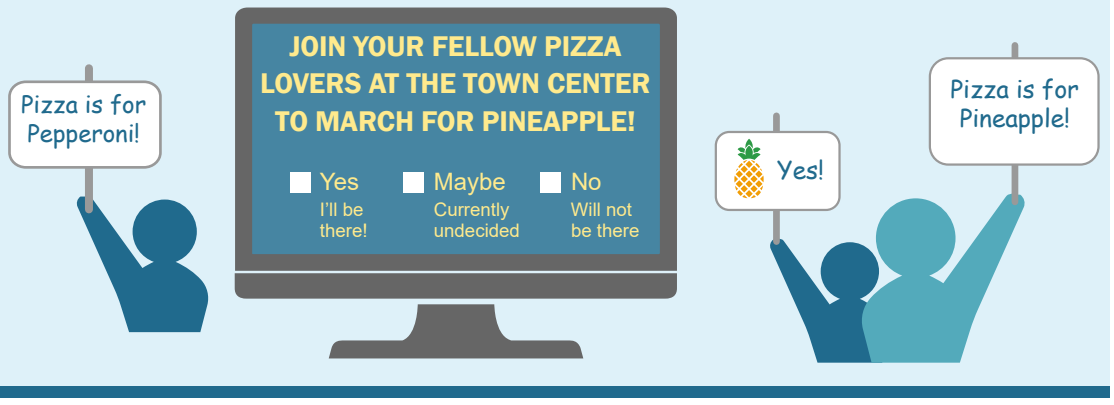
Sometimes controversies make it into the mainstream and create division among Americans. **This is a foreign influencer striking gold! Their meddling is legitimized and carried to larger audiences**.

5. TAKING THE CONVERSATION INTO THE REAL WORLD

In the past, Kremlin agents have organized or funded protests to further stoke divisions among Americans. They create event pages and ask followers to come out.

What started in cyberspace can turn very real, with Americans shouting down Americans because of foreign interference.

Pro Tip: Many social media companies have increased transparency for organization accounts. **Know who is inviting you and why.**



For more information, please visit the #Protect2020 website at https://www.dhs.gov/cisa/protect2020.