USING PUBLIC WI-FI IS LIKE POSTING ON A BILLBOARD
Elizabeth Weise – USA Today – 2/26/16

SAN FRANCISCO – Public Wi-Fi systems such as those found on airplanes, in cafes or at malls are completely insecure and anyone using them should think of everything they type as being broadcast to a billboard in Times Square, say security professionals.

It came as no shock to experts that a USA TODAY columnist had his email hacked when he used his plane's Gogo onboard Wi-Fi network as he flew home to North Carolina last week. The hacker could have used a device or software to access the columnist's data flow. Both are easy to find online, said John Kuhn, a senior threat researcher with IBM Security. "These tools are reasonably priced and you don't have to be extremely technical to use them," he said.

However easy it might be, electronic eavesdropping is still illegal, said Joel Reidenberg, director of the Center on Law and Information Policy at Fordham Law School in New York City. "It's an Electronic Communications Privacy Act violation and subject to fines of up to $10,000," he said. The law dates to 1986.

There's nothing magically safe about Wi-Fi purchased on a plane. The only thing that makes a flight slightly more secure than a mall or Starbucks with free Wi-Fi is that there are potentially fewer people around because it's "limited to the population of the plane in which you're flying," said Michael Belton, vice president of applied research at Optiv, a security firm. Many people are also fooled into using fake Wi-Fi hotspots in airports, notes Pierluigi Stella, chief technical officer for Network Box USA.

"Say you are in the San Francisco airport and your wireless shows SFAIrport, no password, free connection. How many people do you think have the skills or even the mindset to question the legitimacy of that wireless connection? And wonder if that's nothing more than a hacker's device lurking around? You connect, you browse, you email, and all the while, he's logging all your data and hacking your computer," Stella said. In-flight hotspots can also be faked, said John Gunn, vice president of communications for VASCO Data Security.

"A hacker can go on a flight that has no Wi-Fi and present an open network with the name of the airline, and people connect to it thinking it is legit. They try to reach popular websites and the hacker can present the login screen to capture their user name and password, and then present an error message, after which the hacker has access to the account when they land."

Another common fake-out occurs in hotels. "Many hackers present spoof Wi-Fi networks, such as 'HILTON GUEST WIFI.' If they have a stronger signal than the hotel, it will appear as a preferred choice — ahead of the hotel's legitimate network — and a tired, frustrated traveler doesn't always check," Gunn said. That's why many companies require that employees use a virtual private network, or VPN, when accessing public Wi-Fi.

Gogo itself recommends that for anyone trying to send sensitive information over a public Wi-fi network such as Gogo use a virtual private network to protect their data, said CEO Michael Small. These are available at low and even no cost. "VPN's use strong encryption and are a road block that most criminals do not attempt to overcome," Kuhn said. If you're sending email over a public Wi-Fi network and aren't running a VPN, you should act as if "everything you're working on is being broadcast to a billboard in Times Square," said Belton.