Intrada
TECHNOLOGIES

HOW TO SAFELY USE PUBLIC WI-FI

Tips for Staying Safe

Public Wi-Fi, accessible in locations such as cafes, airports, and hotels, frequently falls short in security, making it an attractive target for hackers and cybercriminals. The lack of encryption on these networks leaves personal information, including login credentials and sensitive data, vulnerable to interception.

If you must use public Wi-Fi, here are some recommended safety measures to protect your data:

1. **Verify the Network:** Always confirm Wi-Fi networks with the hotel staff or business to avoid connecting to a rogue hotspot.
2. **Update Software:** Regularly update your device's operating system and security software to protect against vulnerabilities that could be exploited by attackers on the network.
3. **Enable firewall and use antivirus or EDR software:** Ensuring your device is protected with up-to-date security software adds an additional layer of defense against potential cyber threats.
4. **Disable Auto-Connect:** Turn off the setting that automatically connects your device to available Wi-Fi networks to prevent inadvertent connections to unsecured networks.
5. **Avoid Sensitive Transactions:** Refrain from accessing sensitive accounts or making financial transactions while connected to public Wi-Fi.
6. **Use a VPN:** Ensure your connection is encrypted by using a VPN, which provides an additional layer of security by encrypting all the data transmitted between your device and the internet.

Taking precautions significantly lowers the risk of data theft, offering a safer experience on public Wi-Fi. Using your phone's hotspot is a safer alternative, creating a secure Wi-Fi network connection for other devices. Just be aware that hotspots consume more battery life, so make sure your data plan can support your requirements, such as video calls or large file transfers.

31 Ashler Manor Drive
Muncy, PA 17756

intradatech.com
800-858-5745

Exceeding
Expectations.