VOLUME 16 | ISSUE 4
OCTOBER - DECEMBER 2025

SAFETY & LOSS PREVENTION

OUTLOOK

THE STATE OF CYBERSECURITY

ALSO INSIDE:

- October is National Cyber Security Awareness Month
- Protecting Florida's Critical Infrastructure
- AI is Everywhere: Learn How Not To Be Fooled
- Fight the Monsters Lurking in Your Safety Program

OUTLOOK

Issue 4, Volume 16 | Oct-Dec 2025

A Message from the Editor

Click here to take Stuart Thompson's AI Detection Quiz. Can you tell a real video from a deepfake? (For the record, my son got 80% correct. I scored a humbling 60%.)

Recently at dinner, my teenage son and I were discussing the prevalence of AI in entertainment and social media. "Those photos and videos are so obviously fake," he insisted. "I don't know how people can't tell. I've never been fooled by AI." I responded incredulously, "How would you know?"

We are taught to trust our eyes, but as AI technology gets more advanced, the "tells" become harder to detect, especially with a cursory look. I guarantee some AI has slipped by him -- and all of us -- simply because we didn't think hard enough about what our eyes were seeing. And if the deception is successful, how would we even know we have been deceived?

As our digital lives become larger and more complex (the average person now needs around 100 passwords!), it's understandable to want to take shortcuts. Cybercriminals know this and use it to their advantage. This is one reason why cybercrime increases during the holiday season. When shopping online, remember the following precautions:

Beware of phishing messages. Many are designed to look like emails or texts from retailers about holiday sales. Go directly to retailer websites instead of clicking on links.

Check for encryption. The website address should begin with "https". In the Chrome browser, click the "tune" icon for more information about the site.

Choose reputable vendors. Malicious websites may appear very professional. Always verify a business is real before entering any information into their site. The Better Business Bureau allows you to search for accredited businesses.

Use credit whenever possible. Laws limit your liability for fraudulent credit card charges, but you may not have the same level of protection when using credit or online services like PayPal or Venmo.

Wishing you a safe and secure holiday season!

Lori Taylor
Managing Editor

INTERAGENCY ADVISORY COUNCIL

SAFETY & LOSS PREVENTION EXCELLENCE AWARD

If you know an agent, employee, or volunteer who has made exceptional contributions to the reduction and control of employment-related accidents, contact your agency's safety coordinator to submit a nomination. Safety coordinators should submit nominations to the Division of Risk Management's Loss Prevention section at least two weeks prior to an upcoming quarterly IAC meeting. Nominee approvals will be made by IAC members during the meeting.

MARK YOUR CALENDARS

The next Interagency Advisory Council Meeting will take place in person on:

NOVEMBER 4, 2025 at 2:30 pm

at the Hermitage Centre
(located at 1801 Hermitage Blvd., First floor conference room, Tallahassee, Florida, 32308)

and virtually via GoToMeeting

Council Members: Look for an email invitation coming soon

IN THIS ISSUE

NATIONAL CYBER SECURITY AWARENESS MONTH

OCTOBER 2025

In 2003, the U.S. Department of Homeland Security and the National Cyber Security Alliance (NCSA) established the month of October as National Cyber Security Awareness Month (NCSAM). Since its inception, NCSAM has served to promote a culture of shared responsibility for cyber safety, including government, business, and community organizations, as well as the general public.

This year's theme, **Stay Safe Online**, focuses on the simple, yet effective, ways we can protect ourselves from online threats. Staying alert and aware of the latest threats becomes increasingly important as cyber threats get more and more sophisticated. NCSAM seeks to remind us of the vital role that every one of us plays in keeping ourselves, our workplaces, our communities, and the world at large safe and cyber-secure.

THE CORE 4

Here are four easy steps anyone can take to boost their online safety:

1 USE STRONG PASSWORDS

Passwords should be long, unique, and complex. A password manager can help you create nearly hackproof passwords and keep them secure.

2 TURN ON MULTIFACTOR AUTHENTICATION (MFA)

Each method of verification required to login to servers and websites creates another layer of defense.

3 UPDATE YOUR SOFTWARE

Keeping your software up to date can help guard against data breaches and malware by patching the latest vulnerabilities and enhancing security features.

4 RECOGNIZE AND REPORT SCAM ATTEMPTS

Be wary before clicking links or sharing information. Even if you don't fall for a scam, reporting it can alert others to the threat.

These four crucial behaviors serve as a foundation for all employees in your organization to create a secure online environment.

CYBERCRIME STATISTICS

NATIONAL

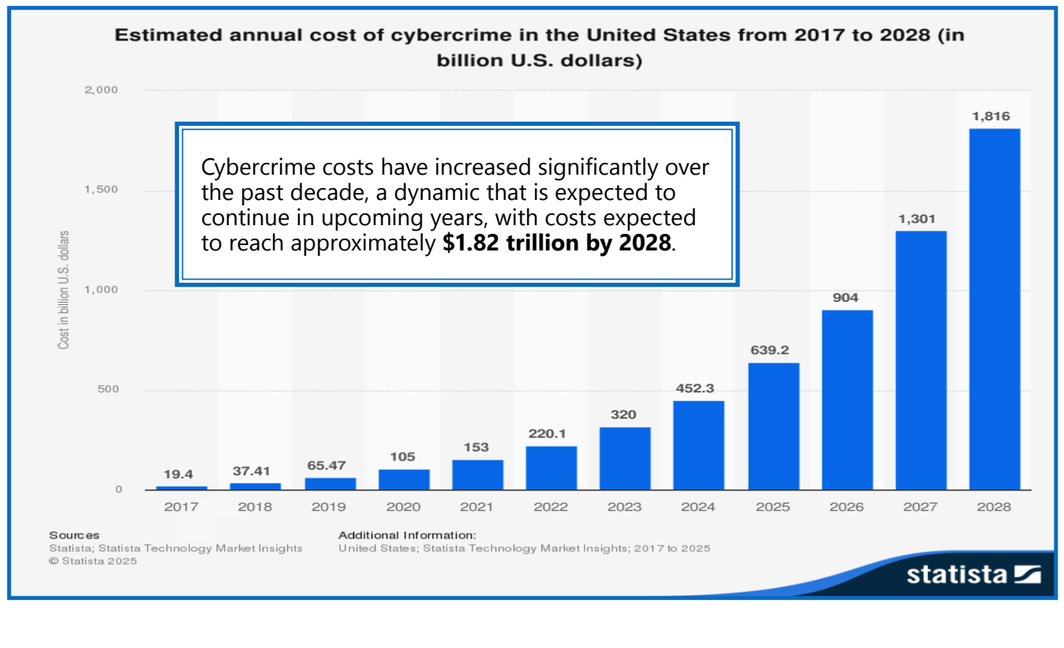
- The FBI received over **800,000** cybercrime reports in 2024, **3,156** of which involved ransomware.
- In 2024, U.S. financial losses from cybercrime reached a record **$16.6 billion -- 33% more** than the previous year.
- Ransomware attacks on U.S. targets surged **146%** in 2025, giving our country the unenviable title of Ransomware Capital of the World.

STATEWIDE

- In 2023, Florida's cybercrime losses put us at ninth per capita and third overall, averaging **$64.47** lost per resident, for a total of approximately **$1.51 billion.**
- Among the most damaging were romance scams, which cost Floridians **$89 million** in 2024. Other common scams involved criminals impersonating businesses (**$54.8 million** in losses) or government agencies (**$45.7 million** in losses).

DID YOU KNOW?

Practicing good cyber hygiene prevents 80-90% of all cybersecurity issues.



STAY CYBERSECURE WITH THE CORE 4

PASSWORDS: LOCK THE DOOR TO STAY CYBERSECURE

Password management can seem time-consuming and frustrating -- constantly being asked to change passwords, making them fit the required parameters, remembering them, keeping them secure -- all of this can make it tempting to cut corners. But keep in mind that passwords stand guard at the door of cybersecurity, acting as the first line of defense against threats. Having weak passwords is like leaving your front door wide open, allowing intruders to come in, make themselves at home, and take whatever they want. Remind yourself and others in your organization that strong passwords help keep the door locked.

"I've been hacked!" Most of the time, when people say this, what they really mean is that bad actors were able to access their accounts, and most of the time, those people invited the bad actors in themselves -- by clicking on a malicious link.

Once compromised, one "hacked" account often leads to others, a domino effect known as "credential stuffing." Criminals know that people often use the same password for more than one account; they only need one password to access multiple accounts.

CRIMINAL TACTICS

How Cybercriminals Steal Your Passwords:

- **Phishing:** Tricking you into clicking on malicious links and entering your credentials on fake login pages
- **Keylogging Malware:** Secretly installing software on your device that records everything you type
- **Brute Force/Password Spraying:** Using AI tools to try common/weak passwords until one works
- **Shoulder Surfing/Social Engineering:** Watching you type a password/tricking you into revealing your password

How Cybercriminals Use Your Passwords:

- **Accessing Financial Accounts:** Logging in and draining your bank, retirement, and investment accounts
- **Shopping Sprees:** Making purchases using your online shopping accounts where your credit card information is stored
- **Controlling Your Devices:** Mining your hard drives for data, deleting files, installing malicious malware (such as keyloggers), turning your computer into a bot to spread spam or commit other crimes
- **Stealing Data To Resell:** Using your personal or employer's information for identity theft or selling it on the dark web
- **Ransomware:** holding your accounts hostage until the demanded ransom is paid

PASSWORD TIPS

- **Longer Is Stronger:** Your password should be at least 12-16 characters.
- **Mix It Up:** Use a combination of upper and lower case, letters, numbers, and symbols. Avoid substitutions like "P@ssw0rd".
- **Avoid Personal Info:** Don't use names, birthdates, addresses, etc. in your password.
- **Make Them Unique:** Use a different password for each account, and never reuse old passwords.
- **Use A Password Manager:** These tools can generate strong passwords and safely store them so you don't have to remember them all.

MULTIFACTOR AUTHENTICATION: INCREASE SECURITY MEASURES

Even strong passwords can be stolen. Multifactor authentication (MFA) adds a critical extra layer of defense by requiring something in addition to the password -- something you **have** (a phone, an email address, a hardware token, etc.) or something that is a **part of you** (a fingerprint or a face). Websites will often send a one-time code to your email or phone to further authenticate your identity. If the password is the lock, MFA is the security system.

In spite of the added security of MFA, criminals have still found ways to get around account protections. Once inside, cybercriminals can take over your accounts, steal your data, phish your friends and coworkers, and even launch larger attacks.

CRIMINAL TACTICS

How Cybercriminals Bypass Your MFA:

- **Phishing:** Using fake login sites or scam messages that trick you into entering both your password and one-time code
- **SIM Swapping:** Convincing a phone carrier to transfer your number to their device, intercepting text-based codes
- **Push Notification Fatigue:** Flooding you with repeated MFA prompts until you accidentally approve one (aka "MFA bombing")
- **Malware:** Stealing authentication tokens directly from a phone or computer using malware
- **Man-in-the-Middle Attacks:** Intercepting login sessions through malicious Wi-Fi hotspots or infected devices

Signs Your MFA Has Been Compromised:

- receiving continuous, suspicious MFA approval requests when not trying to log in
- receiving unexpected password reset or security alerts
- noticing unauthorized logins from unfamiliar locations
- observing suspicious changes to your account settings or mail forwarding
- experiencing sudden lockouts or inability to log in to accounts
- unusual outgoing messages or missing emails
- unauthorized transactions on your accounts

CYBERSECURITY BY THE NUMBERS

- During the first six months of 2025, the U.S. had **18.4 billion** data point leaks, out of which **2.28 billion** were related to passwords.
- Only **34%** of users change their passwords every month. **26%** never change their passwords unless forced to do so. (This is why making scheduled password updates a mandatory policy is so important for your organization.)
- **6%** of adults report that they still have access to the accounts that belong to former romantic partners, roommates, or colleagues.
- **84%** of people reuse passwords across platforms. A Microsoft study found that **44 million** of its users were reusing passwords.
- **24%** of Americans use passwords that are notably easy to guess and take less than **one second** to crack. "123456" is currently in use more than **4.5 million times**.
- **60%** of all security breaches involve a human element, according to Verizon's 2025 report.
- In general, **3%** of an organization's employees will click on a malicious link within a phishing email.
- Malicious emails account for approximately **one in 323** emails received by organizations with less than 250 employees.
- An estimated **91%** of all cyber attacks begin with a phishing email.
- According to data from the FBI, cybercrime is expected to cost more than **$23 trillion** per year worldwide by 2027 -- more than the annual economic output of China.

SOFTWARE: FIX THE CRACKS BEFORE INTRUDERS ATTACK

Every piece of software -- whether it's on your phone, laptop, or workplace system -- has vulnerabilities. Cybercriminals are constantly searching for those cracks in the system they can exploit to slip inside. If the password is the lock, and MFA is the security system, software updates are the maintenance done to fortify any weaknesses in the property's security. Software updates (or "patches") close the gaps before attackers can take advantage. Keeping systems updated isn't just about getting access to the latest features -- it's about protecting your data, your devices, and your organization.

RANSOMWARE: HOW IT WORKS

- CRIMINAL ENTERS SYSTEM
- CHANGES PASSWORDS OR USES MALWARE TO BLOCK ACCESS
- SENDS A MESSAGE THAT THEY HAVE SEQUESTERED & BLOCKED ACCESS TO THE INFORMATION
- DEMANDS PAYMENT IN EXCHANGE FOR REGAINING ACCESS TO THE SYSTEM

CRIMINAL TACTICS

How Cybercriminals Exploit Outdated Software:

- **Using Known Vulnerabilities:** Hackers read the same patch notes as users. If a vendor announces a fix, criminals rush to attack systems that haven't applied it.
- **Installing Malware:** Outdated programs are often the easiest way to deliver destructive code.
- **Gaining Unauthorized Access:** Old security flaws can give criminals backdoor entry into networks.
- **Spreading Attacks Automatically:** Botnets can scan the internet for unpatched systems and infect them without any user interaction.

What Happens If You Ignore Updates:

- **Data Theft:** Sensitive files, personal records, and business data are all up for grabs.
- **System Compromise:** Hackers can gain admin control and use it to spy on activities or disrupt operations.
- **Financial Loss:** From unauthorized account access to ransomware demands, the losses can add up quickly.
- **Reputation Damage:** A preventable breach caused by unpatched software undermines the public trust.

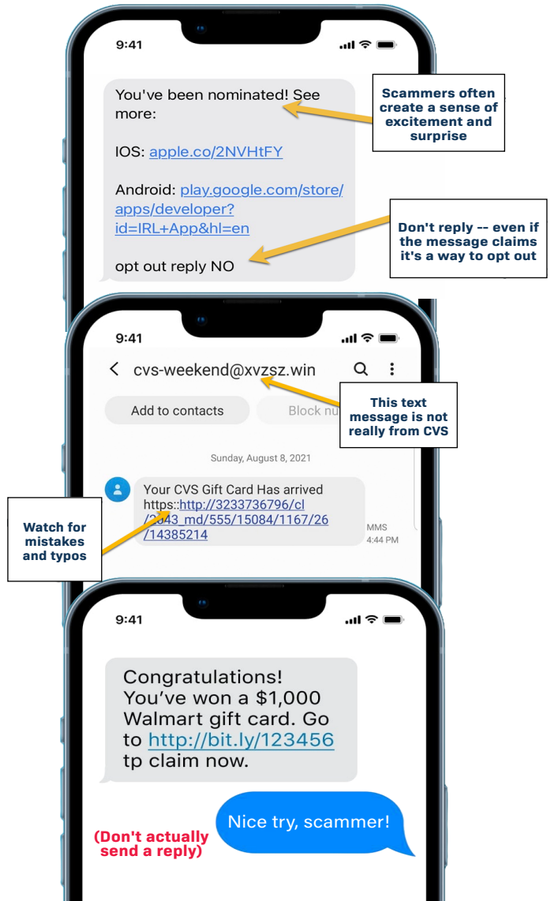
STAYING PROTECTED

- **Turn on automatic updates** whenever possible so patches are installed as soon as they are released.
- **Prioritize security patches** over feature upgrades -- these are critical fixes.
- **Update all devices**, including smartphones, routers, printers, and other gadgets with internet access.
- **Stay informed** about critical security alerts from software vendors.

SCAM ATTEMPTS: DON'T BE FOOLED INTO INVITING CRIMINALS INSIDE

Cybercriminals don't always need to steal your information or break in through cracks in the system -- often all they need is a person to invite them in.

Cybersecurity relies on humans to lock the door, turn on the security system, and patch the holes to keep bad actors out. Scammers can get around these systems by convincing you to not only leave the door unlocked, but open it for them, or tricking you into giving them the key -- a tactic known as "**social engineering**." Your organization's IT system counts on its users to stand guard at the door to keep intruders out.



CRIMINAL TACTICS

How Cyber Scams Work:

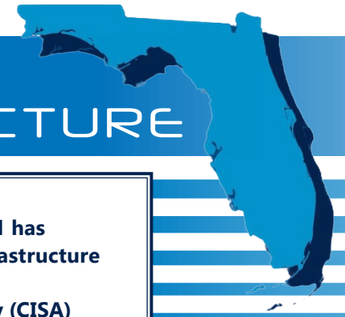
- **Phishing:** Scammers make messages that look official but contain malicious links or attachments. These often include promises of reward, threats of negative consequences, and a sense of urgency to respond.
- **Fake Websites:** Fraudulent login pages look like the real thing but are designed to steal your credentials.
- **Business Email Compromise (BEC):** A scammer impersonates a coworker, a contact at another organization, or a vendor to request money, make changes to contact information ("Please mail checks to my new address listed here"), or gather information.
- **Tech Support Scams:** Fraudsters pose as help desk staff to gain access to your device. They may even claim fraudulent activity has been detected on your account.
- **Spear Phishing**: Scammers target you directly, using personal data they have gathered about you; they have a very high success rate compared with other phishing attacks due to their precision, personalization, and difficulty in detection.
- **Smishing**: Phishing on your phone using SMS data (texting).

AVOIDING SCAMS

- **Pause before you click** on any link; hover over links to see where they really go. Best practice is to go directly to the website by typing the URL rather than clicking a link in an email.
- **Verify requests** by contacting the person or organization directly using known contact info.
- **Check for red flags** such as misspellings, odd formatting, unexpected requests, or urgent demands.
- **Use security tools** to help catch scams, such as spam filters, antivirus software, and browser warnings.
- **Report suspicious messages** to your IT security team -- don't just delete them.
- **Don't let tailgaters into the building** without proper authorization -- you could be giving them free access to your agency's information and resources.

- CHEMICAL FACILITIES
- COMMERCIAL FACILITIES
- COMMUNICATIONS
- MANUFACTURING
- DAMS
- EMERGENCY SERVICES
- ENERGY
- FINANCIAL SERVICES
- FOOD & AGRICULTURE
- **GOVERNMENT**
- PUBLIC HEALTH
- INDUSTRIAL DEFENSE
- INFO TECHNOLOGY
- NUCLEAR FACILITIES
- TRANSPORTATION
- WATER & WASTEWATER

CRITICAL INFRASTRUCTURE



Presidential Policy Directive 21 has identified these 16 critical infrastructure sectors. The Cybersecurity & Infrastructure Security Agency (CISA) works with government and private industry to protect systems within these sectors from threats.

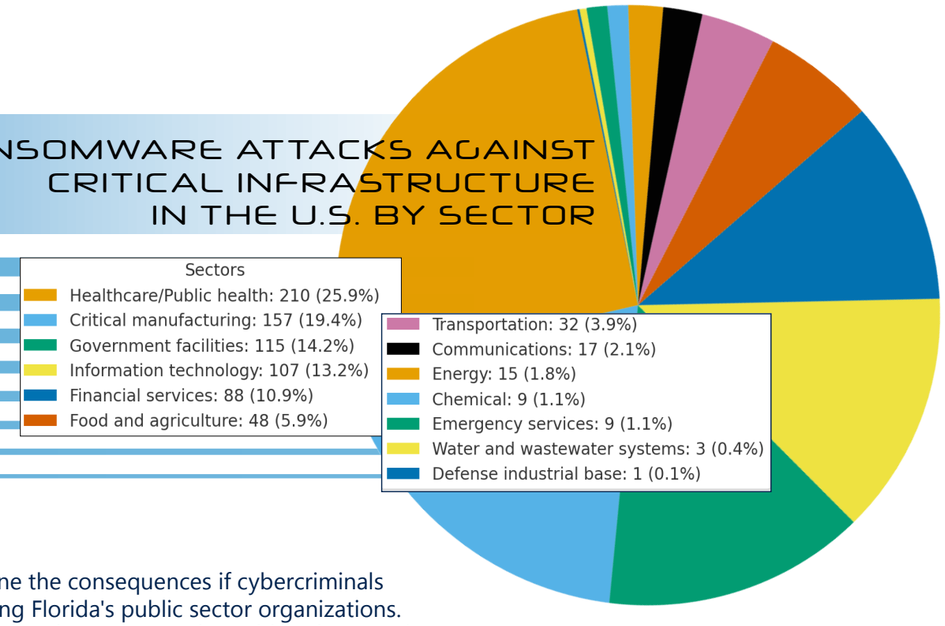
It's been the plot of many futuristic Hollywood movies -- an attack on our country's critical infrastructure that brings our daily lives to a screeching halt and threatens to upheave the world at large. It may be the stuff of fiction, but the risks posed by a potential cybersecurity breach could become a reality.

Critical infrastructure is more than just physical structures; it includes the control and protection of information as well. Because so much of our physical infrastructure now relies on the internet to work, security is made much more complicated -- not only do we need physical guards at the physical gates, we need digital guards keeping cybercriminals out of the systems that run them.

Based on recent reports, the top three targeted sectors are healthcare, manufacturing, and energy/utilities. Ransomware attacks on healthcare groups nearly doubled between 2021 and 2024, as healthcare records hold great value for cyber criminals -- the American Hospital Association found that stolen health records sell for 10 times more than stolen credit card numbers on the dark web. Healthcare breaches also are the most expensive security incidents (average $11 million) and take the longest to fix (average 300 days).

As the country's third most populated state and home to many critical infrastructure and federal assets, Florida is a prime target for cyberattacks, and that includes our state agencies and universities. Compared with the private sector, state and local agencies stand to lose considerably more, due to their responsibilities as public servants to control and protect citizens throughout the state.

RANSOMWARE ATTACKS AGAINST CRITICAL INFRASTRUCTURE IN THE U.S. BY SECTOR



It's not hard to imagine the consequences if cybercriminals succeeded in breaching Florida's public sector organizations. Unfortunately, we've already seen several notable cybersecurity incidents that have made headlines in recent years:

In 2020, a Distributed Denial-of-Service (DDoS) attack targeted one Florida county's public school system, occurring amid the COVID-19 shift to online learning and disrupting the first week of the school year.

In 2021, cyber criminals obtained unauthorized access to the supervisory control and data acquisition (SCADA) system at a central Florida water treatment plant and attempted to increase the amount of sodium hydroxide (lye) into the water supply. The FBI reported that the plant's use of outdated software may have contributed to the attacker's ease of access.

In 2022, one Florida university suffered a serious ransomware attack -- the eighth university in the U.S. to receive such an attack that year.

These incidents highlight potential cybersecurity vulnerabilities and stress the importance of our state agencies and universities being ready to fend off an attack on our critical infrastructure.

KEY ELEMENTS OF THE NIST FRAMEWORK

INVENTORY: A list all technology, data, and people gives your organization an accurate picture of what needs protecting (or recovering after an incident).

CONTROLS: Keeping hardware, software, and multifactor authentication up to date can help patch weaknesses.

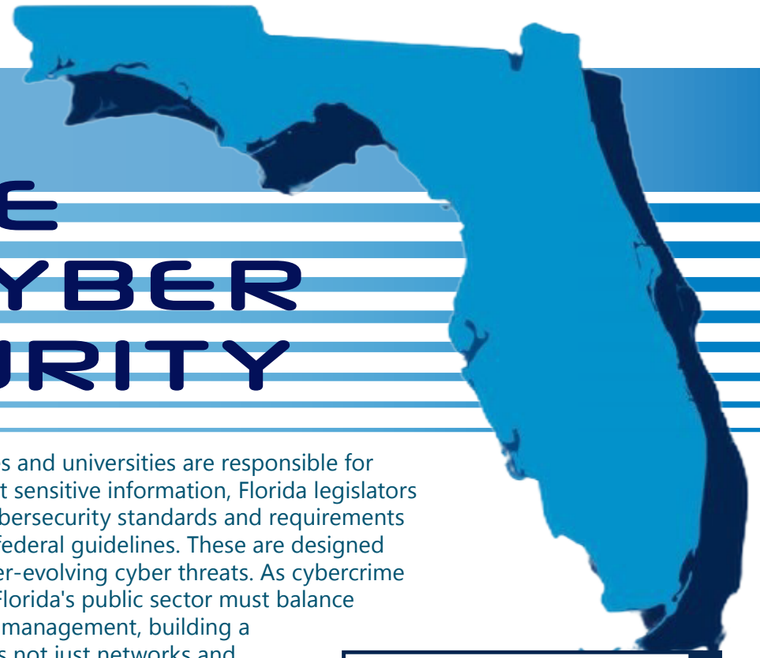
VULNERABILITY MANAGEMENT: Proactive and continuous process assessment helps keep systems safe.

IDENTITY & ACCESS MANAGEMENT (IAM): Controlling who has access to certain systems in your organization is very important, especially with vendors.

CONFIGURATION: A secure setup and ongoing management of systems ensures usability while reducing vulnerabilities.

RECOVERY: Having a solid recovery plan is essential, especially in Florida, where it's illegal to pay or comply with ransomware demands.

THE STATE OF CYBER SECURITY



Because Florida's state agencies and universities are responsible for safeguarding some of our most sensitive information, Florida legislators have implemented rigorous cybersecurity standards and requirements that align with both state and federal guidelines. These are designed to ensure resilience against ever-evolving cyber threats. As cybercrime becomes more sophisticated, Florida's public sector must balance compliance with proactive risk management, building a culture of security that protects not just networks and systems, but also the citizens we serve.

Florida Statute Section 282.318

Otherwise known as the "State Cybersecurity Act," this statute establishes mandatory cybersecurity standards and procedures for all state agencies and universities that are aligned with the National Institute of Standards and Technology (NIST) Cybersecurity Framework. This requires each agency to designate an Information Security Manager, submit a strategic and operational cybersecurity plan to DMS by July 31 each year, conduct risk assessments every three years, and ensure all employees receive annual cybersecurity training. It also determines what actions must be taken when a cybersecurity incident occurs. State vendors and contractors must notify state agencies of cybersecurity breaches within the time parameters set in statute.

Assessing Threats

From accidental deletion of files to willful gathering and sharing of private data, insider threats remain the single largest threat to any organization. Determining the capability of employees to create cyber incidents must be considered when reviewing security protocols, response, and recovery.

CYBER INCIDENT SEVERITY LEVELS

LEVEL 1: low-level incident **unlikely to impact** public health, safety, liberty, economic security, or public confidence

LEVEL 2: medium-level incident that may impact public health, safety, liberty, economic security, or public confidence

LEVEL 3: high-level incident likely to result in **demonstrable impact** to public health, safety, liberty, economic security, or public confidence

LEVEL 4: severe-level incident likely to result in **significant impact** to public health, safety, liberty, economic security, or public confidence

LEVEL 5: emergency-level incident that poses an **imminent threat** to life, wide-scale critical infrastructure, or national, state, or local government security

INCIDENT RESPONSE: ORDER OF OPERATIONS

PHASE 1: INTAKE
- Gather information about the incident

PHASE 2: INTERNAL EFFORTS
- Assemble incident response team
- Report to CSOC within 12 hours

PHASE 3: EXTERNAL EFFORTS
- Report to insurance through designated contact
- Hire as needed in this order: Counsel, Forensics, Rebuild Team, Media Relations

PHASE 4: SYSTEMS WORK
- Forensics (investigate, eradicate, preserve)
- Evaluate backups and restoration
- Clean & harden security on systems

PHASE 5: PII REVIEW
- Assess personally identifiable information (PII) and statutory notice

PHASE 6: POST-MORTEM
- Create After-Action Report summarizing the incident, its resolution, and any insights gained as a result of the incident
- Submit to CSOC within one week after remediation

Three ways to contact the FL[DS] CSOC:
Website: **http://ir.digital.fl.gov/** (preferred method)
Email: **CSOC@Digital.FL.gov**
Phone: 850-412-6074

Incident Severity Levels (as per the U.S. Dept. of Homeland Security)

The State of Florida requires state and local governments to report incidents at **Level 3 or higher** no later than 48 hours, after discovering the incident, or 12 hours if ransomware is involved. Refer to the chart on the previous page for a description of each level. The Cybersecurity Operations Center (CSOC) will report Level 3-5 incidents to the Florida Senate President and Speaker of the House of Representatives.

When a cybersecurity incident occurs

For Individuals:
- Save any evidence you have.
- Report the incident to the local police or sheriff first.
- Visit the FDLE computer crime center; review "common complaints" and follow the instructions that fit your situation.
- File a complaint with the FBI's Internet Crime Complaint Center (IC3) (While the FBI may not respond to your incident, reporting is critical to tracking large-scale scams and criminal activity).

For Agencies & Universities:
- Notify the Florida Digital Service Cybersecurity Operation Center (FL[DS] CSOC) Cybercrime Office of FDLE-- the CSOC will work with your organization and FDLE to coordinate notification to local law enforcement.
- NOTE: If the cyber attack resulted in a data breach, Florida law requires businesses to report the breach to affected consumers within 30 days. If the breach affects 500 or more individuals, businesses must notify the Office of the Attorney General.

REPORTING & RECOVERY

Florida State & Local Government Cybercrime Reporting Requirements

The information reported by the agency must include:

- A summary of facts surrounding the incident
- The physical and/or digital location of backup data
- The date of most recent data backup and whether the backup files were affected
- The types of data compromised
- The estimated fiscal impact
- The details of the ransom demanded (if applicable)
- A statement requesting or declining assistance from the CSOC or FDLE, or the jurisdictional sheriff

Additionally, all ransomware incidents must be reported no later than 12 hours after discovery of the incident.

Critical Infrastructure

Any organization that supports one of the 16 critical infrastructure entities (see pg. 10) is subject to reporting and recording requirements under the Cybersecurity and Infrastructure Security Agency (CISA), an agency under the U.S. Department of Homeland Security. This includes all federal, state, and local government agencies.

Personally Identifiable Information (PII)

Most state agencies and all universities are in possession of some type of citizen data, which must be stored and protected in compliance with state and federal statutes. In 2023, Florida passed Senate Bill 262, also known as the Florida Digital Bill of Rights (FDBR), which puts in place the framework governing how consumers' personal data must be handled. FDBR standards meet or exceed federal requirements.

NIST CS FRAMEWORK CORE FUNCTIONS

These terms help agency leaders to communicate cybersecurity issues more effectively with other agencies, law enforcement, and the general public.

GOVERN (GV): Supports the organizational risk communication with executives, including discussions involving strategy

IDENTIFY (ID): Understand your organization's assets, systems, people, data, and risks

PROTECT (PR): Put saveguards in place to limit or contain the impact of a potential cyber event

DETECT (DE): Build the ability to quickly discover cybersecurity events when they happen

RESPOND (RS): Have plans and actions ready to contain the impact of an incident

RECOVER (RC): Restore capabilities and services after an incident; learn lessons and improve future systems

DID YOU KNOW?

Organizations who experience a data breach spend an average of 287 days and $4.24 million to identify and contain it. Shortening that timeframe also lowers the cost.

Cybersecurity Incident Recovery

Planning ahead can help in restoring capabilities and services affected by a cyber incident more quickly and completely. The type of data and how it is stored will determne the type and components of the recovery plan. Recovering lost data depends on knowing how much data has been lost and at what point in time the system was compromised. CISA has developed the National Cyber Incident Response Plan (NCIRP) as a standard approach for handling significant cyber incidents.

How Online Behavior Outside The Workplace Can Put Your Organization At Risk For Cyberattack

We may like to think of our work and personal lives as separate, but our digital lives have intertwined them in ways we often don't even realize. One weak link in either realm can give cybercriminals a key to unlock systems in the other. Cybersecurity training tends to focus on safe online behavior at work but often overlooks what happens when employees leave the office.

Poor Password Habits

Using the same passwords across personal and work accounts is like leaving the key under the mat for cybercriminals. If one account is breached, attackers can breach other accounts by using the same credentials, a tactic known as "credential stuffing." Weak or predictable personal passwords can reveal patterns that attackers will exploit.

Use of Work Devices for Personal Use

Each of Florida's agencies and universities has its own rules regarding internet use at work, and many block websites deemed unproductive or unsafe (including entertainment, shopping, and social media sites). Clicking on a malicious link in a personal email or website can compromise work-issued devices and the network as a whole. Also, connecting work devices to unsecured Wi-Fi in public places can expose login credentials.

Use of Personal Devices on Work Networks

Most agencies have strict rules about the devices with which logging into the work network is allowed. A devious app downloaded to your personal phone or laptop can install malware, which can then spread to your workplace through the network.

Irresponsible Online Behavior

Employees who have been tricked by phishing in their personal life can make them a more attractive target to hackers. Frequenting "questionable" websites (gambling, illegal downloads, extremist forums, etc.) may make people more vulnerable to blackmail or coercion, turning them into an insider risk.

DON'T:

- ☒ Reuse passwords for multiple accounts
- ☒ Download apps or software from untrusted websites
- ☒ Click on suspicious links in personal email or social media
- ☒ Post sensitive job details or travel plans online
- ☒ Log into work email or apps on public Wi-Fi without a VPN
- ☒ Ignore softare or security updates on personal devices

DO:

- ☑ Use strong, unique passwords for every account
- ☑ Keep personal and work devices separate
- ☑ Enable multi-factor authentication on all accounts and devices
- ☑ Be cautious about oversharing online
- ☑ Use company-approved apps and cloud storage for work data
- ☑ Keep all devices updated to patch security issues
- ☑ Have IT professionals help you set up your personal devices to make sure they are cybersecure

REAL VS. AI PHOTOS: How To Detect The Differences

EXAMINE THE TINY DETAILS

AI technology isn't skilled at mastering the fine details (yet). Look for:

- hands in unnatural positions or with the wrong number of fingers
- extra or distorted limbs
- blurry, jumbled, or unreadable text; misspelled or nonsensical words
- colors or textures that look unnatural (too smooth, glossy, exaggerated, or perfect)
- eyes that are lifeless, unfocused, misshapen, asymmetrical, or misaligned
- objects with details that are "off" (a clock with unreadable numbers, a teapot with two spouts, a chair with five legs, etc.) or appear to be out of place or context (a full cup of coffee with pencils in it, a staircase that leads nowhere, etc.)

CHECK FOR REPETITION OR DISTORTION

AI often uses patterns to generate content, which can result in:

- background elements like trees, buildings, or people that repeat or mirror
- areas that look warped, smeared, or melted, particularly around objects with complex shapes (fences, trees, bicycles, etc.)
- backgrounds or objects that seem patched together from different scenes

Look for order where you would expect disorder (like hair curls that lay too perfectly) and disorder where you would expect order (like objects with straight edges, such as tiles, roads, or buildings, that look warped or bent).

LOOK FOR IMPLAUSIBILITIES & IMPOSSIBILITIES

AI-generated photos often appear to defy physics, or at least logic. Pay attention to:

- objects that just don't look quite right (jewelry that appears melted into skin, clothing that hangs weird)
- people interacting with objects in unconventional ways (someone flipping burgers with a wooden spoon, the Pope wearing a puffer coat)
- lines that don't emerge from the other side of objects in the right way (backpack straps that seem to be growing out of a person's arms, a tree trunk with no corresponding branches)
- shadows that don't match the direction of the light or appear to come from multiple inconsistent light sources
- objects or features with proportions that are incorrect relative to the scene (a bicycle tire-sized tomato, eyes that are too big for the face they are on)
- objects or scenes that look too perfect or unreal (an elaborately-adorned birthday cake, an attractive farmer harvesting overly-hearty crops, the "perfect" vacation spot)
- reflections that don't reflect properly (check mirrors, windows, and water)
- people, animals, or objects doing impossible things (a dolphin perched on a tree branch, a person holding up a car with one hand)
- details that appear out of place or time (an elephant on a Florida beach, a "selfie" of William Shakespeare)

The woman on the right has a head too small for her body, an impossibly long neck ... and ***how many*** fingers??

Pope Francis looks stylish in this Balenciaga coat, but he never actually wore it.

Your local beach probably allows dogs, but you'll have to check the ordinance on elephants.

Kiwi fruits never looked so good! No, really, never.

USE TECHNOLOGY TO DETECT AI-GENERATED IMAGES

Even the most realistic AI-generated images succumb to digital scrutiny.

- Tools such as **Google Images** or **TinEye** can do a "Reverse Image Search" to find where the image appears across the web, check for context, and examine age and usage. Images that are too new or appear in many different, unrelated profiles or contexts are suspect.
- Automated detection tools like **AI or Not** or **Illuminarty** fight AI with AI by analyzing images for telltale patterns invisible to the human eye.
- AI watermark detector, such as **SynthID**, can scan the image for embedded watermarks -- many companies, such as Google and Amazon, hide watermarks in the pixels of images their AI models create.
- Real digital photos contain metadata that records information about the camera, date, and settings used to capture the image -- missing, incomplete, or unusual metadata can be a red flag. Google Images allows you to view metadata for any photo you upload.
- Combine technologies to get the most accurate results. Some sites, such as **Deepware**, use metadata, digital patterns and watermarks, and other data to detect AI-generated photos and videos.

CONSIDER THE CONTENT & CONTEXT

Like mom always said, consider the source. Is it reliable? Is there a motive or gain to be made? Has the validity been verified by multiple credible sources? Photos that seem too strange, unbelievable, or "conveniently timed" are worth a more discerning look, especially those attempting to appeal to your emotions. Develop a healthy skepticism for images that seem too good to be true.

Think you're a master at spotting AI?
See if you can detect which of the images on this page are AI-generated. Answer on pg. 30.

CAN YOU TRUST AI TO JUDGE AI?
We used Google Lens to search for this photo online (it found the website from which the image was originally pulled, but nothing more). Here's how its "AI Overview" (which uses Google's AI program, Gemini) described the photo:

"The image highlights various containers on a desk, all serving as organizational tools for writing instruments and other small office supplies. Top left circle: A small, brown pot containing pens and pencils, likely used for easy access to frequently used writing tools. Middle right circle: A white, cylindrical container holding pens and markers, proving a dedicated spot for different types of writing implements. Bottom left circle: A coffee mug filled with pens and other writing tools, demonstrating a common and informal way to repurpose everyday items for desk organization."

No mention that the flower pots also have potting soil, or that the coffee cup containing pens also contains coffee! Gemini analyzed the photo and described what the image was intended to portray, rather than the details of what is actually shown. It does, however, include a disclaimer at the bottom, reading "AI responses may include mistakes" -- a good reminder to scrutinize AI analyses closely, and that sometimes it still takes a human eye to really see what's there ... for now.

Though AI models have been programmed to sound conversational, they lack a true understanding of what they are being asked, relying instead on patterns. They give information based on whatever has been programmed into their databases, factual or not. And when there are gaps in that knowledge, AI models are prone to "hallucinations" -- they make up responses with whatever seems to make sense. Recent research shows that AI models fabricate 18-69% of their citations, even producing fake references more than half the time they attempt to cite scholarly material.

Why It Matters AI is here to stay -- it's already used extensively both by criminals and those trying to stop them. Hackers create bots and algorithms to steal people's information while internet security experts use the same technology to try to thwart their efforts. Accident investigators will now have to consider the possibility that photo and video evidence being presented to them may not be legitimate, adding a new layer to insurance fraud detection.

In 2001, the movie "Final Fantasy: The Spirits Within" featured the first ever photorealistic computer-animated actress, whose nearly perfect likeness was just imperfect enough to cast the film into the bottom of the uncanny valley and the box office.

On the other hand, Disney's animated film "Frozen" became a huge box office hit, thanks to characters with cartoonish, exaggerated features, clearly human but unrealistic enough to be endearing instead of creepy.

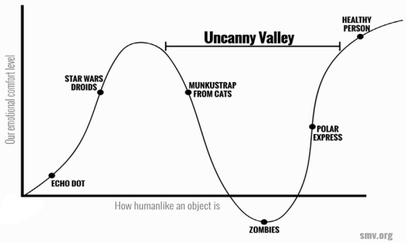
CYBERSECURITY MOVES AT THE SPEED OF AI

The widespread availability of AI tools such as ChatGPT and Adobe Firefly has created an entirely new realm for cyber criminals and IT security professionals alike. In fact, the newest cybercriminals ARE AI -- robots that write with flawless grammar, code like veteran programmers, create nearly perfect deepfakes, and can flood servers with spam like never before. Bad actors use AI models to create fake personas for social engineering or to spread misinformation. An estimated 90% of all hacking is now done using AI.

But what makes AI successful on the offense also works for defense. Cybersecurity companies now use AI to intercept malicious emails and texts, check compliance, search for vulnerabilities, and patch code, all without human interaction. Google announced earlier this year that one of its bots had found a flaw in a code used by billions of computers that cybercriminals could exploit -- something no human had detected.

THE UNCANNY VALLEY EFFECT

In 1970, Japanese roboticist Masahiro Mori proposed a theory that people's affinity for human-like figures (robots, animated characters, etc.) rises as their features look more and more human, but when those features come too close to the real thing, they reach a level of "uncanniness," making them uncomfortable and unsettling to look at. This "valley" of unease rises again if the likeness becomes indistinguishable from a real human.



Artificial intelligence, through photorealistic images, deepfakes, and advanced CGI technology, is challenging our senses to accurately tell what's real and what's not. AI has reached the point where humans find AI faces not only realistic, but as trustworthy as real human faces -- an enormous milestone in the realm of entertainment, but also manipulation and deception.

A small Content Credential icon (seen here) often appears in the corner of authenticated images -- think of it as a "nutrition label" for photos.

Meet the Monsters!

See what's lurking in your safety program

OPTIMISM BIAS

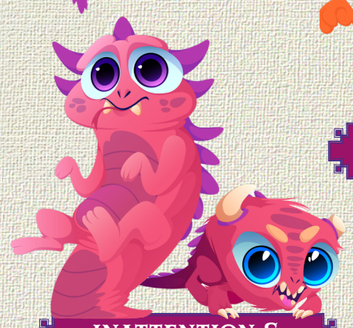
This pie-in-the-sky creature has switched out the safety glasses for rose-colored ones, overestimating the likelihood that everything will be fine and underestimating the risks, resulting in poor decision-making and unsafe behavior.

NORMALIZED DEVIANCE

This party animal breaks the rules over and over and somehow avoids repercussions, creating a false sense of security and tempting others to join the fun.

OBLIVIOUSNESS

Safety protocols? Never heard of 'em! This monster tries to keep workers in the dark about workplace hazards. Especially susceptible to his charms are employees who are new, unsupervised, taking on new tasks, or using unfamiliar equipment.



INATTENTION & HAZARD BLINDNESS

These two best buds hide in plain sight and work as a team to keep workers so focused on their primary task that they become blind to unexpected hazards or threats, even though those threats are right in front of them.

HAZARD DESENSITIZATION

This fella camouflages hazards or makes them seem innocuous and normal, reducing workers' safety vigilance and impairing their judgment of risks, thus lowering their standards of safety.

They may look harmless -- maybe even cute -- but these monsters will infiltrate your safety program and prevent workers from reacting to hazards.

The Combat Guide on page 21 can help you and your team fight these monsters before they wreak havoc in your workplace. **Are you up to the challenge?**

Combat Guide

TAKE ACTION
FIGHT THE MONSTERS
PROTECT YOUR BASE

Step 1: Name the monsters. Have team leaders communicate safety challenges clearly, consistently, and correctly -- not only the hazards themselves, but also the monsters threatening to make people behave in unsafe ways, so that the team knows what they are up against.

Step 2: Remember your training. Make sure you and your teammates are up on the latest rules and safety measures. Learn how to use new tools safely before diving in. Run drills to make sure everyone knows what to do in an emergency.

Step 3: Don't forget your armor! A knight wouldn't try to fight a dragon without the right protective gear, and you shouldn't either -- don't face hazards without the proper protective equipment (PPE).

Step 4: Proceed with caution. Sometimes hazards are able to hide in plain sight because we refuse to believe they will affect us. Scan your battle zone (that is, your workspace) each day, as if for the first time, looking for anything new or out of place. Before any task, take a moment to consider what could go wrong, and go forth accordingly.

Step 5: Follow the map. Your written safety procedures tell you which way to go. Don't take shortcuts or deviate from the path.

Step 6: Work as a team. Ask others to spot-check your work zone or work methods. Speaking up when you see hazards and calling out risky behavior protects everyone on the team.

Step 7: Watch your back! Be aware of your surroundings at all times. Don't forget -- the monsters like to attack when you aren't looking, when you are too engrossed in a task to notice them sneaking up on you. Slow down and pay careful attention to what you're doing so you can see the hazards coming.

Step 8: Tell the tales. Whether glory or defeat, every encounter with a safety monster brings lessons learned. Stories of accidents and near misses remind everyone to stay vigilant. Reporting hazards exposes the monster's tricks.

Step 9: Celebrate your victories! Reward the heroes of safety for fighting fiercely, avoiding hazards, and slaying those monsters!

ORGANIZATIONAL OUTREACH

monthly topics
for your safety calendar

OCTOBER

NATIONAL SUBSTANCE ABUSE PREVENTION MONTH

This observance strives to raise awareness about substance abuse, address the challenges of prevention and treatment, encourage open conversations, reduce stigma, promote healthier choices, and offer treatment and recovery solutions. Substance abuse increases the risk of injuries, and injuries (whether work-related or not) increase the risk of substance abuse. Employers can help employees by encouraging and facilitating access to treatment and supporting workers in recovery. Find info on how to create a **Workplace Supported Recovery (WSR) program here**.

NATIONAL FIRE PROTECTION WEEK: OCTOBER 5-11, 2025

Each year during the week of October 9, this event commemorates the Chicago fire of 1871 by aiming to reduce fire-related injuries and deaths through education. NFPW offers a great opportunity for your organization to review workplace fire hazards and safety procedures, participate in fire drills and fire alarm demonstrations, and recognize first responders with appreciation or community outreach events.

HALLOWEEN: OCTOBER 31

Staying safe at work doesn't have to be scary! Find creative ways to incorporate this festive theme into your safety training. Don't forget to include safety policies for any Halloween-themed events -- costumes that don't block vision or create tripping hazards, pumpkins decorated with markers or paint instead of carving them, and office decor that keeps doorways and walkways clear.

NOVEMBER

DROWSY DRIVING PROTECTION WEEK: NOVEMBER 2-8, 2025

For those of you who work with fleets, this is a good one to reinforce with your drivers. The National Sleep Foundation's Drowsy Driving Prevention Week encourages everyone to prioritize sleep and only drive when we are alert and sleep-refreshed.

COMPUTER SECURITY DAY: NOVEMBER 30, 2025

Since 1988, National Computer Security Day offers the opportunity to engage with employees in your organization about cybersecurity issues and reinforce cyber safety practices in order to better protect our personal and organizational data from cyber threats.

DECEMBER

IMPAIRED DRIVING PREVENTION MONTH

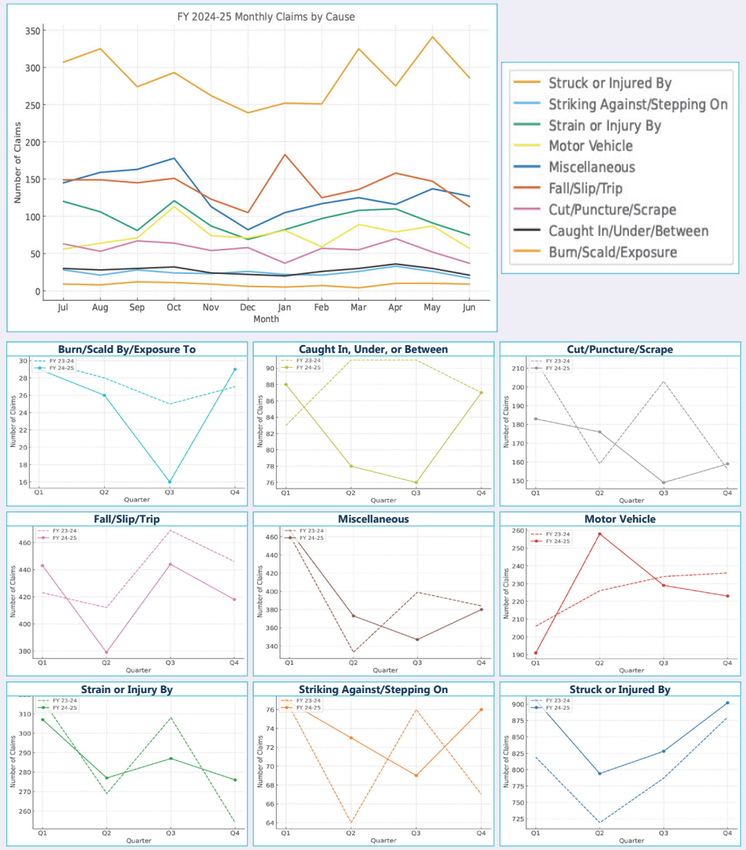
Holiday celebrations bring people together throughout the month of December, which means more traveling, socializing, and for some, "tying one on," which unfortunately means more people driving while impaired. Impaired drivers cause nearly one-third of all traffic deaths in the U.S. each year -- most of them during the holiday season.

This observance brings to light the dangers of driving while impaired and reminds us that impairment can be caused by alcohol, marijuana, pharmaceuticals (legal or not), or even fatigue. Encourage your coworkers to stay safe this holiday season by making safe choices, such as designating a sober driver or using a ride-sharing service.

OUTLOOK SNAPSHOT

State of Florida Workers' Compensation Claim Trends

FY 2023-24 & 2024-25 COMPARISON



OVERALL TRENDS Total claims rose slightly in FY 24-25 (10,120) from FY 23-24 (10,061), less than a 1% increase. However, several categories experienced notable shifts in volume by quarter and/or cause.

QUARTERLY INSIGHTS FY 24-25 claims increased in the first half of the year (+193) and decreased in the last half (-134) from the previous fiscal year. The largest increases occurred in Q2, with higher numbers in nearly every category.

BEST FY IMPROVEMENTS "Burn/Scald By/Exposure To" (-9,1%), "Caught In, Under, or Between" (-6.5%), and "Cut/Puncture/Scrape" (-8.9%) -- these categories may be worth analyzing what changed in order to replicate success.

QUARTER	FY 23-24	FY 24-25	CHANGE	% CHANGE
Q1	2,631	2,691	+60	+2.3%
Q2	2,301	2,434	+133	+5.8%
Q3	2,592	2,445	-147	-5.7%
Q4	2,537	2,550	+13	+0.5%
TOTAL	10,061	10,120	+59	+0.6%

BURN/SCALD BY/EXPOSURE TO (-10) FY 24-25 had 9.1% fewer claims overall -- a notable decrease, given the low-frequency event type.

CAUGHT IN, UNDER, OR BETWEEN (-23) Mostly flat across quarters, with some improvement in FY 24-25, particularly in Q2 & Q3.

CUT/PUNCTURE/SCRAPE (-65) A substantial improvement in FY 24-25, especially in Q1 & Q3.

FALL/SLIP/TRIP (-66) An encouraging drop in the number of claims in FY 24-25; Q3's numbers were affected by a rare Florida snowstorm, causing an unusual number of claims due to slips on ice.

MISCELLANEOUS (-11) Claims rose in the first half of FY 24-25 and fell enough in the second half to finish slightly down from the previous FY.

MOTOR VEHICLE (-1) Total claim numbers are flat, but claims rose 14% in Q2 of FY 24-25.

STRAIN OR INJURY BY (-1) Stable across all quarters between both fiscal years.

STRIKING AGAINST/STEPPING ON (+11) Only slight variability between quarters; both fiscal years ended with nearly identical totals.

STRUCK OR INJURED BY (+225): FY 24-25 followed the same quarterly trends as FY 23-24, but with more claims. Claims in the subcategory "Fellow Worker; Patient" went up (+99), but this does not account for the total increase. When those claims are excluded, overall claims were still up (+124) over the previous FY.

KEY TAKEAWAYS Total number of claims stayed relatively flat between the two fiscal years, suggesting more safety & loss prevention efforts are needed to get this number trending downward.

Most concerning are the increased numbers in Q2, especially in "Cut/Puncture/Scrape", "Miscellaneous", "Motor Vehicle", and "Struck or Injured By" categories. Agencies may benefit from looking at workplace activities during Q2 in particular (October-December) to pinpoint seasonal hazards that can be addressed.

"Struck or Injured By" claims need attention. especially in subcategories "Animal or Insect", "Fellow Worker; Patient", and "NOC".

Safety pros and impostor syndrome

Tips for overcoming the hurdles

August 24, 2025 | Barry Bottino

Photo: Cravetiger/gettyimages

"I don't belong here."
"I'm going to mess this up."
"I don't want to make a fool of myself."

Anyone who struggles with impostor syndrome can relate to these feelings.

The National Institutes of Health describes impostor syndrome as a "behavioral health phenomenon" that affects high-achieving individuals who have pervasive feelings of self-doubt, anxiety, depression or fear of being "found out" as a "fraud" at work.

One study found that 62% of employees globally have experienced impostor syndrome -- and it reaches all levels of organizations.

"The way I look at impostor syndrome is those who are in positions where they don't feel prepared or ready but they have to be 'on,'" said Monique Parker, senior vice president of environmental health and safety at Piedmont Lithium, a North Carolina-based mining company.

When faced with a question or issue from a co-worker or manager, the effect can be devastating.

"I tend to describe it as a paralyzing and debilitating fear," said Bryce Griffler, co-founder of Safety is for Everyone, a consulting and training firm. "The words 'paralyzing' and 'debilitating' are really important because it's not just this nagging discomfort of self-doubt, but it truly is this internalized, constant twisting in your stomach."

The impact

For safety pros, thoughts of failing associated with impostor syndrome can be intense.

"The fear of failure is terrifying for an EHS professional," Griffler said. "Failure can mean the difference between life and death or life and ill health."

Allie Kroeger knows the feelings all too well.

Despite having more than a decade of professional experience in the EHS field and a master's degree, as well as being fluent in Spanish, nagging doubts were a constant.

"You feel like you try so hard to make something of yourself, but then you wonder, 'Is this right? Am I doing it right?'" said Kroeger, safety director at Buckeye Elm Contracting near Columbus, OH. "There were all kinds of questions.

"You have the inspectors that show up to the site that know all the citations. They know all the codes. You ask them a question and they'll spout out, '29 CFR 1926 blah, blah, blah.' I'm like, 'I've got to look that up.' I'm not good at memorizing. I have to see the process. I have to figure out how it works."

As a manager, Parker has seen how impostor syndrome affects others.

"There was a young lady who used to work for me, and I immediately saw her ability and the impact that she could have," she said. "But *she* had no clue. It's more about their confidence in their own abilities vs. their skills and knowledge."

The hurdles

Griffler says safety pros experiencing impostor syndrome can be hesitant to share innovative ideas, join special projects or "tiger teams" that work on a specific goal, or identify a known issue and stop work.

"It's almost introducing another avenue where a person might find out that they don't belong here," he said. "It's a bit of self-preservation."

Along with experiencing negative emotions, safety pros can feel like they aren't working effectively.

"In daily work, sometimes it makes people feel like they're slower," Parker said.

For some safety pros, including Kroeger, impostor syndrome can result in procrastination. Others may have a fear of failure or a fear of success and/or experience perfectionism, NIH says.

The unrelenting daily challenges can disrupt careers -- or even end them.

"A lot of time when you deal with impostor syndrome, you put limits on yourself," Parker said. "You stop your career growth because you feel like you need to check all the boxes or you need to know everything about every piece of occupational safety. That's just not realistic."

The day-to-day plan

Griffler recommends focusing on data and celebrating each day. Whenever someone completes a goal, it should be treated as a success.

"There are going to be metrics of success," he said. "Whatever that success looked like, focus on those numbers. Focus on that evidence of what you achieved, because that's the objective."

Safety pros can set a calendar invite or put a sticky note on their computers as a reminder to celebrate small wins.

"We fail to actually celebrate," Griffler said. "Where's that reminder to ask, 'What are you proud of today?'"

If a glove program results in 60% of your workers wearing them, Kroeger suggests talking to that group about what it likes and declaring that a win. Then, focus on what the other workers don't like and what fixes can be made.

And she has a reminder for safety pros: You're never truly alone. Every glove program, for example, has a distribution representative who can help ensure compliance and solve problems.

"I consider a successful safety professional as someone that doesn't know everything but knows somebody that can help," she said.

And these days, when Kroeger wakes up thinking about the "30 gazillion things" on her task list, she leans on her advance work on taming anxiety.

"Before I go to bed, I say, 'Which one of these isn't something that can wait, but if it doesn't happen, what's the consequence?'" she said. "If the consequence is just for me, I say, 'If I get to it, great. If I don't, then it will be the next day.'"

For Parker, meditation is an effective tool to "ground yourself and get rid of the noise that's around you. Start your day on a level place where you are in a positive mindset."

Then, when the inevitable challenge comes up, you'll be more prepared to manage it.

"If you promise yourself in the beginning of the day how you're going to respond to those negative areas, then it will allow you to be in a better mindset when they do come about."

What can managers do?

Griffler, who's set to present on impostor syndrome during the 2025 NSC Safety Congress & Expo in Denver, said employers can help support workers with impostor syndrome.

Managers should avoid trivializing a high-achiever's feelings or comments, which can reinforce that they've successfully concealed their perceived incompetence and could lead to additional fears of being exposed.

Griffler also recommends providing teaching opportunities to help safety pros gain expertise on a subject matter. Allowing someone the opportunity to teach a topic forces them to conduct a variety of preparation activities.

If someone struggling with impostor syndrome is already knowledgeable on a certain safety topic, teaching to a room full of people can alleviate a person's perception of incompetence.

"Continuing to try to hide and mask is so exhausting and not sustainable," Griffler said. "It's so uncomfortable to be vulnerable. But it's so important. It's not a sign of weakness. In a lot of ways, it's a sign of strength."

Originally published in Safety + Health Magazine
nsc National Safety Council

Miss a previous issue? Browse our online library!

CLICK HERE FOR COMPLETE COLLECTION

The safety training required per section 284.50, F.S. for all newly-appointed safety and alternate safety coordinators is now being provided through online training modules available at your convenience.

NOW AVAILABLE!

BASIC SAFETY TRAINING

USE THE SEARCH BAR TO FIND THIS COURSE

PEOPLE FIRST USERS

CLICK HERE

Go to **TALENT MANAGEMENT ➔ LEARNING ➔ FIND LEARNING**

Type **"DFS_RM"** into the search bar for a list of current courses

Click **"START COURSE"** on the module of your choice

ALL OTHER USERS

CLICK HERE

Submit your information to register for access to the **PEOPLE FIRST LEARNING MANAGEMENT SYSTEM**

Registration will allow access to all current and future trainings

SAFETY & LOSS PREVENTION OUTLOOK TEAM

Florida Department of Financial Services
Division of Risk Management
200 E. Gaines St., Tallahassee FL 32399

Office of the Director 850-413-4700

State of Florida Loss Prevention Section
850-413-3121

Bureau of State Liability & Property Claims
850-413-3122

Bureau of State Employee Workers' Compensation Claims 850-413-3123

Safety Coordinator Appointment Form
850-413-3121

Wendy McSwain
Staff Editor

Lori Taylor
Managing Editor
Lead Writer
Layout / Graphics

Eston Crew
Creative Director

Kelly Fitton
Assistant Division Director

Jeffrey W. Cagle
Chief of Risk Financing & Loss Prevention

Molly Merry, CPA
Division Director

Wendy McSwain
Loss Prevention Section Administrator

VISIT OUR WEBSITE
Click here to visit:
https://www.myfloridacfo.com/division/risk

CONTACT US
Click here to send us an email at:
StateLossPreventionProgram@myfloridacfo.com

If you would like to receive future issues of the OUTLOOK directly in your inbox, send us your email address by clicking the link above. You can also email us with your comments or suggestions. We appreciate your feedback!

The Safety & Loss Prevention Outlook newsletter is for informational purposes only. The Department of Financial Services does not endorse or support any websites, products, brands, or services referenced herein.

REFERENCES & RESOURCES

Experimental Musings Blog. (2022, Mar 28.) Question Your World: Have We Bridged the Uncanny Valley? Science Museum of Virginia. https://smv.org/learn/blog/have-we-bridged-uncanny-valley/

David Carson. JSK Journalism Fellowship Blog. (2024, Dec 18.) Seeing is no longer believing: Artificial Intelligence's impact on photojournalism. Stanford University. https://jsk.stanford.edu/news/seeing-no-longer-believing-artificial-intelligences-impact-photojournalism

Renee Diresta & Josh A. Goldstein. Misinformation Review. (2024, Aug 15.) How spammers and scammers leverage AI-generated images on Facebook for audience growth. Harvard Kennedy School. https://misinforeview.hks.harvard.edu/article/how-spammers-and-scammers-leverage-ai-generated-images-on-facebook-for-audience-growth/

A.J. Vicens. (2025, Apr 23.) Complaints about ransomware attacks on US infrastructure rise 9%, FBI says. Reuters. https://www.reuters.com/world/us/complaints-about-ransomware-attacks-us-infrastructure-rise-9-fbi-says-2025-04-23/

Mella McEwen, Oil Editor. (2025, Mar 27.) Small businesses are especially vulnerable to cybercrime, expert says. Midland Reporter-Telegram. https://www.hearst.com/newspapers/midland-reporter-telegram

Website. (n/d.) Critical Infrastructure Sectors. Cybersecurity & Infrastructure Security Agency, U.S. Department of Homeland Security. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

Website. (n/d.) Estimated annual cost of cybercrime in the United States from 2017 to 2028 (in billion U.S. dollars). Statista. https://www.statista.com/forecasts/1399040/us-cybercrime-cost-annual

Toby Graham. (2025, Jan 07.) Be Thankful for Safety in November: 6 Things to Add to Your Calendar. KPA Consulting. https://kpa.io/blog/be-thankful-for-safety-in-november-6-things-to-add-to-your-calendar

Toby Graham. (2025, Jan 08.) Making a List and Checking it Twice…Here are Your December Safety Observances. KPA Consulting. https://kpa.io/blog/december-safety-observances/

Deren Boyd. (2024, Oct 21.) Are These 5 Monsters Lurking in Your Safety Program? Learn Where They Hide. KPA Consulting. https://kpa.io/blog/are-these-5-monsters-lurking-in-your-safety-program-learn-where-they-hide

Will Jarvis. (2022, Apr 09.) BlackCat ransomware group claims attack on Florida International University. The Record, Recorded Future News. https://therecord.media/blackcat-ransomware-group-claims-attack-on-florida-international-university

Capt. Jennifer Fan, PharmD, J.D. (2022, Dec 08.) The Gift of Sober Driving. Substance Abuse and Mental Health Services Administration. https://www.samhsa.gov/blog/gift-sober-driving

News Alert. (2024, Aug 21.) Cyber Storm Brewing. Florida Trend. https://www.floridatrend.com/article/40882/cyber-storm-brewing

Gary Smith. (2025, Jun 02.) Top Phishing Statistics for 2025: Latest Figures and Trends. Station X. https://www.stationx.net/phishing-statistics/

Karlee Reistroffer. Blog. (2025, Jan 24.) 15 Spam Text Message Examples & How to Identify them. Textedly. https://www.textedly.com/blog/spam-text-message-examples

Website. (n/d.) BBB Tip: Spot the red flags of fake text messages. Better Business Bureau. https://www.bbb.org/all/spot-a-scam/how-to-spot-a-phony-text-message

James Martin. (2023, Nov 15.) AI or Not AI: Can You Spot the Real Photos? CNET. https://www.cnet.com/pictures/ai-or-not-ai-can-you-spot-the-real-photos/

News. (2025, Aug 20.) Florida Among Top 10 U.S. States Where Residents Are Losing The Most Money To Cybercrime. Positively Osceola. https://www.positivelyosceola.com/florida-among-top-10-u-s-states-where-residents-are-losing-the-most-money-to-cybercrime/

Adam Goldman. (2025, Sept 04.) 'Unrestrained' Chinese Cyberattackers May Have Stolen Data From Almost Every American. The New York Times. https://www.nytimes.com/2025/09/04/world/asia/china-hack-salt-typhoon.html

Website. (2021, Feb 08.) Hacker tries to poison water supply of Florida city. BBC News. https://www.bbc.com/news/world-us-canada-55989843

Website. (2021, Feb 12.) Compromise of U.S. Water Treatment Facility. Cybersecurity & Infrastructure Security Agency. U.S. Department of Homeland Security. https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-042a

Bryce Hoffman. (2024, Dec 29.) How To Harness Optimism Bias Without Letting It Derail Your Success. Forbes. https://www.forbes.com/sites/brycehoffman/2024/12/29/how-to-harness-optimism-bias-without-letting-it-derail-your-success/

Marcus White. (2025, Apr 30.) Nine ways MFA can be breached (and why passwords still matter). Specops. https://specopssoft.com/blog/ways-mfa-breached-passwords/

Nayeem Islam. (2025, Jun 12.) The Fabrication Problem: How AI Models Generate Fake Citations, URLs, and References. Medium. https://medium.com/@nomannayeem/the-fabrication-problem-how-ai-models-generate-fake-citations-urls-and-references-55c052299936

Stuart A. Thompson. (2025, Jun 29.) A.I. Videos Have Never Been Better. Can You Tell What's Real? The New York Times. https://www.nytimes.com/interactive/2025/06/29/business/ai-video-deepfake-google-veo-3-quiz.html

Travis Ray Caverhill. (2025, Aug 09.) US Now the Ransomware Capital of the World: The Alarming Shift to Data Theft Over Encryption. Medium. https://medium.com/hacking-the-hacker/us-now-the-ransomware-capital-of-the-world-the-alarming-shift-to-data-theft-over-encryption-3b27d783390a

Blog. (2025, May 27.) What Are Common Examples Of Social Engineering Attacks? Keepnet Labs. https://keepnetlabs.com/blog/what-are-common-examples-of-social-engineering-attacks

Renee DiResta, Abhiram Reddy, Josh A. Goldstein. (2024, Apr 24.) AI-generated images draw in social media users. United Press International. https://www.upi.com/Voices/2024/04/24/artificial-intelligence-generated-images-social-media/6141713964302/

Matthew Groh, et al. (2024, Sept 09.) 5 Telltale Signs That a Photo Is AI-generated. Kellogg Insight Magazine. Northwestern University. https://insight.kellogg.northwestern.edu/article/ai-photos-identification

Mehrdad H.M. Farimani. (2024, Jul 02.) Uncanny Valley Theory in the Design of Robots: Bridging the Gap Between Affinity and Aversion. Medium. https://medium.com/@hm.morvaridi/uncanny-valley-theory-in-the-design-of-robots-bridging-the-gap-between-affinity-and-aversion-0673a673829b

Alex Marquardt, Eric Levenson, Amir Tal. (2021, Feb 10.) Florida water treatment facility hack used a dormant remote access software, sheriff says. CNN. https://www.cnn.com/2021/02/10/us/florida-water-poison-cyber/index.html

Whitepaper. (2025.) 2025 Ransomware Emergency Kit. ThreatDown. Malwarebytes. https://www.threatdown.com/wp-content/uploads/2025/03/CORP_2025-REK-v6.pdf

Newsletter. (2023, Oct 03.) The "Core 4" Behaviors. Pasadena Department of Information Technology. https://www.cityofpasadena.net/information-technology/cybersecurity-newsletters/the-core-4-behaviors/

Blog. (2023, Oct 16.) 4 Core Behaviors to Promote During Cybersecurity Awareness Month. Haxxess Enterprise Corporation. https://www.haxxess.com/blog/behaviors-promote-cybersecurity-awareness-month/

Naveen Kumar. (2025, Jul 28.) 35 Password Statistics 2025 – Data Breaches & Industry Report. Demandsage. https://www.demandsage.com/password-statistics/

Website. (2021, Feb 01.) Understanding Denial-of-Service Attacks. Cybersecurity & Infrastructure Security Agency. U.S. Department of Homeland Security. https://www.cisa.gov/news-events/news/understanding-denial-service-attacks

Blog. (2025.) The Security Fallout of Cyberattacks on Government Agencies. Enzoic. https://www.enzoic.com/blog/cyberattacks-on-government-agencies

Whitepaper. (2025.) 2025 Data Breach Investigations Report. Public Sector Snapshot. Verizon. https://www.verizon.com/business/resources/infographics/2025-dbir-public-sector-snapshot.pdf

Zac Amos, Features Editor. (2024, Feb 28.) Why Higher Education Is So Vulnerable to Cyber Attacks – And What to Do. Cyber Defense Magazine. https://www.cyberdefensemagazine.com/why-higher-education-is-so-vulnerable-to-cyber-attacks-and-what-to-do/

Website. (n/d.) Credential Stuffing Tools. DeepWatch. https://www.deepwatch.com/glossary/credential-stuffing-tools

Wiz Experts Team. (2025 Apr 17.) Credential Stuffing 101: What It Is and How to Prevent It. Wiz. https://www.wiz.io/academy/credential-stuffing

Website. (n/d.) Cybersecurity Awareness Month: Building a Cyber Strong America. Cybersecurity & Infrastructure Security Agency. U.S. Department of Homeland Security. https://www.cisa.gov/cybersecurity-awareness-month

Sead Fadilpasic. (2025, Aug 04.) US becomes ransomware capital of the world as attacks rise by almost 150 percent. TechRadar Pro. https://www.techradar.com/pro/security/us-becomes-ransomware-capital-of-the-world-as-attacks-rise-by-almost-150-percent

Rob Laugher. (2024, May 02.) Is that image AI? Here are 14 telltale signs to look for. Medium. https://roblaughter.medium.com/is-that-image-ai-here-are-14-telltale-signs-to-look-for-d40e5cff2d0a

Capitology Blog. (2024, Mar 18.) How to Spot AI-generated Content: Is It Fact or Fiction? Capitol Technology University. https://www.captechu.edu/blog/how-spot-ai-generated-content-it-fact-or-fiction

Journal. (n/d.) How to Spot AI Generated Images. Everypixel Journal. https://journal.everypixel.com/how-to-spot-ai-generated-images

Miami Times Staff Report. (2024, Apr 02.) FMU hit by widespread cyberattack. Miami Times. https://www.miamitimesonline.com/news/local/fmu-hit-by-widespread-cyberattack/article_189afdc2-ef98-11ee-8ca8-035bc2994d17.html

Tarik Minor. (2024, Jul 04.) I-TEAM: Florida Department of Health data in the hands of a cybercrime group. News 4 Jacksonville. https://www.news-4jax.com/news/local/2024/07/04/i-team-florida-dept-of-health-data-in-the-hands-of-a-cybercrime-group/

Adrian Andrews. (2024, Jul 12.) Experts are chiming in on the latest cyber attacks in Florida. WFSU News. https://news.wfsu.org/state-news/2024-07-12/2024-cybersecurity-experts-are-chiming-in-on-the-latest-cyber-attacks-happening-in-florida

Blog. (2024, Jul 17.) The Week in Breach News: 07/10/24-07/16/24. ID Agent. https://www.idagent.com/blog/the-week-in-breach-news-07-10-24-07-16-24/

Dr. Frederik Lipfert. (2022, Jul 18.) Cyber Security Statistics and Malware Trends for 2022 (Updated Regularly). VPNCheck. https://www.vpncheck.org/cyber-security-statistics/

Andrew Lawson. (2025, Apr 17.) 55 Cybersecurity Statistics to Know in 2025. Privacy Radar. https://privacyradar.com/statistics/cybersecurity-statistics-facts/

Michael Wilson. (2025, Sept 18.) I've Written About Loads of Scams. This One Almost Got Me. The New York Times. https://www.nytimes.com/2025/09/18/nyregion/zelle-chase-banking-scam.html

John Minnix. (2025, Jun 29.) 195 Cybersecurity Statistics (Updated June-2025). Bright Defense. https://www.brightdefense.com/resources/cybersecurity-statistics/

Website. (2025, Jun 12.) 2025 Cybersecurity Awareness Month: Empowering a Digitally Secure World. Keepnet Labs. https://keepnetlabs.com/blog/cybersecurity-awareness-month

Shannon Bond. (2024, May 14.) AI-generated spam is starting to fill social media. Here's why. All Things Considered. NPR News. https://www.npr.org/2024/05/14/1251072726/ai-spam-images-facebook-linkedin-threads-meta

Daniel Thomas. (2022, Nov 11.) The state of ransomware in state and local government. SC Media. https://www.scworld.com/resource/the-state-of-ransomware-in-state-and-local-government

Staff Writer. (2025, Aug.) Cybersecurity Risk in Florida: New SOAX Data Reveals Where the State Stands. Central Florida Lifestyle Magazine. https://www.centralfloridalifestyle.com/tech/cybersecurity-risk-in-florida-new-soax-data-reveals-where-the-state-stands/

Website. (2025, Jul 30.) Key Cyber Security Statistics for 2025. SentinelOne. https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-statistics/

Website. (2025, Apr 23.) FBI Releases Annual Internet Crime Report. Federal Bureau of Investigations News. https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report

Elise Elam and Benjamin Wanger. (2022, Nov 07.) Florida Prohibits State Agencies from Paying Cyber Ransoms. Florida Bar News. https://www.floridabar.org/the-florida-bar-news/florida-prohibits-state-agencies-from-paying-cyber-ransoms/

Website. (n/d.) Shop Safely This Holiday Season. Cybersecurity & Infrastructure Security Agency. U.S. Department of Homeland Security. https://www.cisa.gov/shop-safely-holiday-season

Mark Gill, (2024, Jan 09.) 14 Shocking data loss and disaster recovery statistics. Comparitech. https://www.comparitech.com/data-recovery-software/disaster-recovery-data-loss-statistics/

Toby Graham. (2025, Sept 24.) Four October Safety Observances to Celebrate This Spooky Season. https://kpa.io/blog/4-safety-observances-to-celebrate-this-spooky-season-kpa/

Jack D. Gordon Institute for Public Policy; Steven J. Green School of International & Public Affairs. (2025, May.) Online Cybersecurity Course. Florida International University. https://gordoninstitute.fiu.edu/cybersecurity-policy/training/cybersecureflorida/index.html?utm=lori.taylor@myfloridacfo.com

Think Report. (2025.) Cost of a Data Breach Report 2025: The AI Oversight Gap. IBM. https://www.bakerdonelson.com/webfiles/Publications/20250822_Cost-of-a-Data-Breach-Report-2025.pdf

Judson Jones. (2025, May 22.) NOAA Predicts 'Above Average' Hurricane Season. The New York Times. https://www.nytimes.com/2025/05/22/weather/noaa-forecast-hurricane-season.html

IMAGE ATTRIBUTION

All other images created by DFS, used with permission, or in public domain.

Image by freepik on Freepik.com

Image by lifeforstock on Freepik.com

Image by freepik on Freepik.com

Image by upklyak on Freepik.com

AI-Generated Image Quiz pg. 17 Answer:

ALL of the images on the page were AI-generated.