SESSION 1: RISK MANAGEMENT

OCTOBER 13, 2020
IN THIS PRESENTATION

- Company Overview
- Series Overview
- Why Training
- Human Element
- Key Terms

COMPANY OVERVIEW: TILLMAN CYBER SERVICES, LLC

Service-Disabled Veteran, Minority-Owned Small Business

Over 40 Years of Combined IT, Cybersecurity & Risk Management Experience

COMPANY OVERVIEW: CAPABILITIES

- Cyber Vulnerability Assessment & Remediation
- Intrusion Detection & Incident Response
- Cyber Forensics
- Encryption
- Network Traffic Analysis
- Policy & Procedure Development
COMPANY OVERVIEW: CAPABILITIES
- Virtualization
- Network Development & Implementation
- Classified Computing Environment
- Server Management
- Programming & Scripting
- Technical Documentation

IN THIS PRESENTATION
- Company Overview
- **Series Overview**
- Why Training
- Human Element
- Key Terms

TRAINING SERIES OVERVIEW
- Backup Strategies
- Information Security
- Network Protection
- User Behavior
- Risk Management
- Document Development
WHY TRAINING

“Two key mistakes small companies make that leave them vulnerable to cyber attacks are they assume they won’t be targeted, and they don’t provide any cybersecurity training for their employees.”

- Cyrus Walker, Managing Principal, Data Defenders

WHY TRAINING

- Raise awareness about cybersecurity’s importance
- Help keep data from bad actors
- Understand reality of socially engineering
- Understand and learn steps to mitigate risks
- Reduce volume and impact of attacks
- No program leads to 100% success
“Ransomware is more about manipulating vulnerabilities in human psychology than the adversary’s technological sophistication.”

- James Scott, Sr. Fellow, Institute for Critical Infrastructure Technology
“94% of malware is delivered by email.”

“Phishing is the #1 type of social engineering attack, accounting for 80% of reported incidents.”

- CSO Online

HUMAN ELEMENT – 8 MOST COMMON CAUSES OF DATA BREACH

- Weak and Stolen Passwords
- Social Engineering
- Too Many Permissions
- Improper Configuration
- Insider Threats
- User Error
- Application Vulnerabilities
- Malware
“People always make the best exploits. I’ve never found it hard to hack most people. If you listen to them, watch them, their vulnerabilities are like a neon sign screwed into their heads.”

- Elliot Alderson, Mr. Robot

IN THIS PRESENTATION

• Company Overview
• Series Overview
• Why Training
• Human Element
• Key Terms

KEY TERMS: CYBERSECURITY

“The art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.”

- U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA)
KEY TERMS: INFORMATION SECURITY

- Cyber-Security
- Operational Security
- Contingency Planning & Disaster Recovery
- Physical Security
- Privacy
- Personnel Security

KEY TERMS: CYBER ATTACK VS. DATA BREACH

DATA BREACH
Unauthorized movement or disclosure of sensitive information that...
May or may not interfere with normal business operations

CYBER ATTACK
Intends to interfere with normal business operations by manipulating, disrupting, or deleting data.

KEY TERMS: BAD ACTOR/HACKER
Person or nation-state seeking to exploit weaknesses in software and computer systems to create data breaches and/or cyber attacks for their own gain.
KEY TERMS: MALICIOUS CYBER ACTIVITY

- Malware
- PII
- Ransomware
- Social Engineering
- Phishing

IN THIS PRESENTATION

- Cyber Attack Impacts & Stats
- COVID-19 Based Attacks
- Cyber Attack Examples
- Risk Management Model
- Risk Assessment Approach

CYBER ATTACK IMPACT AND STATISTICS

“There are two kinds of people in American today: Those who have experienced a cyber-attack and know it, and those who have experienced a cyber attack and don’t know it.”

- Frank Wolf
What percentage of online attacks are aimed at small businesses?

a) 27%  b) 43%  c) 61%  d) 89%

Percentage of online attacks aimed at small businesses

What percentage of small businesses suffered a breach in the last year?

a) 25%  b) 50%  c) 75%  d) 100%
CYBER ATTACK IMPACT AND STATISTICS

Percentage of small businesses that have suffered a breach within the last year:

31%

What is the average cost of a cyberattack to a business?

- a) $50,000
- b) $100,000
- c) $200,000
- d) $500,000

32

Average cost of cyberattacks to businesses of all sizes:

$____,____

33
CYBER ATTACK IMPACT AND STATISTICS

What percentage of companies go out of business after a cyberattack?

a) 30%  
b) 40%  
c) 50%  
d) 60%

---

Percentage of companies that go out of business within six months of being victimized

---

What percentage of small business leaders don't think they are cyber targets?

a) 44%  
b) 55%  
c) 66%  
d) 77%
Percentage of senior decision-makers at small businesses who think they are unlikely to be targeted by online criminals

What percentage of small businesses are prepared to defend themselves?

a) 14%  b) 34%  c) 56%  d) 78%
CYBER ATTACK IMPACT AND STATISTICS

The COVID-19 Environment

- 667% increase in COVID-19 phishing attacks
- Scammers preying on coronavirus fears
- Fake links, emails, texts, social media posts
- Phony promotions of awareness & prevention
- Requests to donate to victims
- Bogus product offerings and treatment advice

In This Presentation

- Cyber Attack Impacts & Stats
- COVID-19 Based Attacks
- Cyber Attack Examples
- Risk Management Model
- Risk Assessment Approach
Dear citizen,

<who_int@protonmail.ch>
Orders of our President Tedros Adhanom and his august office.

COVID-19 PHISHING EXAMPLE

- COVID-19 outbreak has reached epidemic proportions
- Conventional health care strategies have failed in containing the disease
- The future of healthcare systems looks bleak as the strain on these systems is becoming unbearable
- The office of our president is monitoring the situation and will issue periodic updates on the situation

I am hereby requesting you to download the attached...
KEY TERMS: COVID 19 PHISHING EXAMPLE

You will also get a free WHO NCOVID healthcare kit if you sign and share this document over the next 15 hours.

IN THIS PRESENTATION

• Cyber Attack Impacts & Stats
• COVID-19 Based Attacks
• Cyber Attack Examples
• Risk Management Model
• Risk Assessment Approach

CYBER ATTACK EXAMPLES
CYBER ATTACK EXAMPLES: 2013 TARGET DATA BREACH

- 41 Million Customers Affected
- Cost Target $18.5 Million
- Hackers gained access to Target’s network by infiltrating one of its business relationships, a small HVAC company.

CYBER ATTACK EXAMPLES: SHIPPING COMPANIES

- MAERSK (2017)
- COSCO SHIPPING (JUL 2018)
- MSC (APR 2020)
- CMA CGM (SEP 2020)

CYBER ATTACK EXAMPLES: FACEBOOK & YAHOO

- 540 Million Use Records Exposed
- Cost Facebook between $1B-$5B in Fines
- 3 Billion Customer Accounts Affected
- Cost Yahoo $350 Million
IN THIS PRESENTATION
- Cyber Attack Impacts & Stats
- COVID-19 Based Attacks
- Cyber Attack Examples
- Risk Management Model
- Risk Assessment Approach

RISKS MANAGEMENT MODEL

THREATS
- Environmental
- Business Resources
- Hackers/Criminals

VULNERABILITIES
- Weakness in security protections

LIKELIHOOD – CHANCE OF THREAT AFFECTING THE BUSINESS
- Occurrence based on history/industry statistics
- For adversarial threats: Capability & Intent

IMPACT – POTENTIAL HARM TO THE BUSINESS
- Theft or disclosure of sensitive business information
- Business information or systems being modified
- The loss of information or system availability

WHAT IS YOUR RISK?
- 41% of online attacks aimed at small businesses
- 50% of small businesses suffered a cyber breach in the last year
- $200,000 is the average cost of cyberattack to all businesses
- 66% of decision makers do not believe they are targets
- 60% of businesses suffering an attack go out of business within 6 months

The loss of information or system availability

$200,000 is the average cost of cyberattack to all businesses

41% of online attacks aimed at small businesses
IN THIS PRESENTATION

- Cyber Attack Impacts & Stats
- COVID-19 Based Attacks
- Cyber Attack Examples
- Risk Management Model
- Risk Assessment Approach

RISK ASSESSMENT APPROACH

1. Periodically assess risk to organizational operations
2. Scan for vulnerabilities
3. Remediate Vulnerabilities

RISK ASSESSMENT APPROACH

1. Periodically identify and prioritize risks
2. Develop and implement risk mitigation plans
3. Manage non-vendor-supported products separately and restrict as necessary
RISK ASSESSMENT APPROACH

- Catalog and periodically update threat profiles
- Employ threat intelligence
- Perform scans for unauthorized ports across network perimeter
- Develop and update a plan for managing IT supply chain risks

Utilize an exception process for non-whitelisted software

Analyze the effectiveness of security solutions at least annually

SUMMARY

“The five most efficient cyber defenders are: Anticipation, Education, Detection, Reaction and Resilience. Do remember: Cybersecurity is much more than an IT topic.”

- Stephane Nappo
SUMMARY

- Create a Culture around Cybersecurity
- Assume You are a Target
- Be Vigilant
- Train Your Employees
- Assess, Identify, Plan, Mitigate

SUMMARY: CYBER SECURITY MONTH

DO YOUR PART.
#BECYBERSMART

THANK YOU!

SESSION 2: INFORMATION SECURITY
THURSDAY, OCTOBER 15, 2020
11:30 AM
Reducing your organization's cyber risks requires a holistic approach - similar to the approach you would take to address other operational risks. As with other risks, cyber risks can threaten:

- Your ability to operate / access info
- Your reputation / customer trust
- Your bottom line
- Your organization's survival

Managing cyber risks requires building a culture of cyber readiness.

**Essential Elements** of a *Culture of Cyber Readiness*:

**Yourself** - The Leader

- Drive cybersecurity strategy, investment and culture
  - Your awareness of the basics drives cybersecurity to be a major part of your operational resilience strategy, and that strategy requires an investment of time and money.
  - Your investment drives actions and activities that build and sustain a culture of cybersecurity.

**Your Staff** - The Users

- Develop security awareness and vigilance
  - Your staff will often be your first line of defense, one that must have - and continuously grow - the skills to practice and maintain readiness against cybersecurity risks.

**Your Systems** - What Makes You Operational

- Protect critical assets and applications
  - Information is the life-blood of any business; it is often the most valuable of a business' intangible assets.
  - Know where this information resides, know what applications and networks store and process that information, and build security into and around these.

**Your Data** - What the Business is Built On

- Make backups and avoid the loss of information critical to operations
  - Even the best security measures can be circumvented with a patient, sophisticated adversary. Learn to protect your information where it is stored, processed, and transmitted.
  - Have a contingency plan, which generally starts with being able to recover systems, networks, and data from known, accurate backups.

**Your Actions Under Stress**

- Limit damage and quicken restoration of normal operations
  - The strategy for responding to and recovering from compromise: plan, prepare for, and conduct drills for cyberattacks as you would a fire. Make your reaction to cyberattacks and system failures an extension of your other business contingency plans.
  - This requires having established procedures, trained staff, and knowing how - and to whom - to communicate during a crisis.
Organizations living the culture have:
- Led investment in basic cybersecurity.
- Determined how much of their operations are dependent on IT.
- Built a network of trusted relationships with sector partners and government agencies for access to timely cyber threat information.
- Approached cyber as a business risk.
- Led development of cybersecurity policies.

Organizations living the culture have:
- Leveraged basic cybersecurity training to improve exposure to cybersecurity concepts, terminology and activities associated with implementing cybersecurity best practices.
- Developed a culture of awareness to encourage employees to make good choices online.
- Learned about risks like phishing and business email compromise.
- Identified available training resources through professional associations, academic institutions, private sector and government sources.
- Maintained awareness of current events related to cybersecurity, using lessons-learned and reported events to remain vigilant against the current threat environment and agile to cybersecurity trends.

Organizations living the culture have:
- Learned what is on their network. Maintained inventories of hardware and software assets to know what is in-play and at-risk from attack.
- Leveraged automatic updates for all operating systems and third-party software.
- Implemented secure configurations for all hardware and software assets.
- Removed unsupported or unauthorized hardware and software from systems.
- Leveraged email and web browser security settings to protect against spoofed or modified emails and unsecured webpages.
- Created application integrity and whitelisting policies so that only approved software is allowed to load and operate on their systems.

Organizations living the culture have:
- Learned who is on their network. Maintained inventories of network connections (user accounts, vendors, business partners, etc.).
- Leveraged multi-factor authentication for all users, starting with privileged, administrative and remote access users.
- Implemented secure configurations for all hardware and software assets.
- Granted access and admin permissions based on need-to-know and least privilege.
- Leveraged unique passwords for all user accounts.
- Developed IT policies and procedures addressing changes in user status (transfers, termination, etc.).

Organizations living the culture have:
- Established regular automated backups and redundancies of key systems.
- Learned how their data is protected.
- Leveraged malware protection capabilities.
- Leveraged protections for backups, including physical security, encryption and offline copies.
- Learned what is happening on their network. Managed network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities.

Organizations living the culture have:
- Led development of an incident response and disaster recovery plan outlining roles and responsibilities. Test it often.
- Leveraged business impact assessments to prioritize resources and identify which systems must be recovered first.
- Learned who to call for help (outside partners, vendors, government / industry responders, technical advisors and law enforcement).
- Led development of an internal reporting structure to detect, communicate and contain attacks.
- Leveraged in-house containment measures to limit the impact of cyber incidents when they occur.
CISA INSIGHTS
Risk Management for Novel Coronavirus (COVID-19)

The Threat and How to Think About It
This product is for executives to help them think through physical, supply chain, and cybersecurity issues that may arise from the spread of Novel Coronavirus, or COVID-19. According to the U.S. Centers for Disease Control and Prevention (CDC), COVID-19 has been detected in locations around the world, including multiple areas throughout the U.S. This is a rapidly evolving situation and for more information, visit the CDC’s COVID-19 Situation Summary.

COVID-19 Risk Profile
On March 11, the COVID-19 outbreak was characterized as a pandemic by the WHO. The virus that causes COVID-19 is infecting people and spreading easily from person-to-person. Cases have been detected in most countries worldwide and community spread is being detected in a growing number of countries.

In anticipation of a broader spread of COVID-19, globally and within the United States, organizations should plan for continued impacts to their workforce and operations.

CISA’s Role as the Nation’s Risk Advisor
The Cybersecurity and Infrastructure Security Agency (CISA) is working closely with partners to prepare for possible impacts of a COVID-19 outbreak in the United States. COVID-19 containment and mitigation strategies will rely heavily on healthcare professionals and first responders detecting and notifying government officials of occurrences.

CISA will use its relationships with interagency and industry partners to facilitate greater communication, coordination, prioritization and information-sharing between the private sector and the government.

As the situation changes, the virus may affect essential operations for businesses and federal, state, local, tribal, and territorial (SLTT) government entities.

To stay current with CISA’s efforts regarding the COVID-19, visit: cisa.gov/coronavirus.

Additional Information:
Visit the CDC website, or contact CDC for COVID-19-related issues or to share critical and timely information by sending an email to eocjiclead2@cdc.gov and eocjictriage2@cdc.gov or by calling 1-800-232-4636.
Actions for Infrastructure Protection

Planning and preparedness are critical to reducing the impact of COVID-19 on the Critical Infrastructure community and CISA recommends taking the following precautions to prepare for possible impacts from COVID-19:

- **Designate** a response coordinator and assign team members with specific responsibilities.
- **Implement** a formal worker and workplace protection strategy.
- **Train** workers on personal and worksite protection strategies.
- **Establish** and test flexible worksite (e.g., telework) and work hour policies.

Identify essential functions, goods, and services your organization requires to sustain its own operations and mission.

- **Determine** how long your organization can expect to continue providing essential functions, goods, and services in potentially reduced quantities.
- **Identify and prioritize** suppliers of critical products and services for your organization.
- **Continuously assess** ongoing preparedness activities to adjust objectives, effects, and actions based on changes in the business and greater economic and social environments.
- **Monitor** federal, state, local, tribal and territorial COVID-19 information sites for up-to-date information on containment and mitigation strategies.

Actions for your Supply Chain

- **Assess** your organization’s supply chain for potential impacts from disruption of transport logistics and international manufacturing slowdowns resulting from COVID-19.
- **Discuss** with those suppliers any challenges they may be facing or may expect to face due to the ongoing situation.

Identify potential alternate sources of supply, substitute products, and/or conservation measures to mitigate disruptions.

Communicate with key customers to keep them informed of any issues you have identified and the steps you are taking to mitigate them.

Cybersecurity for Organizations

As organizations explore various alternate workplace options in response to COVID-19, CISA recommends examining the security of information technology systems by taking the following steps:

- **Secure** systems that enable remote access.
  - **Ensure** Virtual Private Network and other remote access systems are fully patched.
  - **Enhance** system monitoring to receive early detection and alerts on abnormal activity.
  - **Implement** multi-factor authentication.

Ensure all machines have properly configured firewalls, as well as anti-malware and intrusion prevention software installed.

Test remote access solutions capacity or increase capacity.

Ensure continuity of operations plans or business continuity plans are up to date.

Increase awareness of information technology support mechanisms for employees who work remotely.

Update incident response plans to consider workforce changes in a distributed environment.

Cybersecurity Actions for your Workforce and Consumers

Malicious cyber actors could take advantage of public concern surrounding COVID-19 by conducting phishing attacks and disinformation campaigns. Phishing attacks often use a combination of email and bogus websites to trick victims into revealing sensitive information. Disinformation campaigns can spread discord, manipulate the public conversation, influence policy development, or disrupt markets.

CISA encourages individuals to guard against COVID-19-related phishing attacks and disinformation campaigns by taking the following precautions:

- **Avoid** clicking on links in unsolicited emails and be wary of email attachments.

Do not reveal personal or financial information in emails, and do not respond to email solicitations for this information.

Review CISA’s Tip on Avoiding Social Engineering and Phishing Scams for more information on recognizing and protecting against phishing.

Review the Federal Trade Commission’s blog post on coronavirus scams for information on avoiding COVID-19 related scams.

Use trusted sources—such as legitimate, government websites—for up-to-date, fact-based information about COVID-19.
COVID-19 Disinformation Activity

False and misleading information related to the coronavirus (COVID-19) are a significant challenge. This CISA Insight provides an overview of coronavirus disinformation and steps that can be taken to reduce the risk of sharing inaccurate information with your friends and family.

COVID-19 DISINFORMATION

After the initial outbreak of COVID-19, disinformation campaigns appeared online. Information manipulation and fabrication about COVID-19’s origin, scale, government response, and/or prevention and treatment surged as creators leveraged people’s increased uncertainty.

Virus Origin

China and other authoritarian governments have promoted false claims about the origins of the virus in an attempt to shift blame overseas and divide free societies against themselves. Common tactics they use include censoring news, injecting false narratives onto social media platforms, and promoting slick government-produced videos.

Virus Scale

Chinese state-backed media continue to promote content emphasizing China’s claimed success rapidly controlling the virus, while suggesting the U.S. and other Western countries have failed in their response. These narratives are amplified on a variety of social media platforms.

5G and COVID

Disinformation campaigns have promoted false narratives that 5G technology suppresses immune systems and that 5G spectrum bands spread the virus.

Government Response to COVID-19

Disinformation involving the government’s response to COVID-19 has been circulated to cause confusion among Americans, including false claims the National Guard Bureau would be supporting nationwide quarantines.

Prevention and Treatment of COVID-19

False information about COVID-19 treatments continue to circulate on social media, including potentially extremely harmful suggestions to drink bleach or chlorine dioxide, to use vitamin C or boiled garlic, or that illicit drug activity can “cure” the virus.

PROTECT YOURSELF

There are simple steps you can take to minimize the likelihood of amplifying disinformation.

1. Go to trusted sources of information like www.Coronavirus.gov. FEMA has also established a coronavirus rumor control website at www.FEMA.gov/coronavirus/rumor-control where you can learn more about specific disinformation campaigns.

2. Check the source of the information.

3. Search for other reliable sources of information on the issue.

4. Think before you link – take a moment to let your emotions cool down before sharing anything online.

CISA’S ROLE AS THE NATION’S RISK ADVISOR

CISA collaborates with industry and government partners to help organizations understand and counter critical infrastructure and cybersecurity risks associated with the malicious activities of nation-state and non-state actors. CISA provides recommendations to help partners stay vigilant and protected against potential foreign influence operations.

Contact Information:

CISA.gov has more information about COVID-19, as well as information on identifying and combating disinformation. We ask that anyone with any relevant information, or indication of a compromise, contact us immediately.
CISA INSIGHTS

ACTIONS TO COUNTER EMAIL-BASED ATTACKS ON ELECTION-RELATED ENTITIES

SEPTEMBER 10, 2020

THE THREAT AND HOW TO THINK ABOUT IT

Malicious cyber actors have been known to use sophisticated phishing operations to target political parties and campaigns, think tanks, civic organizations, and associated individuals. Email systems are the preferred vector for initiating malicious cyber operations. Recent reporting shows 32 percent of breaches involve phishing attacks, and 78 percent of cyber-espionage incidents are enabled by phishing.\(^1\),\(^2\)

Cyber actors launching phishing attacks often seek to entice users to do one of three things.

- Click on a link and turn over credentials (username and password), so the cyber actor can gain access to an account.
- Open an attachment or click a link that delivers the cyber actor’s malware.
- Click a link to a website that the cyber actor monitors; this verifies that the email account is valid for subsequent targeting.

Cyber actors can also use credential-based techniques to gain access to accounts in various ways.

- Password spraying attacks rely on cyber attackers using a commonly used password against multiple usernames.
- Brute-force attacks rely on cyber attackers knowing the username and attempting several passwords.
- Credential stuffing attacks rely on cyber attackers using usernames and password combinations gained from data breaches against other accounts.

To protect against these attacks, the Cybersecurity and Infrastructure Security Agency (CISA) strongly recommends organizations involved in any election-related activities prioritize the protection of accounts from email-based attacks by:

- Using provider-offered protections, if utilizing cloud email.
- Securing user accounts on high value services.
- Implementing email authentication and other best practices.
- Securing email gateway capabilities.

WHEN USING CLOUD EMAIL, USE PROVIDER-OFFERED PROTECTIONS

Organizations that use cloud email providers should enable various protections their provider offers.

a. Require multi-factor authentication (MFA) for all user email accounts.
   - Use either physical security keys (such as those following the FIDO2 standard) or authentication apps (such as those following the TOTP algorithm).
     - Physical security keys offer protection against phishing attacks by working as a second, physical factor of authentication and only authenticating when a user is on the correct

---

\(^1\) Verizon 2019 Data Breach Investigation Report, [https://enterprise.verizon.com/resources/reports/dbir/](https://enterprise.verizon.com/resources/reports/dbir/)

website. Thus, even if a user is tricked into supplying their password to a phishing website, the physical security key will still block attackers from accessing their account.

- Authentication apps work by having a user enter a code from an app. Although authentication apps can still be vulnerable to phishing attacks, they offer more protection than SMS or email-based MFA.
  - Only use SMS and email-based MFA methods if other forms of MFA are unavailable. SMS and email-based MFA methods are vulnerable to phishing and SIM swap attacks, though they still offer better protection than password-based single-factor authentication.

b. When available, enroll user accounts in advanced protection services.
  - These services provide the highest level of protection against phishing and other attacks, applying robust filtering techniques, with many requiring physical security keys. For instance, Google offers an Advanced Protection service for all users, and Microsoft offers an Advanced Threat Protection service. Google also offers an Enhanced Account Protection service at no cost to at-risk election-related organizations. Note: CISA includes these references with the intention of highlighting the types of services available; doing so does not constitute endorsement of any particular company or service.

SECURE USER ACCOUNTS ON HIGH-VALUE SERVICES

Protect individual accounts on high-value services to mitigate the impact of a successful phishing attack.

a. Enroll in a password manager service for your organization and encourage employees to use it.
  - Password managers protect against phishing by generating secure, random passwords and automatically filling passwords when visiting websites. Password managers will not automatically enter passwords on malicious websites, giving employees a crucial cue that they should not proceed.

b. Require MFA for user accounts on all high-value services when possible.
  - If possible, deploy physical security keys for access to high-value services.
  - After physical keys, authentication app-based MFA (TOTP) is the next safest option, followed by SMS and email-based MFA. Use SMS and email-based MFA only when no other MFA options are available.
  - If a high-value service does not support any form of MFA, consider switching to a similar service that does offer MFA.

c. Eliminate unnecessary password composition and rotation requirements in favor of secure, human-friendly requirements.
  - Recent research shows that excessive password requirements (such as including special characters or numbers) tend to cause user frustration and may reduce security. Consider adopting password requirements to match guidance from the National Institute of Standards and Technology (NIST) in Special Publication 800-63B, which recommends long, human-friendly, memorable passwords (e.g., sequences of several words).

d. Consider registering your organization for a password breach monitoring service.
  - Password reuse is a leading cause of account compromise. Attackers often use breached credentials to attempt to access other services for which the victim may have reused credentials. In addition to encouraging use of password managers to reduce password reuse, organizations should consider monitoring password breaches for exposed employee credentials. Several vendors offer password breach monitoring services and will send notifications to an organization if employee passwords appear in a data breach.

---

IMPLEMENT EMAIL AUTHENTICATION AND OTHER BEST PRACTICES

Implement email authentication and other best practices to reduce attackers' ability to send spoofed phishing emails originating from your organization. For additional guidance, refer to CISA Binding Operational Directive (BOD) 18-01.

a. Enable STARTTLS.
   ➢ When enabled by a receiving mail server, STARTTLS signals to a sending mail server that the capability to encrypt an email in transit is present. While it does not force the use of encryption, enabling STARTTLS makes on-path attacks more difficult.

b. Disable outdated protocols and ciphers.
   ➢ Ensure that outdated, insecure protocols—such as SSLv2 and SSLv3—as well as 3DES and RC4 ciphers are disabled on mailing servers.

c. Implement SPF and DKIM.4
   ➢ SPF and DKIM allow a sending domain to effectively “watermark” their emails, making unauthorized emails (e.g., spam, phishing email) easy to detect.

d. Configure a DMARC policy of “reject”, if possible, or at minimum, “p=none”.5
   ➢ When an email is received that does not pass an organization’s posted SPF/DKIM rules, DMARC tells the recipient what the domain owner would like done with the message.
   ➢ Setting a DMARC policy of “reject” provides the strongest protection against spoofed email, ensuring that unauthenticated messages are rejected at the mail server, even before delivery. Additionally, DMARC reports provide a mechanism for an organization to be made aware of the source of an apparent forgery—information that they would not normally receive otherwise. Multiple recipients can be defined for the receipt of DMARC reports.

SECURE EMAIL GATEWAY CAPABILITIES

Organizations operating their own email gateways should secure email gateways, appliances, and services to intercept phishing emails.

a. Deploy an email filter solution that screens based on headers and malicious content (e.g., infected attachments), categorizes email, inspects Uniform Resource Locators (URLs) against reputation feeds, and has customizable rule-based filters.

b. Strip and/or block emails containing active content (e.g., ActiveX, Java, Visual Basic for Applications [VBA]), or macros) by default. Administrators should allowlist such content only for legitimate reasons.

c. Consider reformatting hyperlinks in the body of email messages by rewriting URLs as plaintext.

d. Deploy sandboxing or detonation chambers to safely isolate malicious links.

e. Ensure detection signatures and blocklists are up to date.

f. Block email beyond a certain size and/or containing attachments that exceed a certain size.
   ➢ Consider legitimate needs to receive large file sizes and limit file size to suit organizational need.

g. Block certain file extensions—including unknown or unused attachments that should not typically be transmitted over email—to prevent vectors such as .scr, .exe, .pif, and .cpl.

---

➢ To the extent feasible, filter out mislabeled file extensions, for example, an executable (.exe) file labeled as a document (.doc) file.

h. Open and analyze compressed and encrypted formats, such as .zip and .rar, that attackers may use to conceal malicious attachments in obfuscated files or information. If unable to open and analyze such content, consider blocking encrypted .zip and other files. However, blocking attachments might keep legitimate files from reaching recipients, which may hinder business functions. Consider using workarounds, such as allowlisting (e.g., trusted senders), to limit negative impacts to operations.

➢ Consider removing the encrypted content from the message and putting it in an out-of-band delivery solution (e.g., web-based portal), replacing the content with a token/link in the original message.

i. Ensure all email gateways, appliances, or services are configured to use only approved Domain Name System (DNS) resolvers and forwarders.

j. Consider implementing warning banners to alert users about emails (particularly those with links and attachments) that originate from outside the organization (place trusted domains on your allowlist to reduce unnecessary implementation).
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:

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 passwords.** 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.
E-SKIMMING

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.

WHAT IS IT?
Cyber criminals introduce skimming code on e-commerce payment card processing web pages to capture credit card and personally identifiable information and send the stolen data to a domain under their control.

HOW DOES IT WORK?
Skimming code is introduced to payment card processing websites by:

- Exploiting a vulnerability in the website’s e-commerce platform
- Gaining access to the victim’s network through a phishing email or brute force of administrative credentials
- Compromising third-party entities and supply chains by hiding skimming code in the JavaScript loaded by the third-party service onto the victim website
- Cross site scripting which redirects customers to a malicious domain where malicious JavaScript code captures their information from the checkout page

The malicious code captures credit card data as the end user enters it in real time. The information is then sent to an Internet-connected server using a domain name controlled by the actor. Subsequently, the collected credit card information is either sold or used to make fraudulent purchases.

WHO IS BEING TARGETED?
Any business accepting online payments on their website is at risk of an e-Skimming attack. This threat has impacted e-commerce companies in the retail, entertainment, and travel industries as well as utility companies and third-party vendors. E-Skimming is also commonly targeting third-party vendors such as those who provide online advertisements and web analytics. The cyber criminals are evolving their tactics and have also been seen using malicious code that targets user and administrative credentials in addition to customer payment information.
WHAT ARE THE WARNING SIGNS?
- Complaints of fraudulent activity on several customers’ accounts after making a purchase from victim company
- Identifying a new domain not known to be registered by victim company
- JavaScript code has been edited

HOW CAN YOU MINIMIZE RISK?
The FBI recommends taking precautionary measures to mitigate the threat of e-Skimming attacks. In an attempt to make attribution, the FBI determined the malicious skimmer code has varied in complexity, which limits the ability to identify a specific set of indicators of compromise. Vulnerable companies should secure websites to prevent malicious code injection. In addition, companies should implement proper network segmentation and segregation to limit network exposure and minimize lateral movement of cyber criminals.
- Perform regular updates to payments software
- Install patches from payment platform vendors
- Implement code integrity checks
- Keep anti-virus software updated
- Ensure you are PCI DSS compliant
- Monitor and analyze web logs
- Refer to your Incident Response Plan, if applicable

WHAT CAN YOU DO IF YOU ARE A VICTIM?
- Identify source of skimming code to determine access point - network, third party, or other
- Save a copy of skimming script or malicious loader domain to report to law enforcement
- Change pertinent credentials
- Refer to your Incident Response Plan, if applicable
- File a detailed complaint at www.IC3.gov and review additional resources under the “Press Room” link
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 and “Do Your Part. #BeCyberSmart”? Take these simple steps to connect with confidence and safely navigate the social media world.

Why Should We Care?

• Cars, appliances, fitness trackers and other wearables, lighting, healthcare, home security, and more 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

• **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 IT, Protect IT.** 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.
A HOW-TO-GUIDE FOR MULTI-FACTOR AUTHENTICATION

SIMPLE TIPS:
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 IS IT
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 how you can Do Your Part, BeCyberSmart, visit www.cisa.gov/ncsam
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 identity theft. Consider also activating this feature on your social media accounts!
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?

• 45% of Americans have had their personal information compromised by a data breach in the last five years. ¹
• 70% of Americans feel that their personal information is less secure than it was five years ago², up from 49% just two years ago.³
• 72% of Americans believe that most of what they’re doing while online is being tracked by advertisers, technology firms and other companies.²
• Over half of Americans (52%) say they have decided not to use a product or service because they were worried about how much personal information was being collected about them.²

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

• **Shake up your password protocol.** Use 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.

• **Keep 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 IT, Protect IT.** 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.
DO YOUR PART.
#BECYBERSMART

• **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.

---


Ibid.

Ibid.

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:

- **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.

- **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](http://www.nsa.gov) page.
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 and “Do Your Part. #BeCyberSmart”? Take these simple steps to connect with confidence and safely navigate the social media world.

Did You Know?

• In 2020 3.81 billion people worldwide now use social media worldwide. That’s an increase of more than 9% from 2019. Put another way: 49% 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

Simple Tips

• **If You Connect IT, Protect IT.** 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.

• **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.

• **Speak up if you’re uncomfortable.** If a friend posts something about you that makes you uncomfortable or you think is inappropriate, let them 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 help you.

• **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.


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 **average cost of a data breach** for a US company in 2019 was $8.19 million? That’s an increase of 130% since 2006!
- **7-10%** of the U.S. population are victims of identity fraud each year, and 21% of those experience multiple incidents of identity fraud.

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 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. 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. 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 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.


• [IC3.gov](https://www.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](http://www.IC3.gov).

• [SSA.gov](https://www.ssa.gov): If you believe someone is using your SSN, contact the Social Security Administration’s fraud hotline at 1-800-269-0271.

For more information about how you can Do Your Part. #BeCyberSmart, visit [www.cisa.gov/ncsam](http://www.cisa.gov/ncsam).
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**

**Before You Go**

- **If You Connect IT, Protect IT.** 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.

- **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.

- **Keep 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.

- **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.

- **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 devices.** 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.

For more information about how you can Do Your Part. #BeCyberSmart, visit [www.cisa.gov/ncsam](http://www.cisa.gov/ncsam)
5 WAYS TO BE CYBER SECURE AT WORK

Businesses face significant financial loss when a cyber attack occurs. In 2019, the U.S. business sector had a 17% increase in data breaches: 1,473 breaches. 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:

1. **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.

2. **Don’t make passwords easy to guess.** 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.

3. **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.

4. **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 oversharining 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.

5. **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 how you can Do Your Part. #BeCyberSmart, visit [www.cisa.gov/ncsam](http://www.cisa.gov/ncsam)
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

• **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 how you can Do Your Part. #BeCyberSmart, visit www.cisa.gov/ncsam