Using Public WiFi? Protect Yourself From Attacks First

[fa icon="calendar"] May 18, 2016 9:09:49 AM / by Michael Stone

The coffee-drinking, frequent-flying, hotel-sleeping faithful that depends on businesses offering free WiFi might already know it, but let's have TechQuickie's Linus Sebastian remind us: "Public WiFi is about as secure as a screen door — made of cheese." An exaggeration? Maybe.

But some might be surprised at how insecure such connections can be. New York Times tech columnist David Pogue noted his shock back in 2007. Three years prior, he wrote an article that "attempted to throw water on scare-tactic computer-magazine articles" that preached about the insecurity.

Pogue's change of heart came after a tech consultant used a coffee shop's WiFi to see copies of all Pogue's sent and received emails, the websites he visited and those websites' display graphics.

The consultant was essentially a person acting between Pogue and his connection, leading to such an attack being commonly called a "man-in-the-middle attack." (This is demonstrated in a quick video by AARP.)

The consultant's spying was done through a free program called Eavesdrop, and this and similar programs are readily available across the Web and can be easy to operate for even the least techy of users.

Filter by Topic

Healthcare (27)
Finance (22)
Government (18)
Retail (18)
Service Providers (16)
Higher Education (15)
K-12 (14)

Pogue's demonstration was nearly a decade ago, of course, but the problem persists.

Many of today's larger, company-wide hacks and advanced persistent threats come via other methods. They include: easy-to-guess passwords, like Passw0rd; phishing, or setting up fake websites and other cyber entities that seem legitimate to get employees to enter sensitive information; and watering-hole attacks, or inserting malware into sites external to the company's but that workers might visit often, like Forbes.com and financial- and defense-industry employees.

While the specifics of individual attacks over public WiFi might be less reported because it's typically the individual that's affected, pieces of work-related information certainly could lead back to the individual's employer.

To prevent public WiFi attacks, experts continue to put out warnings that advise:

- ✓ Asking a staff member of the business to confirm the network's exact name because that "Free WiFi" network could be a trap.
- ✓ Making the connection more secure by installing a virtual private network, or VPN, on Windows, Mac, and Android or iOS mobile devices.
- ✓ Visiting only sites that are SSL- or TLS-enabled, meaning the user sees "https" instead of just "http" in the URL. (The major common players, such as Gmail, YouTube, Facebook, banks and credit-card companies, are already going to be encrypted by "https," but any and all sites can have it equipped by installing HTTPS Everywhere.)
- ✓ Avoiding mobile apps because the user can't see whether there's "https" encryption — and it should be assumed there isn't.
- ✓ Disabling mobile devices from automatically connecting to in-range WiFi networks.
- ✓ Having different passwords for different sites so one password isn't a single key that fits all logins, including those that provide access to the user's work network.

Read tips on evaluating and improving your security posture

Download Now

Written by Michael Stone

Michael Stone is a writer and photographer based in Gainesville, Florida, who has had his work published in several newspapers, magazines, and websites. He writes about a variety of topics, including technology and its impact on healthcare and education. He holds degrees in journalism and communications from the University of Florida and Middle Tennessee State University. You can read more about him on his website, www.MichaelStoneOnline.com.