**Describe two WLAN vulnerabilities that present risks for Alliah, based on the details in the scenario**

1. Evil Twin - "An evil twin attack is a spoofing cyberattack that tricks a user into connecting to a fake Wi-Fi access point that mimics a legitimate network". (Panda Security, Many Evil Twin attacks involve a captive portal, designed to mimic the captive portal login page of the original WLAN. This allows malicious attackers to harvest credentials. When an Evil Twin attack is used on a corporate WLAN the attacker is able to harvest domain credentials, they are also able to monitor traffic that is being passed through the Evil Twin.

2. Denial of Service -

**Describe two mobile vulnerabilities that present risks for Alliah, based on the details in the scenario**

1. Malicious Applications (Malware)

2. Browser Exploits

**Summarize the steps for mitigating each identified WLAN and mobile vulnerability, including the specific tools or documentation that will be needed for mitigation.**

To Summarize....

1. Evil Twin mitigation

2. Denial of Service mitigation

3. Malicious Applications (Malware)

4. Browser Exploits

**Recommend preventive measures to maintain the security posture of WLAN and mobile environments in a small business, such as Alliah. Reference federal, state, or industry regulations that justify these measures.**

**Recommend a solution for the company's BYOD approach, including research to justify your recommendation.**

References

1. Panda Security - Evil Twin - https://www.pandasecurity.com/en/mediacenter/security/what-is-an-evil-twin-attack/