

By Gabriel Perna | 08/27/2010 7:54 PM HKT

Threats Permeate Wi-Fi Hotspots

Latest News in Tech

- Alcatel-Lucent signals revolution in base st...
- Intel to ship flawed chipsets in some cases
- Oscar producers seek tweeting moms on awards...

Article

RATE STORY: +1 EMAIL PRINT SHARE RSS

In the post 9-11 real world, thanks to heightened security measures, an airport terminal is one of the safest places for travel. But in the virtual world, it's still extremely vulnerable.

A recent research note by a leading Symantec engineer warned of potential "scareware," which is a fake anti-virus software system that appears on your computer, floating through a Wi-Fi network in an airport terminal. Web security experts say this type of malware is just one of the many examples of the threats that occur in Wi-Fi hotspots.

"If you're traveling away from home or the workplace where there is a degree of control, as soon as you connect to someone else's network, whether its' an airport terminal, café, hotel or whatever, you're exposed to an internet that you are not in control of," said Paul Wood, senior analyst at Symantec.

An unsafe network means hackers have an easier time spying on potential victims. Once they're on the open Wi-Fi, hackers can sniff out anything that's transmitted through that network. For example, Wood says a hacker could install a key logger on an unsuspecting victim's computer. With that key logger, the hacker would know exactly what that person was typing.

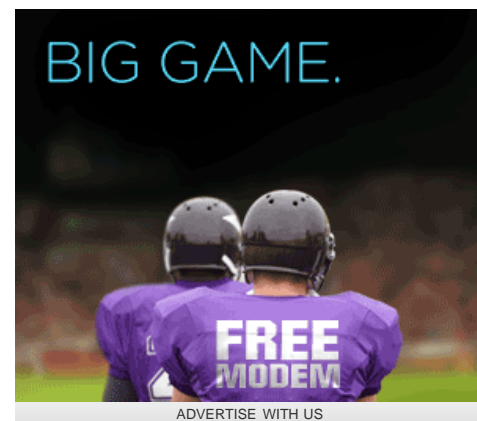
"That means if you log onto social networks or webmail, the hacker will know your passwords. [Social networks](#) are attractive to criminal activity because you can use trusted relationships to spread malware. If I send you a link, and you trust me, you'll probably click on that link. What you don't know is that's taking you to a website with malicious content," Wood said.

Jeremiah Grossman, chief technology officer and co-founder of WhiteHat Security, said unlike Eastern European crime syndicates which pose financial security threats, Wi-Fi hotspot hackers are usually after data.

"They want your data," Grossman said. "If you log into your bank to do a financial transaction, of course they'll steal money. But they're after data."

Beth Jones, senior threat researcher at security antivirus firm Sophos, said while these attacks can happen anywhere, web criminals like to choose hot spots like airports because it's easier to catch people off-guard. In certain airports with shops before security checkpoints, a hacker is able to set up an attack without even buying a ticket. "You can't spot a hacker, it could be someone next to you, it could be someone in the parking lot. They'll set up a hot spot with a very similar name to the official one, and if you're not paying attention, you could easily step into one of those and they'll start monitoring your traffic," Jones said.

Recently, Jones said she was at Boston's Logan International Airport and logged into her computer to sign onto the official airport Wi-Fi. She said she noticed there was another Wi-Fi network called, "Logan



Related Topics



Cybercrime



Social networks



Facebook



Crime

Tech

Today Past week Past Month

1. [Sprint To Unveil Kyocera Phone At New York Event](#)
2. [Confirmed: Sprint To Roll Out Kyocera Echo](#)
3. [How Arianna Huffington managed to lure AOL to buy The Huffington Post](#)
4. [Genzyme, Sanofi boards meet to clinch \\$20 billion deal](#)
5. [With new executive, Google steps up mobile ad](#)

Airport Free Wi-Fi."

"I know for a fact they don't offer free Wi-Fi, so that's not their log-in. But I wonder how many people thought it was, and logged in," Jones said.

The experts agree there are a number of ways to avoid falling victim to Wi-Fi hotspot malware. Grossman said the simplest way is what he calls the "paranoid approach."

"Don't log in somewhere that has data that you can't afford to lose. Only surf the web on safe sites that are encrypted. Facebook, Gmail - those aren't encrypted entirely, so avoid logging into them," Grossman said.

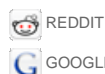
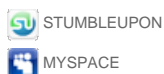
Another suggestion by all three experts was to connect over a VPN (virtual private network) either through work or a home office. This routes all the traffic to a private network, where much of the data is still out in the open, but it's obviously in safe hands.

Grossman also suggests users make sure they are running an upgraded browser. "Don't use IE (Internet Explorer) 6, use Google Chrome, IE 8 or Firefox. In my experience that's the most important thing you can do. Browsers are the gateway," Grossman said.

This article is copyrighted by International Business Times, the [business news](#) leader

SHARE

17 tweets



retweet

RATE THIS STORY: +1 EMAIL PRINT TEXT SIZE: - +

People who viewed this also read

IBTimes

[Alcatel-Lucent signals revolution in base stations](#)

[Intel to ship flawed chipsets in some cases](#)

[Oscar producers seek tweeting moms on awards night](#)

Around the web

[Aging Baby Boomers Reduce Jobless Rate, Matus Says: Tom Keene](#)

[Asian Stocks Fluctuate as Profits Advance, Oil Stocks Retreat](#)

[Asian Stocks Climb Amid Rising Profits, Improved Economic Data](#)

[Asian Stocks Advance as Earnings, U.S. Jobs Bolster Optimism](#)

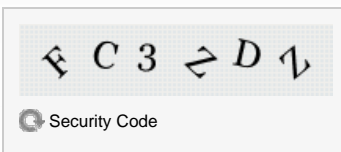
[Japanese Stocks Rise on U.S. Jobs, Earnings; Toyota Advances](#)

[Japanese Stock Futures Rise on U.S. Jobs, Australian Shares](#)

Discuss this Story

ADD COMMENTS AS GUEST OR [SIGN IN](#) TO FOLLOW COMMENTS

*Name



efforts

- 6. Alcatel creates tiny base stations for data surge
- 7. Sony Ericsson's Xperia Play Makes Its Official Debut At Superbowl

ADVERTISE WITH US

Most Popular in

Today Past week Past Month

1. Flying cars set to hit market by 2012
2. Most awaited Super Bowl Commercials 2011
3. Top 5 Bungee Jumping Locations
4. Battle of Titans: Motorola Zoom vs iPad vs Galaxy Tab
5. World Market Overview 8/2/2011
6. China makes fake rice from plastic: report
7. Google makes it easier to build sites for Google TV

FREE e-Newsletters

- Select All
- Entertainment Daily
- Global Choice
- Equities Center

INSIDE IBTIMES

- World
- Australia

TOOLS & FORMATS

- Topics
- RSS Feeds

INTERNATIONAL EDITIONS

- Africa Edition

Tech Insider
Top Finance
Asia Business Watch
The Opinion Desk
Daily Investor
FX Insights
Auto Journal

Health Weekly
Life & Style Times
Travel Guide
IBT Exclusive Offers

Sign up

We value your privacy. Your email address will not be shared.

- Economy
- Global Markets
- Companies
- Tech
- Education
- Travel
- Forex
- Health
- Market Data

- E-Library
- Archives
- Search IBT
- Stock Watch List

- Australia Edition
- Brazil Edition
- China Edition
- Germany Edition
- Hong Kong Edition
- India Edition
- Japan Edition
- Korea Edition
- Mexico Edition
- Russia Edition
- U.K. Edition
- U.S. Edition

ABOUT IBTIMES

[About IBTimes](#) [Terms of Service](#) [Media Kit](#)
[Privacy Policy](#) [The Economic Monitor](#) [Advertise](#)

[HOME](#) | [WORLD](#) | [HK](#) | [ECONOMY](#) | [GLOBAL MARKETS](#) | [COMPANIES](#) | [TECH](#) | [HEALTH](#) | [FOREX](#) | [EDUCATION](#)

© Copyright 2011 International Business Times. All Rights Reserved.