COMPANY OVERVIEW: TILLMAN CYBER SERVICES, LLC

Service-Disabled Veteran, Minority-Owned Small Business

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

EMAIL: CONTACT@TILLMANCYBER.COM

ADDRESS: 1314 MADEIRA DR. SE / SUITE C-2 / ALBUQUERQUE, NM 87108

PHONE: (505) 688-4726

WEB: WWW.TILLMANCYBER.COM

COMPANY OVERVIEW: CAPABILITIES

Cyber Vulnerability Assessment & Remediation

Intrusion Detection & Incident Response

Cyber Forensics

Encryption

Network Traffic Analysis

Policies & Procedures Development

VIRTUALIZATION

Network Development & Implementation

Classified Computing Environment

Server Management

Programming & Scripting

Technical Documentation

IN THIS PRESENTATION

• Company Overview
• Physical Security

• Series Overview
• Contingency Planning & Disaster Recovery

• Risk Recap
• Operational Security

• Information Security Model
• Personnel Security

• Privacy
• Cybersecurity
Trainings Overview

- Raise awareness about cybersecurity’s importance
- Help keep data from bad actors
- Understand reality of socially engineering
- Understand steps to mitigate risks
- Reduce volume and impact of attacks
- No program leads to 100% success

In This Presentation

- Company Overview
- Series Overview
- Risk Recap
- Information Security Model
- Privacy
- Physical Security
- Contingency Planning & Disaster Recovery
- Operational Security
- Personnel Security
- Cybersecurity
RISK RECAP

THREATS
43% of online attacks aimed at small businesses

VULNERABILITIES
66% of decision makers do not believe they are targets. 14% of businesses are prepared.

LIKELIHOOD – CHANCE OF THREAT AFFECTING THE BUSINESS
50% of small businesses suffered a cyber breach in the last year. A typical firm experiences 130 breaches per year.

IMPACT – POTENTIAL HARM TO THE BUSINESS
$200,000 is the average cost of cyberattack to all businesses. 60% of businesses suffering an attack go out of business within 6 months.

WHAT IS YOUR RISK?

Priority 3 – Schedule a resolution. Focus on Respond and Recover solutions.

Priority 1 – Implement immediate resolution. Focus on Detect and Protect solutions.

Priority 2 – Schedule a resolution. Focus on Detect and Protect solutions.

No action needed

Name the company that was breached when hackers gained access to its systems through one of its business relationships, a small HVAC company.

a) Maersk  b) Equifax  c) Facebook  d) Target
Name the company that was breached when hackers gained access to its systems through one of its business relationships, a small HVAC company.

a) Maersk  b) Equifax  c) Facebook  d) Target

What percentage of small businesses are prepared to defend themselves against cyber attacks?

a) 78%  b) 56%  c) 14%  d) 34%
**RISK RECAP**

What is the priority when the risk likelihood is high and the impact is high?

a) No Action  
b) Priority 1  
c) Priority 2  
d) Priority 3

---

**RISK RECAP**

Attacks utilizing false emails, chats, phone calls or websites designed to impersonate a legitimate communication in order to convince you to click a link, download a file or provide your personal information.

a) Phishing  
b) Malware  
c) PII  
d) Hacker
RISK RECAP

Attacks utilizing false emails, chats, phone calls or websites designed to impersonate a legitimate communication in order to convince you to click a link, download a file or provide your personal information.

a) Phishing  b) Malware  c) PII  d) Hacker

RISK RECAP

A variation of malware that causes damage to a computer system and then demands money to restore it to working order.

a) Kidnapware  b) Malware  c) Ransomware  d) Hostageware

RISK RECAP

A variation of malware that causes damage to a computer system and then demands money to restore it to working order.

a) Kidnapware  b) Malware  c) Ransomware  d) Hostageware
IN THIS PRESENTATION

- Company Overview
- Series Overview
- Risk Recap
- Information Security Model
- Privacy
- Physical Security
- Contingency Planning & Disaster Recovery
- Operational Security
- Personnel Security
- Cybersecurity

INFORMATION SECURITY

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Confidentiality

Integrity

Availability
Protecting personal information

- Full name
- Home address
- Email address
- Telephone number
- Credit/Debit Card/Bank Account numbers
- Date of birth

- Social Security Number
- Driver’s License
- Passport Number
- Taxpayer ID Number
- Any State-Issue ID Number
- Biometric Records
IN THIS PRESENTATION

- Company Overview
- Series Overview
- Risk Recap
- Information Security Model
- Privacy
- Physical Security
- Contingency Planning & Disaster Recovery
- Operational Security
- Personnel Security
- Cybersecurity

INFORMATION SECURITY: PHYSICAL SECURITY

The protection of property, for example, using fences, locks, etc.
INFORMATION SECURITY: PHYSICAL SECURITY

- Limit physical access to organizational information systems
- Protect and monitor the physical facility
- Escort visitors and monitor visitor activity
- Maintain audit logs of physical access
- Control and manage physical access devices
- Enforce safeguarding measures at alternate work sites

HUMAN ELEMENT

“Hardware is easy to protect: lock it in a room, chain it to a desk, or buy a spare. Information poses more of a problem. It can exist in more than one place; be transported halfway across the planet in seconds; and be stolen without your knowledge.”

- Bruce Schneier, Protect Your Macintosh, 1994

IN THIS PRESENTATION

- Company Overview
- Series Overview
- Risk Recap
- Information Security Model
- Privacy
- Physical Security
- Contingency Planning & Disaster Recovery
- Operational Security
- Personnel Security
- Cybersecurity
Also known as Business Continuity Planning, the resuming of normal operations following an incident.

- Test/engage disaster recovery plan
- Contact appropriate stakeholders
- Test/recover backed up data
- Continuously improve processes, procedures & technologies
- Consider cyber insurance
Statistically, something will happen whether it’s accidental, environmental or malicious.

“We will bankrupt ourselves in the vain search for absolute security.”
- Dwight D. Eisenhower

IN THIS PRESENTATION
- Company Overview
- Series Overview
- Risk Recap
- Information Security Model
- Privacy
- Physical Security
- Contingency Planning & Disaster Recovery
- Operational Security
- Personnel Security
- Cybersecurity
IN THIS PRESENTATION

- Company Overview
- Series Overview
- Risk Recap
- Information Security Model
- Privacy
- Physical Security
- Contingency Planning & Disaster Recovery
- Operational Security
- Personnel Security
- Cybersecurity

INFORMATION SECURITY: PERSONNEL SECURITY

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

Using background checks for employees
Screen individuals prior to authorizing access to systems
Conduct full, nationwide, criminal background checks
Ensure systems are protected during and after terminations
“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)
This part of information security focusses on background checks for new employees and protecting information when employees are terminated.

a) Privacy  b) Physical  c) Personnel  d) Cybersecurity

This type of information security sets clear guidelines on what is allowed and not allowed. It clearly defines the responsibilities and authorization, as well as disciplinary actions in case of breaches.

a) Privacy  b) Cybersecurity  c) Personnel  d) Operational
**SUMMARY QUIZ**

This type of information security sets clear guidelines on what is allowed and not allowed. It clearly defines the responsibilities and authorization, as well as disciplinary actions in case of breaches.

a) Privacy  b) Cybersecurity  c) Personnel  d) Operational

---

**SUMMARY QUIZ**

This type of information security focuses on protecting credit card, bank account, driver's license and social security numbers.

a) Privacy  b) Cybersecurity  c) Personnel  d) Physical

---

**SUMMARY QUIZ**

This type of information security focuses on protecting credit card, bank account, driver's license and social security numbers.

a) Privacy  b) Cybersecurity  c) Personnel  d) Physical
SUMMARY QUIZ

**Resuming normal business after a cyber incident would be greatly aided with this part of the information security model.**

a) Disaster Recovery  
b) Physical Security  
c) Crossing Fingers  
d) Taking a Vacation

When you leave for lunch, you lock documents in the file cabinets, turn off your computer and secure it to your desk, and lock your office door. This is...

a) Disaster Recovery  
b) Physical Security  
c) Privacy  
d) Personnel Security
When you leave for lunch, you lock documents in the file cabinets, turn off your computer and secure it to your desk, and lock your office door. This is...

- a) Disaster Recovery
- b) Physical Security
- c) Privacy
- d) Personnel Security

SUMMARY

Create a Culture around Cybersecurity
Assume You are a Target
Develop an Information Security Plan
Be Vigilant about Implement the Plan
Train Employees to Follow Information Security Plan
Incentivize Employees to Follow Plan
Assess, Identify, Plan, Mitigate

SUMMARY: CYBER SECURITY MONTH

DO YOUR PART.
#BECYBERSMART
SUMMARY: NEXT SESSION

SESSION 3: USER BEHAVIOR
THURSDAY, OCTOBER 20, 2020
11:30 AM

THANK YOU!

TILLMAN CYBER SERVICES, LLC
AMERICA'S SBDC
NEW MEXICO
The real threats posed by trusted insiders

Cybersecurity measures are frequently focused on threats outside an organization, rather than threats posed by untrustworthy individuals inside an organization. In fact, well-publicized insiders have caused irreparable harm to their organizations, as well as national security interests. An insider threat can be defined as the potential violation of system security policy by an authorized user. Although policy violations can be the result of carelessness or accident, the core concern is deliberate and intended actions such as malicious exploitation, theft, or destruction of data; or the compromise of networks, or other information technology (IT) resources.

A research portfolio to aggressively curtail elements of Insider Threat

The U.S. Department of Homeland Security (DHS) Science and Technology Directorate (S&T) Cyber Security Division’s (CSD) Insider Threat project is developing solutions that compliment and expand the capabilities of existing commercial insider threat tools. In many systems, the integrity, availability, and total system survivability are of the highest priority and can be compromised by insiders. S&T CSD’s research includes a project with Northrop Grumman focusing on the exfiltration of data residing in a database management system. CSD is working with Carnegie Mellon University/Software Engineering Institute to develop insider threat case studies based on investigative casework.

Given the universal challenges presented by insiders, this research area considers the global problem and is partnering with the United Kingdom (UK) Centre for the Protection of National Infrastructure to complement ongoing research programs and allow collaboration among researchers.

Another important element of the Insider Threat project is the development of a freely available research dataset for researchers to test their tools. Generating test data in this space is time consuming for academics and small companies, so S&T is developing a collection of insider threat data that will be made available for use by the entire community.

In fiscal year 2015, DHS S&T participated within the Enduring Security Framework Insider Threat Working Group, a DHS/NSA-led partnership between the private sector and government agencies to develop a comprehensive insider threat program using technology and analytics within modern, cloud-based architectures.

Organizations will have a more complete approach to the insider threat problem

Current, widely implemented insider threat detection tools provide capabilities to inform operational use, however they are not considered to be a complete solution. The research conducted through this project will focus on elements that are not currently available via commercial tools. In doing so, S&T’s work in this space will benefit a wide range of potential customers including national security bodies, government officials who need controlled unclassified information, healthcare, finance, and many other critical infrastructure sectors where sensitive and valuable information is managed.

Performers

- Northrop Grumman/Purdue University
- Carnegie Mellon University/Software Engineering Institute
- Massachusetts Institute of Technology – Lincoln Labs

To learn more about Insider Threat, contact Megan Mahle, Program Manager, at SandT-Cyber-Liaison@HQ.DHS.GOV.
Privacy at DHS

DHS empowers its programs to succeed by integrating privacy protections from the outset. The DHS Privacy Office is the first statutorily mandated privacy office in the Federal Government, and serves a unique role as both an advisor and oversight body for the Department.

DHS views privacy as more than just compliance with privacy law and policy. Privacy at DHS is also about public trust and confidence, and how the government acts responsibly and transparently in the way it collects, maintains, and uses personally identifiable information (PII).

DHS employs a layered approach to privacy oversight for the Department’s cybersecurity activities. It starts with the Chief Privacy Officer and extends through NPPD’s Senior Privacy Officer and dedicated privacy staff across the Department.

The Fair Information Practice Principles

DHS uses the Fair Information Practice Principles (FIPPs) to guide and inform the design, deployment, compliance, and oversight of all its programs and technologies. In 2008, DHS formalized these principles as department policy:

1. **Transparency**: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII.

2. **Individual Participation**: DHS should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. DHS should also provide mechanisms for appropriate access, correction, and redress regarding DHS’s use of PII.

3. **Purpose Specification**: DHS should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.

4. **Data Minimization**: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).

5. **Use Limitation**: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.

6. **Data Quality and Integrity**: DHS should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.

7. **Security**: DHS should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

8. **Accountability and Auditing**: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

These principles were also adopted as part of the National Strategy for Trusted Identity in Cyberspace (NSTIC) and the 2013 Executive Order 13636, “Improving Critical Infrastructure Cybersecurity.”

Transparency

DHS publishes its Privacy Impact Assessments (PIAs), Privacy Compliance Reviews (PCRs), and other reports on [www.dhs.gov/privacy](http://www.dhs.gov/privacy), the DHS Privacy Office’s webpage. DHS also created a separate site dedicated to the Department’s cybersecurity efforts, which includes its privacy work on cybersecurity: [www.dhs.gov/cybersecurity](http://www.dhs.gov/cybersecurity).
Privacy Impact Assessments

As part of its privacy compliance responsibilities, DHS conducts PIAs. PIAs provide an opportunity for the Department to identify privacy issues early in the development process and to build privacy protections into programs from the beginning.

DHS has conducted PIAs on all stages of the Department’s EINSTEIN program as well as other cybersecurity programs:

- EINSTEIN 1, 2004
- EINSTEIN 2, 2008
- National Cybersecurity Protection System (NCPS), 2012
- Enhanced Cybersecurity Services (ECS), 2015
- EINSTEIN 3 Accelerated, 2016
- Automated Indicator Sharing (AIS), 2016
- Continuous Diagnostics and Mitigation (CDM), 2016

Each PIA describes the particular program and analyzes privacy risks according to a standard set of considerations, from data collection, use, and retention to information sharing, notice, and safeguarding.

Oversight

DHS reinforces privacy compliance through a separate oversight process to assess performance of the privacy requirements established through PIAs and PCRs. In 2012, DHS conducted a PCR on the EINSTEIN program. The PCR report is published on the DHS website: www.dhs.gov/privacy. Following recommendations from the 2012 DHS PCR, the NPPD Office of Privacy periodically conducts Privacy Oversight Reviews for PII handling for its cyber programs.

Outreach

DHS participates in a whole of government approach to securing the nation’s critical infrastructure and government services. A vital part of meeting its responsibilities to serve the public is to share its work on privacy with the rest of government so that other departments and agencies may integrate privacy protections into their systems and programs.

DHS also benefits from the advice it receives from its Data Privacy and Integrity Advisory Committee (DPIAC). DHS shares the Committee’s reports with other agencies and the public through its webpage, www.dhs.gov/privacy so that all may benefit from the Committee’s work. Additionally, in 2009, the DPIAC formed an ad hoc subcommittee to address privacy issues related to cybersecurity, as DHS is increasingly addressing cybersecurity in ways that impact privacy.

Education

The Federal Privacy Council sponsors a semi-annual Privacy Boot Camp, open to all staff at all federal agencies. For more information, email privacy.council@gsa.gov.

Revised September 2018
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.

What’s in this guide:

- Cybersecurity for Organizations
- Actions for your Supply Chain
- Actions for Infrastructure Protection
- Actions for your Workforce and Consumers

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 organizations take 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.

• 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.
CTIONS 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

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.
  o 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.³ 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).
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 combatting disinformation. We ask that anyone with any relevant information, or indication of a compromise, contact us immediately.
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.

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

For more information about how you can Do Your Part. #BeCyberSmart, visit www.cisa.gov/ncsam
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
INTERNET OF THINGS

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.

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

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 “fishy,” 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 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.

• **FTC.gov:** The FTC’s free, one-stop resource, [https://www.identitytheft.gov/](https://www.identitytheft.gov/) can help you report and recover from identity theft. Report fraud to the FTC at [ftc.gov/OnGuardOnline](http://ftc.gov/OnGuardOnline) or [https://www.ftccomplaintassistant.gov](https://www.ftccomplaintassistant.gov).

• **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](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.
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.

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

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 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.

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.

---

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.