BLINN.COMmunications

August 2019

179 Caren Avenue • Worthington • Ohio 43085-2520 • 718.577.1054 (NYC) • 614.785.9359 (Ohio)

Portable and Dangerous to Your Data (Part One)

Just about everybody has a mobile phone and more than 4 in 5 of us have smart phones, a number that is doubtless higher for business owners and workers. There's convenience and danger here.

The Pew Research Center says 96% of people in the 18-29 age range have smart phones. The percentage never drops below 50%, even for those who are 65 and older. More than half of us have tablet computers and about the same number have either desktop or notebook computers. Desktop systems stay put but smart phones, notebook computers, and tablets add up to a huge number of devices that are constantly in motion.

These devices contain user names and passwords, financial data, and maybe some proprietary files from the office. Perhaps you have a thumb drive or two in your pocket, briefcase, or purse and most thumb drives are not encrypted so anyone who finds one that you've lost will have access to your private information.

It's no surprise that security experts are concerned about loss or theft of these devices, but the situation is even more alarming when we consider how many devices are used in locations with public Wi-Fi systems that are entirely open.

The convenience the devices provide is wonderful and it's easy to forget about the dangers or to simply ignore them and hope for the best. We've just passed the 50th anniversary of the first lunar landing. The results would not have been as good if the rocket scientists had known about potential dangers and then simply decided to ignore them and hope for the best.

NASA learned that lesson in 1986 when the shuttle Challenger was cleared for launch even though some raised the issue of problems caused by low overnight temperatures. We can't foresee everything, but it's not wise to ignore conditions that have the potential for disaster.

Portable devices offer great convenience for us and also for data thieves.

Even so, convenience and security are almost always at odds with each other. Security means using a device will be more difficult while ease of use means that the device will be less secure.

Every situation is different and that makes the problem even more complex, but security must be a given. "Oh, there's nothing important on my phone," is an answer that is neither adequate nor honest. It's impossible to imagine a smart phone that doesn't contain credentials for on-line services at the very least and most people's smart phones, tablets, and notebook computers contain far more valuable data.

If your electronic device is lost or stolen, you'll have to pay to replace the device. The data, however, is another story. It is far harder to replace and much more valuable to thieves.

There's no one-size-fits-all solution, so the cost of security varies. Costs include the obvious (what you pay for security software, hardware, and services) and those that are less visible (costs that accrue from inconvenience). These costs need to be considered and balanced against the potential cost of losing control of essential data.

Severe and Worsening

It's not uncommon for smart phones to have 32GB or even 64GB of memory and you can buy a 256GB SD card for about $30 and plug it into your notebook computer.

Add a 256GB thumb drive or two (around $30 each) and you could easily carry the equivalent of nearly 250 million pages of text. That, in fact, is why some corporations forbid the use of thumb drives and may even go so far as to block the USB ports on any devices owned by the company.

When important business documents are copied to a thumb drive and taken home for review, the result can be disastrous. A lost thumb drive exposes the company's information, but that's only part of the problem. Maybe the home computer the employee uses to work on data at night has a virus. That virus loads itself onto the thumb drive and, when

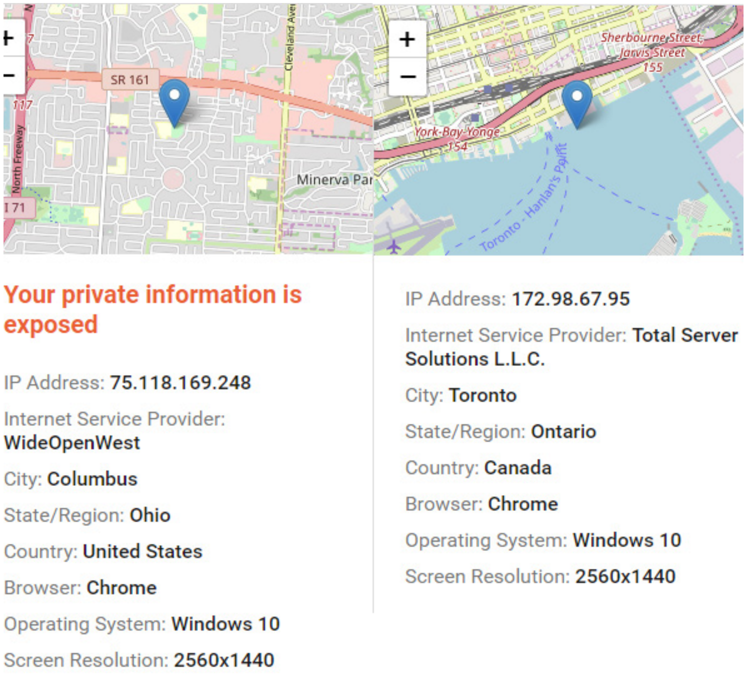
the employee plugs the device into the office computer to update the files, the USB drive loads the virus onto the computer. And then? Then it begins replicating across the network, infecting other desktop computers and potentially compromising the company's servers.

Thumb drives terrify some system managers, and three good reasons exist for that fear: A lost or stolen thumb drive can contain an enormous amount of proprietary data, a disgruntled employee with high access can walk out of the office with a every important file on a single easily concealed device, and thieves can drop infected thumb drives in a parking lot hoping that an employee will take the "found" drive inside and plug it in.

The disadvantage to thumb drives, from a crook's perspective, is that these are physical devices that must be in the crook's possession to be useful. Wi-Fi hotspots are far more valuable to crooks. All they have to do is set up shop where people use a hotspot, create their own bogus but realistic hotspot, and wait for people to connect.

The danger varies. I live in a suburban Columbus city, population about 13,000. Columbus has a population nearing one million and the metro area is a little over two million people. Coffee shops and restaurants near me have Wi-Fi hotspots, but there aren't a lot of high-value targets here. Going naked on a Wi-Fi hotspot at the nearby McDonald's probably isn't risky but I still use VPN software.

Crooks aren't stupid. Bank robber Willie Sutton said that he decided to rob banks "because that's where the money is." If you're a data thief, you'll probably hang out in airports because that's where the data is. (Or, if you want to be pedantic about it, that's where the data are.) They sit in an airport and observe all the unencrypted data that's available for the taking.



Your private information is exposed

IP Address: 75.118.169.248

Internet Service Provider: WideOpenWest

City: Columbus

State/Region: Ohio

Country: United States

Browser: Chrome

Operating System: Windows 10

Screen Resolution: 2560x1440

IP Address: 172.98.67.95

Internet Service Provider: Total Server Solutions L.L.C.

City: Toronto

State/Region: Ontario

Country: Canada

Browser: Chrome

Operating System: Windows 10

Screen Resolution: 2560x1440

I live in Worthington, Ohio, a suburb of Columbus. When my VPN is inactive, it's easy to obtain my IP address, the internet service provider, and an approximate location. The blue pin on the left is about 3 miles from my house. With an active VPN, much of this information is hidden and the blue pin on the right is about 430 miles from my house.

Once they've pulled user names and passwords out of the air, thieves can gain access to protected resources at their leisure.

Phones and tablets are a double threat because they usually come with large amounts of built-in memory and they can communicate wirelessly over non-secure networks, so thieves have two opportunities: They can steal the physical device or they can steal data as it's being transmitted to an open Wi-Fi hotspot.

How Crooks Use Wi-Fi

It's not difficult and you can do it. The software needed is commonly available and free.

These applications are primarily intended to be used for troubleshooting and analysis. Use a search engine to locate and download FaceNiff, Firesheep, Ethereal, or Wireshark; then visit a nearby restaurant, coffee shop, or library where Wi-Fi is in use. Customers who visit public Wi-Fi hotspots interest criminals and data thieves. Large organizations have already deployed public Wi-Fi security technologies, so it's easier to steal data from locations that lack security. Without encryption, your data is public.

VPN applications have other benefits, including the ability to make it harder for organizations to track you. Identity protection obscures information about you when you are browsing. The VPN hides your location and even your internet service provider.

Next month, we'll continue to look at security problems and examine additional solutions to protect both you and your data.