5 TIPS

Best Practices for Enhancing Security During Client Visits

Slawomir Jasinski

Solutions Architect, AI Consultant

01

Always Log Out

Always log out from all devices when stepping away, even for brief moments.

This simple action prevents unauthorized access to sensitive information, crucial when leaving devices unattended in a meeting room or public space.

02

Screen Privacy Protectors

Implement screen privacy filters when working in environments where others might see your screen, like cafes or communal workspaces.

This helps maintain confidentiality and prevents data leakage in public settings.

03

Secure Your Wi-Fi Connection

Opt for secure network connections by using either the client's network or your own secure mobile data, especially important in uncontrolled environments like hotels or conferences where Wi-Fi may not be secure.

04

Caution with USB Devices

Avoid using unfamiliar USBs or external devices on your laptop, particularly relevant in scenarios like conferences or workshops where sharing of digital materials is common.

Such devices could introduce malware or compromise system security.

05

Multi-Factor Authentication (MFA)

Enhance access security with MFA or physical security keys like YubiKey, which are essential when accessing sensitive information from potentially insecure locations, adding an extra layer of protection to ensure that only you can access your accounts.

FOLLOW ME

For more tips on working with clients every day.

Slawomir Jasinski

www.jasinski.us