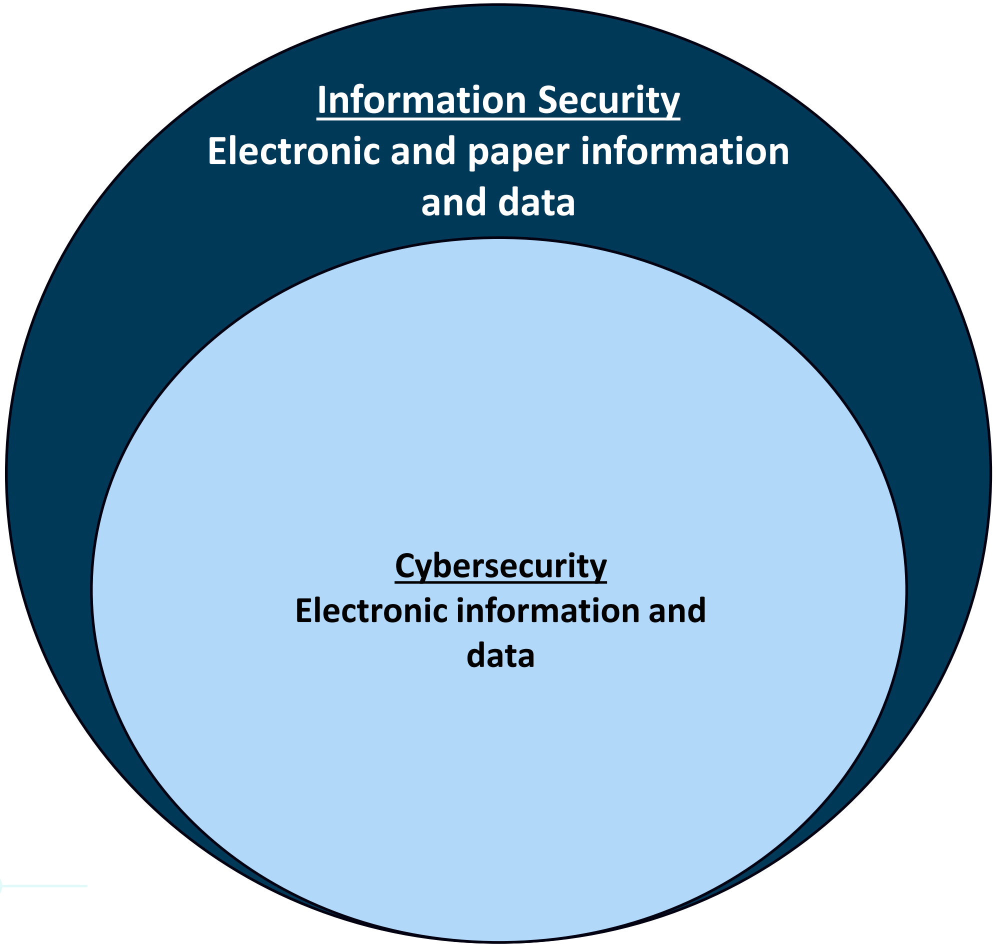
AaSys®
Solutions are our Business®

Information Security and Cybersecurity Awareness Training

2026

Information Security & Cybersecurity – What are they?

Information Security can be defined as the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording, or destruction.



Information Security

Electronic and paper information and data

Cybersecurity

Electronic information and data

Cybersecurity, as a component of Information Security, can be defined as security that is applied to computers, computer networks, and the data that is stored and transmitted over them.

Situational Awareness

Situational Awareness is the process of:

- **Understanding** what is going on around you,
- **Anticipating** what could happen – whether good or bad,
- **Responding** in an appropriate manner.

Maintaining situational awareness can help keep your data secure.

Phishing

- Phishing attacks continue to be the most-used method of cybersecurity exploitation. The Cybersecurity & Infrastructure Security Agency (CISA) states that at least 90% of successful cyber attacks begin with a phishing email.
- Phishing emails may appear to be from a trustworthy source – a coworker, customer, colleague, or vendor. Email may include links or attachments that, when clicked, can launch malware or lure a victim to disclose data, such as user credentials.

Indicators of a Phishing Attempt

- Suspicious Sender Address
- "Internal" email with "External" banners
- Generic Greetings or Signature
- Spelling and Layout
- Suspicious Writing Style
- Suspicious Links
- Suspicious Attachments
- Unsolicited Email
- Sense of URGENCY!

But It Looks Legit!

- Encrypted Email – A continued trend is for cyber criminals to send phishing email through legitimate accounts and legitimate encrypted channels. Often a hacker will compromise an Office 365 account and then send out phishing email. The recipient receives the Office 365 email and considers it legitimate. The victim is prompted to enter their credentials and two-factor authentication code. This compromises the account, as the cyber criminal has run a script to capture the code that was entered. The cyber criminal registers a new two-factor code for the account, and they are able to get into the account any time in the future. They may then use this account to send legitimate-looking encrypted email. These emails are sent to victims, who log on to the mail system to get the encrypted file, find an attachment, and click on it – then they are infected.
- Brand abuse – Phishing emails often carry the logo of or information about trusted brands. In their 2023 State of the Phish Report, Proofpoint comments that the most obvious way to take advantage of a brand is to use their logo or styling in a malicious message. But malicious links hosted on cloud storage solutions like Microsoft OneDrive, Google Drive, and Dropbox are likely to benefit from positive brand associations, as are malicious files created with familiar Microsoft 365 software.
- The use of AI (artificial intelligence) for producing phishing emails is gaining popularity, making phishing attempts appear legitimate.

Vishing

- Oxford Languages dictionary defines Vishing as the fraudulent practice of making phone calls or leaving voice messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as bank details and credit card numbers. Additionally, vishing may be used to have a victim download an install software that may be used for an attack.
- Types of Vishing Attacks include Caller ID Spoofing, Voice Mail Scams, Fake Tech Support Calls, Client Calls and AI Calls (with voice mimicking). Often Vishing is paired with other Social Engineering techniques, such as dumpster diving, to gather information.
- Situational Awareness: Follow customer identification procedures that are in place. Be skeptical of callers that ask for confidential or non-public information. Do not give callers your user credentials or multifactor authentication codes.

Smishing

- Smishing is very similar to vishing or phishing except that the attack is made through text messages.
- Text messages are sent to the intended victim that may include links to malicious websites, phone numbers to call, or other requests for sensitive information. Text messages may also include information used to entice an individual, such as coupons, prizes, or shipment tracking.
- Situational Awareness: Ignore and delete suspicious or unexpected text messages.

Situational Awareness - Email

- You receive an email from an individual “out of the blue”. You have had no conversation with the individual regarding the email topic.
- You do not know this individual who sent you the email.
- You receive an email that appears to be from a coworker but the email contains a warning banner that states it is “External”.

- Understanding the Situation
  - Are you expecting this message?
  - What type of a response or action is being requested?
  - Are there indicators of a phishing attempt?
- Anticipating the Outcome
  - If there is an attachment or link to click, and it is malicious, what could happen?
  - If you divulge confidential information, how could it be used?
- Responding Appropriately may include
  - Contacting the individual through an alternative channel (phone, in person),
  - Resisting the urge to click on the attachment or links,
  - Disregarding or deleting the email,

Ransomware

- 💰 Phishing emails continue to be the most popular vector, or method of attack, used by cyber criminals for the delivery of ransomware to organizations.
- 💰 Ransomware is a type of malicious software that threatens to block access to data or a computer system, usually by encrypting it, until the victim pays a ransom fee to the attacker.
- 💰 In many cases, the ransom demand comes with a deadline. If the victim doesn’t pay in time, the data is gone forever or the ransom increases.
- 💰 Prior to encrypting data, ransomware cyber criminals often exfiltrate the victim’s sensitive data and threaten to publish it if demands aren’t met. Likewise, cyber criminals threaten to “out” the victim by publishing the details of the breach.

Password Safety

Choosing Wisely…

- Choose unique passwords.
- Choose the longest password permissible on the system.
- Consider passwords based on a memorable phrase. Consider the use of numbers for letters or the use of acronyms.
  - DunkinD0nuts4ever!<3
  - B4seB4llHFNY13326! (Base Ball Hall of Fame New York Zip Code)

Don’t Choose…

- Name of close relative, friend, pet, or something that can be found through social media
- A password that is used for another account.
- A shared password. If someone else has the password, create another.
- An easily guessed password. (12345; Winter2023)
- Dictionary words (without adding numbers/symbols)
- Short passwords or passphrases.

Situational Awareness - Passwords

It is time to change your Windows password …. AGAIN! You are sure you just did that a few days ago – is it time to do it again already?!?! You begin to think about your new password and what is should be. You are leaning towards making it as easy as possible for yourself…

- Understanding the Situation
  - Are you accessing an information system that stores confidential information?
- Anticipating the Outcome
  - If a threat actor were to “crack” your password and access a system, would confidential data be at risk?
- Responding Appropriately may include
  - Resisting the urge to cut corners with password safety,
  - Consideration of a password or passphrase that is meaningful to you, while …
  - Creating a password that is strong, and complex.

Remote Access Safety

- A hybrid model whereby employees spend time in the office AND work from home has attackers concentrating their efforts on home devices. As employees connect over a VPN, attackers try to move into a network by compromising these home networks and gaining access to the VPN. Even before the COVID pandemic, financial institutions used remote access as part of business continuity processes.

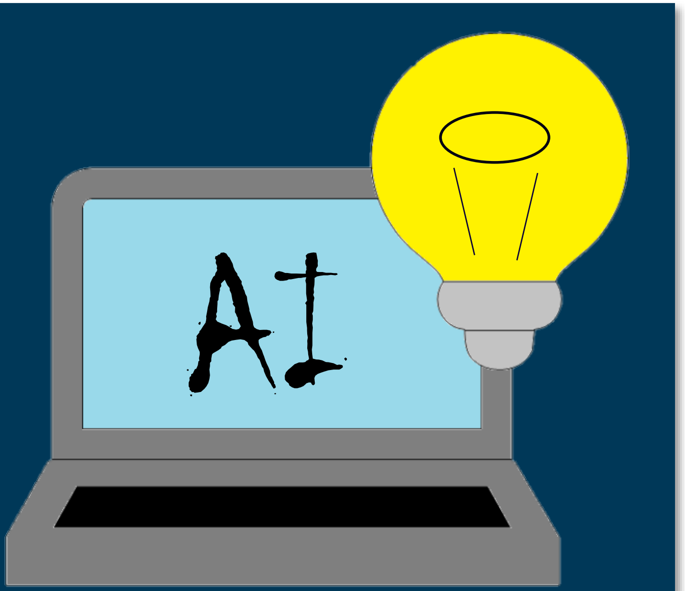
When working remotely…

- Use complex, unique passwords.
- Use multi-factor authentication wherever possible,
- Protect home computers with antivirus and antispam solutions,
- Maintain sound patch management practices:
  - Patch home computers and networking devices,
  - Keep your computer patched regularly,
- Encryption of sensitive data – Make sure internet transmissions are HTTPS.

Remote Access – Mobile Device Security

- Use strong access controls for your device. Controls may include
  - complex password; fingerprint biometrics; facial recognition; finger swipe – Multi-Factor Authentication
- Maintain physical control of the device.
- If your mobile device contains confidential or non-public information, it must be encrypted.
- Install security software on mobile devices (antivirus/endpoint protection).
- Turn on auto-lock after a period of inactivity
- Applications can get you! Only use trusted sources.
  - Read app reviews
  - Check app permissions and data privacy information.
- Install operating system updates
- Watch out for unsecured, public Wi-Fi networks.
- Make sure your data is backed up. This is especially important if your device is out of the office (or Internet access) when devices are being patched.
- Don’t jailbreak the device or modify it in a manner that circumvents security configurations
- Turn off location tracking services if needed.

Artificial Intelligence



What is AI?

- AI is a set of technologies that allow computers to perform tasks that usually require human intelligence. AI can learn, solve problems and make decisions.

Examples of AI in Use

- Wearable Fitness Trackers (FitBit, etc.) that record exercise and sleep patterns,
- Online shopping recommendations based on your previous purchase history,
- Email systems that identify mail as “Spam”,
- Music playlist recommendations,
- “Chatbots” used to answer questions or provided service online,
- A security camera that sends an alert when there is an unrecognized person at the door.

Situational Awareness – Artificial Intelligence

You would like to type an email. You recently saw an ad for an application that, using generative AI, can write your email for you! You would like to try it out – and there's no time like the present.

- Understanding the Situation
  - Is this an application that is approved for use?
  - Will use of this system require input of confidential data?
- Anticipating the Outcome
  - Use of this service could result in a nicely-written email.
  - However, what happens with the data? Could it be used by the AI system for other purposes?
- Responding Appropriately may include
  - Using other methods of assistance with writing the email.

Situational Awareness – Incident Response

Possible Scenarios:

- You click on an attachment that doesn't seem to open.
- Your screen is inundated with annoying ads.
- Your computer starts acting sluggish.
- Your computer crashes or freezes.
- There's a weird increase in your system's Internet activity.
- Your browser settings change.
- You lose access to your files.

- Understanding the Situation
  - Something out of the ordinary is happening to your computer or a device that you are using.
- Anticipating the Outcome
  - You may not be able to work effectively if the event keeps happening,
  - This abnormality may be a symptom of malicious activity,
- Responding Appropriately may include
  - Using automated reporting such as phishing buttons, helpdesk tickets, or other internal systems,

Situational Awareness - Not All Data is Digital

Paper-Based Information

You have a document in your hand that needs to be thrown away.

- Understanding the Situation
  - What is on the paper you need to discard?
- Anticipating the Outcome
  - Could someone use this information maliciously?
- Responding Appropriately may include
  - Tossing the paper into a locked shred bin,
  - Placing the document into a locked drawer or cabinet until it can be discarded.

Spoken/Verbal Information

You are standing in the lobby when a coworker approaches you and begins to talk about a customer's account or loan.

- Understanding the Situation
  - Are other customers or bank personnel in the lobby?
  - Is confidential information being discussed?
- Anticipating the Outcome
  - Could someone overhear?
- Responding Appropriately may include
  - Relocating to an office or other restricted area,
  - Postponing the conversation until a later time.

Summary

While we are on the cusp of technological innovations such as Artificial Intelligence, malicious threats of the past few years, like phishing campaigns and ransomware, are still trending. And people remain the weakest link. Don't be the person who brings down your network by opening the doors to criminals, threat actors, and those with malicious intent.

Practice situational awareness, take a deep breath, and think before you click.

While The Credit Union has assigned responsibilities to specific individuals to manage and monitor information and cybersecurity …

Security is the responsibility of **EVERYBODY!**