Security Awareness Tips

Use Caution Online While Away From Home or Office

The next time you're looking for a wireless hot spot and locate one called Free Wi-Fi, beware – you could become victim to the latest technology scam.

These Wi-Fi scams are enabling hackers to access personal information, emails, usernames, passwords and credit card numbers. This can happen anywhere you try to connect to the internet while on the go, but it is especially prevalent at airports.

The problem occurs when you think you are connecting to an actual hot spot but it is really a peer-to-peer or computer-to-computer network. The only reason you have access to the internet is because the attacker has set up their PC to allow people to browse the Internet through their connection. Since you're using their internet connection, all your traffic goes through their computer, which means he/she can see everything you do online. And, the worst part of it is you can't actually see what's happening – the hacker can steal information or plant a virus, leaving you completely unaware.

This is especially dangerous for business travelers whose laptops may be attacked by a virus when they unknowingly connect to a peer-to-peer network while on the road. When they return to the office and connect to their company's network, that virus can then affect others.

Computer hackers are motivated by a variety of reasons. Some want to interfere with networks to do damage, commit fraud or steal data, or view breaking security as a challenge.

And even if your devices have virus scanners and enforced security measures, you aren't completely safe. Unfortunately, hackers see most security systems as a test, not an obstacle.

Security Tips

The truth is no one connected to any computer network is ever safe from these attacks. But you can try to limit your risk by following these security tips:

- Do not connect to unfamiliar networks.
- Never connect to a network identified as computer-to-computer.
- Make sure your computer is not set up to automatically connect to networks.
- Turn off file sharing while on the road.
- Use antivirus software and keep it updated.
- Install security patches.
- Use a firewall.
- Use your browser's security settings.
- Avoid opening email attachments.
- Treat Instant Messaging suspiciously.

For more information on protecting your portable technologies from threats...

FBI–Cyber investigations: How to Protect Your Computer:
www.fbi.gov/cyberinvest/protect_online.htm

Better Business Bureau – Business Travelers Beware:
www.bbb.org/alerts/article.asp?ID=770

AlliedBarton® Security Services

Local Response | National Support