

From: CFTC Communication
To: All CFTC
Subject: Acceptable Use of CFTC-Issued Mobile Devices and Hotspots
Date: Monday, March 16, 2026 10:19:11 AM
Attachments: image002.png
image005.png
image001.png
image004.png

CFTC COMMUNICATION

SUBJECT: Acceptable Use of CFTC-Issued Mobile Devices and Hotspots

What do you need to know?

- This communication serves as a reminder and clarification regarding the acceptable use of CFTC-issued mobile devices, standalone hotspots, and CFTC mobile phone-based hotspots. For additional information please refer to the linked policy documents on **Use of CFTC Information and Information Systems**, and **Limited Personal Use Policy**. In addition, please note that the following federal statutes apply to the expected use of GFE.

- 5 C.F.R Part 2635 Standards of Ethical Conduct for Employees of the Executive Branch
- 41 C.F.R § 102-192.50 Restrictions on Personal use of GFE
- Violations could be prosecuted under federal law even in cases where a certain action is not expressly forbidden in CFTC policies.

How can you protect yourself and the Agency?

● **CFTC-Issued Mobile Device and Hotspot usage**¹

- A user may use CFTC-Issued mobile device for limited personal reasons only if such use:
 - Does not interfere with the Commission's mission and/or operations.
 - Is not otherwise prohibited and does not violate the Standards of Ethical Conduct for Employees of the Executive Branch, including the standard on proper representation.
 - Is appropriate and does not misuse CFTC-Issued mobile device.
 - Occurs during the user's non-work time.
- Do NOT share confidential data through unsecured applications or public platforms.

- Do NOT post or browse personal social media sites during work hours using CFTC-issued mobile devices unless authorized for official business
- Do NOT visit websites unrelated official business ¹
- CFTC issued standalone Hotspots or CFTC phone-based hotspots may be used when secure Wi-Fi is unavailable, especially during travel or remote work.
- Hotspots must be password protected.
- Do NOT share hotspot access with unauthorized users.
- Do NOT connect personal devices to your CFTC-issued standalone hotspot or CFTC Mobile phone hotspot for unofficial activities and entertainment. ¹

¹  **CFTC Limited Personal Use Policy** provides clarity on when government issued devices may be used for non-official purposes)

Best Practices on Safe Use of CFTC-Issued Mobile devices

It's crucial to follow best practices to protect sensitive information and reduce risks when using mobile devices to conduct CFTC business. Here are some important guidelines to keep in mind:

- **Only Use GFE Provided Mobile Devices:** Refrain from using any personal devices to conduct agency business or join business calls.
- **Use Secure Communication Platforms:** Whenever possible, use encrypted messaging apps instead of standard SMS to ensure your messages are secure. *Microsoft Teams is an approved communications platform.*
- **Avoid Sharing Sensitive Information:** Refrain from sending personal, financial, or sensitive business information via SMS. Use secure methods for such communications.
- **Authentication and Verification:** Always verify the identity of the person you're communicating with, especially when dealing with confidential information.
- **Beware of Phishing Scams:** Be cautious of unexpected messages that ask for personal information or direct you to unfamiliar websites. Always

verify the legitimacy of such requests.

- **Regularly Update Your Security Settings:** Keep your phone's operating system and apps up to date to protect against vulnerabilities and ensure the latest security patches are installed. Use the auto update setting on your GFE phone.
- **Use Strong Passwords and Enable Two-Factor Authentication:** Protect your mobile devices and apps with strong, unique passwords, and enable two-factor authentication for an added layer of security.
- **Report Suspicious Activity:** If you receive any suspicious messages or notice any unusual activity on your device, report it immediately to our IT department dcitcsc@cftc.gov.

Questions?

- For more information, please refer to the [PDF CFTC Policy: Use of CFTC Information and Information Systems](#) and the [PDF CFTC Policy: Limited Personal Use](#)
- If you have any questions or need assistance, please contact dcitcsc@cftc.gov

From: [CFTC Communication](#)
To: [All CFTC](#)
Subject: CFTC's CyberWise Newsletter – June 2026
Date: Wednesday, June 24, 2026 10:03:15 AM
Attachments: [image001.png](#)
[CyberWise Newsletter – June 2026.pdf](#)

CFTC COMMUNICATION

SUBJECT: CFTC's CyberWise Newsletter – June 2026

Cyber- Wise

What are CyberWise Newsletters?

- CyberWise Newsletters are short 1–2-page publications that include information about important cybersecurity and privacy topics, best practices, current events, useful tips, and resources. Newsletters will be released on a quarterly basis and are meant to provide resources and materials that further enhance your awareness and understanding of key topics. Attached to this email is the June 2026 edition of the CyberWise Newsletter.

This month's topic is Shadow AI: The Hidden Threat Lurking on Corporate Networks

Where can I find previous versions of this Newsletter?

- The Cyber and Physical Security Branch (CPSB) began this initiative in January 2023.

Questions?

- If you have any questions, please feel free to email CTraining@CFTC.gov

Cyber-Wise

CPSB Quarterly Cybersecurity Awareness Newsletter

Shadow AI: The Hidden Threat Lurking on Corporate Networks

Artificial Intelligence tools are becoming more common in the workplace every day. From helping draft emails and summarize reports to generating code and automating tasks, AI can significantly improve efficiency and productivity. However, while these tools offer convenience, they also introduce serious cybersecurity and data privacy risks.

Many may not realize that entering company information into public AI tools can expose sensitive business data, confidential client information, proprietary intellectual property, or internal operation to third-party systems outside of organizational control. What may seem like a harmless shortcut can quickly become a potential incident capable of damaging the organization's reputation, finances, and compliance posture.

As organization's continue integrating AI into daily operations, it is critical that everyone understand the dangers of unauthorized AI usage and their role in maintaining a secure cyber environment.

What Are Unapproved AI Tools?

Unapproved AI tools are artificial intelligence applications, platforms, or services that have not been reviewed and secured by an organization's IT or cybersecurity department. These may include:

- AI writing assistants
- File summarizing tools
- AI image and media generators
- AI transcription or note taking platforms
- Public chatbots

While many of these tools appear safe and useful, organizations often cannot verify:

- Who has access to the information
- How the data is stored
- Whether the data is encrypted
- If the vendor follows security compliance standards
- Whether the tool introduces malware or unauthorized access risks

SHADOW AI

Shadow AI encompasses any artificial intelligence or machine learning tools that operate outside of an organization's official governance framework.

VS

SHADOW IT

Shadow IT encompasses the use of software, hardware, or information technology within an enterprise network without the approval, awareness, or oversight of the IT department.



Reminder – All CFTC users (employees, interns & contractors) are required to complete the New Hire Cybersecurity Training within 2 days of onboarding.



Why Are Unapproved AI Tools So Dangerous on Corporate Networks?

Using unauthorized AI platforms on company systems can create several major cybersecurity threats:

- **Data Leakage & Exposure:** Data is unknowingly uploaded such as customer records, employee data, contracts, passwords, financial information, healthcare information into external AI systems.
- **Malware & Phishing Risks** - Some AI applications or browser extensions may contain malicious code, spyware, or hidden vulnerabilities that attackers can exploit to gain access to corporate systems and networks.
- **Shadow IT Risks** - When employees install or use software without IT approval, it creates "Shadow IT." Shadow IT reduces visibility for cybersecurity teams and increases the attack surface across CFTC.
- **Misinformation & Inaccurate Outputs** - AI tools can generate inaccurate, misleading, or fabricated information. Relying on unverified AI-generated content can lead to operational mistakes, or poor business decisions.

How Can You Stay Cyber Safe?

Every employee plays a critical role in protecting CFTC systems and sensitive information. Here are important ways employees can stay cyber safe when using AI technologies:

- **Only use Approved AI Tools** - Always use AI applications that have been reviewed and approved by CFTC.
- **Follow the CFTC AI Acceptable Use Guidelin** - Review and comply with CFTC policies regarding AI usage, data handling, and acceptable technology practices.
- **Avoid Installing Unauthorized Extensions or Software** - Do not download AI browser extensions, applications, or plugins, without proper approval from IT.
- **Verify AI-Generated Information** - Always fact-check and validate AI-generated responses before using them for business decisions, reports, or communications.
- **Report Suspicious AI Tools or Activity** - If you encounter suspicious AI applications, unusual behavior, report it immediately to IT.

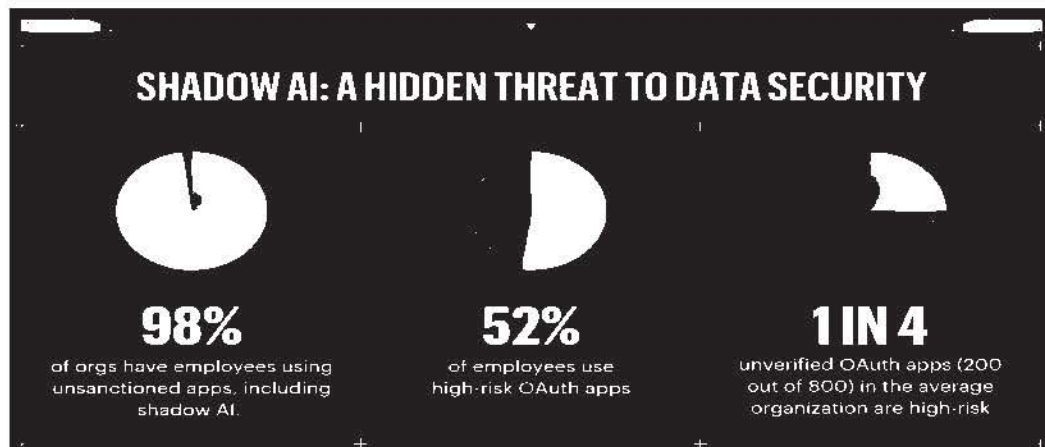
USEFUL RESOURCES:

- CFTC Cybersecurity Education
- CFTC CLA
- CISA Learning
- AI Program Tools
- AI Acceptable Use Guidelines
- Use of CFTC Information and Information Systems Policy



Cyber security checklist for **Individuals**

- ☐ Use strong, unique passwords
- ☐ Enable multi-factor authentication
- ☐ Be cautious with email attachments and links
- ☐ Limit what personal info you share online
- ☐ Avoid public wifi for sensitive transactions
- ☐ Exercise caution when using artificial intelligence (AI) tools
- ☐ Use encryption for sensitive information
- ☐ Stay informed about cyber security threats



SECURITY is your RESPONSIBILITY!!

For questions, please contact the CFTC Cybersecurity Awareness Training & Education Team – CTraining@CFTC.gov

From: [CFTC Communication](#)
To: [All CFTC](#)
Subject: Important Security Notice: Personal Device Connection to CFTC Network or Equipment Prohibited
Date: Wednesday, March 11, 2026 10:04:56 AM

CFTC COMMUNICATION

SUBJECT: Important Security Notice: Personal Device Connection to CFTC Network or Equipment Prohibited

Maintaining the security and integrity of our network is a shared responsibility and requires consistent adherence to established cybersecurity practices.

What do I need to know?

- Personal devices **must not** be connected to CFTC equipment or to the CFTC network under any circumstances, especially for charging purposes.
- Such connections trigger alarms which could result in the affected network port to be immediately disabled.
- Additional actions, such as sanitizing of the equipment to which a personal device was connected may need to be undertaken.
- Prohibited actions includes, but is not limited to:
 - Connecting personal cell phones connected to docking stations for charging.
 - Connecting personal phones to work laptops via USB cables for charging.
 - Connecting personal computers, tablets, smartwatches, flash drives, or external hard drives to the work laptop or the docking station for any reason.
 - Connecting any non-CFTC-issued device to docking stations or network ports.

Connecting personal devices to the CFTC network or equipment can introduce malware, create unauthorized access points, and put sensitive organizational data at risk. Even connecting “just for charging” can unintentionally transmit data or create vulnerabilities.

What do I need to do?

- To protect our network; and our data, please use only CFTC-issued equipment with CFTC systems and approved charging methods.
- If you need to charge a personal device, please use a wall outlet with your personal charging adapter, not your workstation equipment.