Who Knows What Evil Lurks in the Hearts of Public Wi-Fi?

Your employees are the biggest risk to the security of your networks.

According to Politico, an IT company set up various fake Wi-Fi networks around the RNC with names such as “Google Starbucks,” “I vote Trump! free Internet” and “I vote Hillary! free Internet.” The goal was to see how many people would join the unsecured networks. The answer: 1,200, with 68 percent compromising the information on their devices.

“I use public Wi-Fi all the time,” you say. “After all, wireless data is expensive. What’s the harm in using a public network?”

Watch this **video**, and then let’s chat about how to discuss this important security issue with your employees.

As I’ve mentioned before, your employees are the biggest risk to the security of your networks. And, as the RNC experiment illustrates, one of the biggest dangers they pose is exposing your data on unsecured public Wi-Fi networks.

So, what’s the solution? Let me offer 5 suggestions, each of which boils down to training and cyber-education.

1. Knowledge. Ensure that your employees understand the risk and act with caution. They need to know that public Wi-Fi is inherently insecure, that any device that connects to public Wi-Fi (laptop, smartphone, or tablet) is at risk, and that they should treat all public Wi-Fi links with suspicion.

2. Avoidance. Your employees should avoid public Wi-Fi when possible, and use a cellular connection instead. They should also beware what they share, and avoid accessing certain websites—those that expose sensitive information (bank accounts or credit-card information), and those that expose personal information that cyber criminals can use for phishing or social engineering (*e.g.*, social media).

3. Confirmation. If your employees must use public Wi-Fi, they should not do so without first confirming the legitimacy of the link. As the RNC experiment illustrates, they cannot assume that “Google Starbucks” is a valid Wi-Fi network. Cyber criminals often try to scam users by using bogus links with a connection name deliberately similar to a legitimate coffee shop, hotel, or other venue. They should not connect until they can confirm the legitimacy of Wi-Fi access point via the connection’s name and IP address with an employee at the location that is offering the public Wi-Fi.

4. Protection. Consider offering your employees a virtual private network to use. A VPN establishes a private pipeline that encrypts all data that passes through the network. This can help to prevent cyber criminals from intercepting data, even on public Wi-Fi. If a VPN is not available, they should at least use SSL connections (connecting via “https” instead of “http”), which will add an extra layer of encryption to transmitted data. It’s far from perfect, but it’s better than nothing.

5. Disconnection. Your employees should turn off Wi-Fi on their devices when not using it. Even if you are not actively connected to a network, the Wi-Fi hardware in your device is still transmitting data. And if you're transmitting, you are attracting cyber criminals to snoop. If you don't need the Wi-Fi connection, turn it off. Bonus—much longer battery life.

The 1,200 conventioneers who connected to the bogus hot spots exposed bank account information, emails, and messaging apps, but the content they accessed the most? Pokémon Go.