



Risk Alert







Meaningful. Actionable. Timely.

July 11, 2024

Airplane Wi-Fi Cyberattacks

Recent warnings from the Federal Bureau of Investigations (FBI) and Transportation Security Administration (TSA) have highlighted significant cybersecurity risks associated with using in-flight Wi-Fi networks. These networks often lack robust security protocols, making them attractive targets for hackers who can intercept communications, set up rogue networks, and exploit device vulnerabilities. This poses a risk to both personal and professional data on connected devices, potentially leading to data breaches and significant operational and reputational damage. All university personnel are advised to exercise caution and follow best practices when connecting to Wi-Fi networks while traveling.

Potential Risk Impacts to the University

-  **Data Breach and Leakage**
If university employees connect to in-flight Wi-Fi and their devices are compromised, sensitive university data, including research, student records, and confidential communications, could be exposed.
-  **Financial Loss:**
Cyberattacks could lead to financial repercussions, including costs associated with data recovery, legal fees, potential regulatory fines, and loss of funding or donations due to damaged reputation.
-  **Operational Disruption:**
Compromised devices can lead to the spread of malware within the university's network, disrupting administrative functions, online classes, and other critical operations.
-  **Reputational Damage:**
A data breach involving university employees could severely damage the institution's reputation, eroding trust among students, parents, faculty, and donors.
-  **Compliance Issues:**
Unauthorized access to sensitive information can result in non-compliance with data protection regulations, leading to potential legal actions and fines.
-  **Intellectual Property Theft:**
Research data and intellectual property can be targeted, leading to theft of valuable information that could be used by competitors or malicious actors.



Alert Type

Awareness

Watch

Warning



"I cannot stress enough the critical importance of avoiding in-flight Wi-Fi without proper security measures, as a single lapse can jeopardize the entire university's sensitive data and operational integrity."

– FAMU Chief Risk Officer Deidre Melton

Tips for Securing Devices and Data While Traveling

1. **Use a VPN (Virtual Private Network):** Always use a VPN when connecting to public or hotel Wi-Fi networks. A VPN encrypts your internet traffic, making it difficult for hackers to intercept and access your data.
2. **Avoid Public Wi-Fi for Sensitive Activities:** Refrain from accessing sensitive information, such as university emails or financial accounts, over public Wi-Fi. Use a FAMU hotspot or wait until you are on a secure, private network.
3. **Keep Devices Updated:** Ensure all your devices (laptops, smartphones, tablets) have the latest security updates and patches installed before traveling.
4. **Enable Device Encryption:** Use full-disk encryption on all devices to protect data in case they are lost or stolen.
5. **Use Strong, Unique Passwords:** Ensure that all your accounts have strong, unique passwords. Consider using a password manager to keep track of them securely.
6. **Enable Multi-Factor Authentication (MFA):** Enable MFA on all accounts that offer it to add an extra layer of security.
7. **Disable Auto-Connect to Wi-Fi Networks:** Turn off the auto-connect feature on your devices to prevent them from automatically connecting to unknown and potentially insecure Wi-Fi networks.
8. **Be Wary of Fake Wi-Fi Networks:** Verify the legitimacy of Wi-Fi networks before connecting. Confirm the network name with hotel or airport staff to avoid connecting to malicious networks set up by hackers.
9. **Secure Your Devices Physically:** Always keep your devices with you. Use a laptop lock in public places and ensure your devices are never left unattended.
10. **Regularly Back Up Data:** Perform regular backups of your data to a secure location. In case of a device compromise, you can restore your information without significant loss.
11. **Monitor Accounts for Suspicious Activity:** Regularly check your accounts for any unusual activity and report any suspicious actions immediately to your IT department.
12. **Educate Yourself and Your Team:** Stay informed about the latest cybersecurity threats and share this knowledge with your team. Encourage a culture of vigilance and proactive security measures.

ERM TEAM



Deidre Melton
Chief Risk Officer

William Knight
ERM Coordinator

Anthony Durden
ERM Intern

ERM Contact Info



Phone
850-412-5479



Email
erm@famuedu