There Is No Vacation from Cybercrime at WiFi Hotspots

BY KENT LAWSON

"More than 12,500,000 Americans were victims of identity fraud last year—one victim every three seconds. Hotspot users need to think before they connect."

GONE ARE THE DAYS when staying connected while you get away from it all meant picking up the phone or sending few postcards to the folks back home. U.S. vacation travelers are addicted to using their smart devices to get online at many of the 825,000 public WiFi hotspots worldwide. A March survey by Prosper Mobile Insights found that nearly eight out of 10 smartphone and tablet users not only bring their devices along on holiday, they use them all the time. Yet, few travelers realize that those smart devices together with their risky behavior at WiFi hotspots create a perfect storm—vastly increasing their risk of identity theft every time they connect.

Since WiFi vulnerabilities were discovered 13 years ago, identity theft has topped the list of consumer complaints at the Federal Trade Commission every single year. Security specialists, journalists, government agencies and consumer watchdog groups have opined nonstop about the dangers of using WiFi hotspots—public-use wireless Internet access networks commonly found in hotels, airports, cafes, libraries, and similar venues.

However, what consumers still seem not to understand is that the majority of WiFi hotspots were designed for convenience, not security. Technologies that make our lives more convenient often tend to make our lives less secure. Nowhere is there a better example of that problematic tradeoff than WiFi hotspots. Since hotspots use radios to transmit data over the public airwaves, the information traveling over them moves at lightning speed, but that data is, by definition, not private. It literally can be grabbed out of thin air. So, it should come as no surprise that the explosion of public WiFi networks and the smartphones and tablets used to connect to them have made these mobile devices top targets for fraudsters. Every time consumers connect to a hotspot without taking proper precautions, they risk having their confidential information stolen in a frightening array of cyber attacks.

Eavesdropping. Using sniffer software that is easy to find (on the Internet) and use, an attacker can intercept unencrypted confidential information sent by hotspot users—everything from passwords and credit card numbers to e-mail and photographs.

Evil twin and man-in-middle attacks. An attacker can set up an evil twin, a rogue hotspot that looks like a real one. When hotspot users connect to an evil twin, without knowing it, they can expose their sensitive online data to hackers. An evil twin can be launched from a laptop at a hotspot or from as far away as 300 feet. Once it has access to your computer, an evil twin can launch a man-in-the-middle (MITM) attack to redirect your traffic to fake websites or mail servers in order to capture passwords and account and payment information.

Sidejacking (session hijacking). In this attack, a hacker does not steal hotspot users' passwords directly; he listens in on users' traffic traveling over unencrypted WiFi networks. Then he saves the user's session cookie information and reuses it to gain access to the sites that were visited. Once a hacker has logged into your vulnerable e-mail or social network accounts, he can send out e-mails or posts in your name and access your friends' e-mail addresses or profiles. In 2010, a Firefox plug-in predator called Firesheep brought sidejacking to the masses.

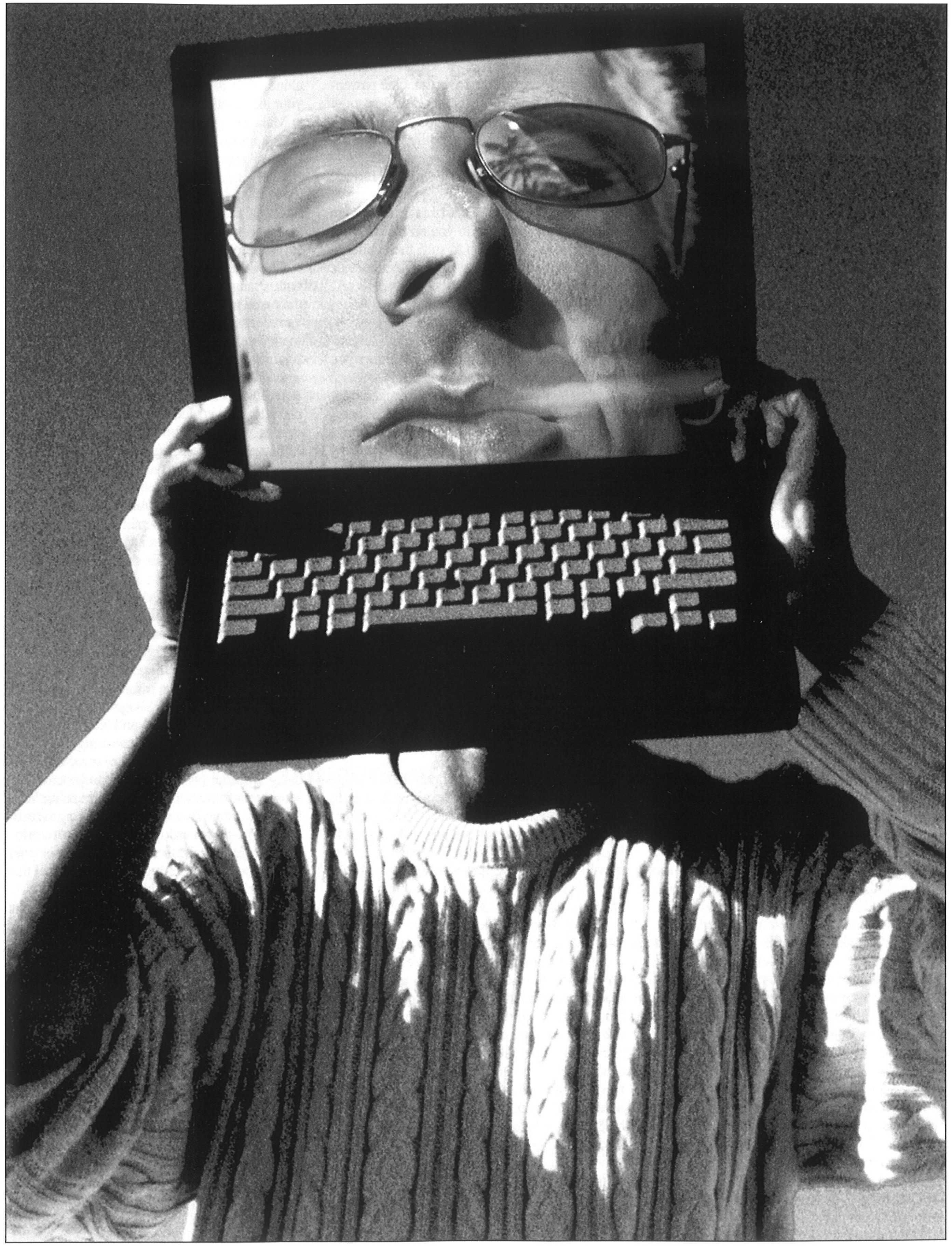
These attacks may sound as though they come straight from the pages of the latest espionage bestseller, but the reality is they are employed around the clock by lone hackers and organized criminal networks. In a 2012 survey by the Cloud Security Alliance of more than 200 enterprise Internet security professionals around the world, four out of five ranked unsecured WiFi hotspots and rogue access points (fake hotspots) among the top security threats.

However, measuring the frequency of hotspot attacks and connecting them to online crimes such as identity theft, credit fraud, and income tax refund fraud is challenging. Hotspot hacking usually is committed by invisible perpetrators against unsuspecting consumers on the move. Nevertheless, the 2012 and 2013 Javelin Strategy & Research Identity Fraud Reports should make the risks of using smart devices at public hotspots painfully clear. This year's report found that smartphone and tablet users in the U.S. are targeted constantly by cyber crooks using malware, exploiting software vulnerabilities, launching phishing and smishing attacks, and compromising unsecured WiFi connections in order to steal users' valuable personal information. Javelin found that tablet owners last year were 80% more likely to become victims of identity fraud: 9.6% compared with 5.3% of all consumers. It also reported that one out of every seven smartphone users was a victim of identity fraud in 2011, a 33% higher incidence rate than the general public. One smartphone user I interviewed had her PayPal account hacked and funds illegally withdrawn within 10 minutes of logging in to a WiFi hotspot.

You might think the mobile cybercrime epidemic would wake up consumers to the dangers of using WiFi hotspots—that it might lead them to take responsibility for their online security. That has not happened. The majority of consumers continue to use hotspots without protecting themselves from the hazards.

In an October 2012 Public WiFi Usage Survey conducted by the Identity Theft Resource Center with my company, 79% of those who responded acknowledged that using public WiFi could lead to identity theft. Yet, 24% said they had made online purchases while using a public hotspot, and 57% admitted to accessing confidential work-related information while using a hotspot. Even more shocking, 44% of those who responded to the survey said they either did not know or did not believe there was a way to protect their data when using a WiFi hotspot. What hotspot users in the survey obviously need is a primer on WiFi hotspot security.

To make matters worse, a 2012 study by Kaspersky Labs, based on data collected by Harris-Interactive, found that smartphone and tablet owners do not take the same security precautions that they routinely take with their desktops and laptops. While 53% of tablet users and 70% of smartphone users access free WiFi hotspots to go online, security solutions are installed on less than half of all tablets and just over one-quarter of mobile phones/smartphones. Contrast this to the 82% of hotspot users who have antivirus software installed on their home PCs and laptops. Another report last year from Juniper Research concluded that the smart device security lapse is even worse: it found that only five percent of global smart-



phones and tablets had security software installed even though those devices account for 57% of hotspot connections, according to the Wireless Broadband Alliance.

Given the media blitz on hotspot hacking dangers, it is troubling that smartphone and tablet users still believe they are invulnerable when they use WiFi hotspots. Whatever the reason, one thing is clear: the quest for mobility and instant connectivity has trumped the need for security. Hotspot users need to remember that, just because their mobile devices are small and easy to use, does not mean they do not contain as much sensitive information as their desktops or laptops. That same information is transmitted across public WiFi networks—everything from names, birthdates, and e-mail to bank log-in, Social Security, and credit card numbers.

It also is troubling that most mobile users—including laptop users—still do not understand the difference between protecting their mobile devices and protecting the information traveling to and from those devices over open wireless networks. Anti-virus and -malware solutions will defend mobile devices against many cyber attacks, but they will do nothing to secure sensitive data traveling to and from mobile devices on public WiFi networks. Yet, the Public WiFi Hotspot Usage Survey found that only 27% of hotspot users routinely use a virtual private network to encrypt their sensitive information.

Nowhere is the hotspot hacking risk greater than when consumers are on the road. That is when they are most dependent on using mobile devices to stay in touch. Vacation travelers may want to connect to a WiFi hotspot with their smartphones to avoid those wildly expensive international roaming charges, or they may be tempted to take out their tablets to pay a few bills online, catch up with friends on Facebook, or check in to see what is going on at work. That is all it takes to become the next vacation hacking victim at WiFi hotspots like these:

Airports and airplanes. WiFi security may be the last thing on air travelers' minds when they are rushing to get through airport security and catch their flight. That is precisely why hackers love air travelers: they often are too tired or distracted to realize that hotspots with names like "Free Airport WiFi" could be fakes designed to steal their personal information. The Better Business Bureau received a complaint from one hotspot hacking victim who believed his WiFi traffic was protected simply because he had gone through airport security—and there is more bad news. Whether airline travelers are using paid hotspots or free ones, their information is not any more secure at 35,000 feet. One airline passenger complained to the Federal Trade Commission that he was hacked in midair. Two days after using a credit card to purchase in-flight WiFi on a trip from San Francisco to Chicago, thousands of dollars in unauthorized charges from iTunes appeared on his credit card statement. First class passengers on long flights make especially juicy hotspot hacking targets.

Trains and train stations. Even though the Federal government runs our nation's railway system, Amtrak's WiFi hotspots are not any more secure than other hotspots. Even worse, virtual private networks are blocked on many of its trains due to limited bandwidth. One passenger wrote my company that his e-mail account was hacked after he logged in using Amtrak WiFi. Hotspot hackers are no different than old fashioned pickpockets who prey on tourists in crowded places, just like the old-fashioned kind, but because they do it online, you rarely will see them at work. That stranger on a train or the one standing next to you on the platform could be using his laptop to sniff the confidential information sent from your mobile device long before you reach your destination.

WiFi-ing under the stars

RV parks and campgrounds. Whether you are planning to hit the road in your RV or rough it with a backpack, many RV parks and campgrounds offer free WiFi so guests can connect under the stars. Since RVers often travel with an assortment of mobile devices, they view WiFi as a basic amenity, not as a luxury, but they are not too happy with RV park hotspots, according to an April survey of rvtravel.com readers. More than half rated park WiFi as terrible, and some mentioned that poor security on many public networks made them think twice about using park hotspots. Yet, hit-or-miss hotspots have not lessened the demand for WiFi in the wild. Some campground operators say their guests would not go camping at all if they did not have Internet access. They simply cannot live without WiFi hotspots. If you are feeling disconnected and you see a hotspot called "Free Campground WiFi," believe it or not, it may not be legitimate. It could be an evil twin set up by a hacker down the road or one in the tent right next to you.

Public parks. Sitting on a park bench while you hop on a hotspot may be a lovely way to spend the afternoon, but a hacker nearby might be sniffing your sensitive information while you are smelling the roses. We went to a hotspot in Central Park, armed with simple hacking tools that anyone can download free online. During a short cyber snooping expedition, we were able to see a wide assortment of sensitive information: consumers checking their online account summaries on bank websites; online shoppers in the checkout line with merchandise from two luxury stores in Manhattan; and tourists logged in to European e-mail services that were not secure.

Hotels. Free WiFi is at the top of the list of amenities hotel guests want: 38% say it is a must, according to a February survey by hotels.com. Some hotels even are offering free WiFi in the lobby but, whether hotel hotspots are free or paid, it is quite likely there is no security at all. Whether you are in your room surfing the Web or answering e-mail by the pool, exercise extreme caution. A hacker in the room right next to you or in the lobby could be looking over your shoulder online. Just because hotel WiFi has a password does not mean you are protected.

Whenever you are using mobile devices at public hotspots, it is safe to assume you are not alone. This is what you need to do to protect your information:

- Make sure you install firewall and anti-malware apps on your mobile devices and promptly install app and OS updates.
- Use long, strong passwords of upper and lower case letters, numbers and symbols, and different passwords for each site—and make sure to uncheck the box that automatically saves them.
- Check before you connect to any hotspots with strange names. Ask the establishment for the name of its hotspot. Watch out for unusual variations in the logo or name of the establishment displayed on the log-in page. That could be a sign it is a fake hotspot designed to steal your data.
- Do not connect to any network name displayed with two little computer symbols. That means you could be connecting directly to someone else's computer, not a legitimate WiFi hotspot. There is no way to tell whether it is safe.
- Disable features that automatically connect your device to any available network. This will prevent you from accidentally connecting to a fake WiFi hotspot or a stranger's computer.
- Disable printer and file sharing options when you are at a hotspot.
- Avoid logging in to websites that do not have secure log-in pages, indicated by the padlock in your browser and https in the URL. Remember, though, an encrypted website only protects the information sent to and from that site. It does not protect all the information sent over a public WiFi hotspot.
- Log out of all websites and turn off wireless connectivity when you are not using it.
- The Federal Trade Commission recommends using a virtual private network to protect your sensitive information when you are using WiFi hotspots: http://www.consumer.ftc.gov/articles/0014-tips-using-public-wi-fi-networks. VPNs (virtual private networks) encrypt your data by sending it through a secure tunnel that makes it invisible to hackers.

Let's face it, online privacy is an oxymoron at public WiFi hotspots. Hotspot hackers are getting better at what they do all the time, and the tools they use to steal users' confidential information are getting more sophisticated. They rarely leave footprints, so they almost never are apprehended. Meanwhile the personal information of their victims is public and free for the taking every time they are logged in to a hotspot. Consumers need to stop ignoring the enormous risks of connecting without protecting their information. Free WiFi is costing us plenty. More than 12,500,000 Americans were victims of identity fraud last year—one victim every three seconds. Hotspot users need to think before they connect. ★

***Kent Lawson** is founder and CEO of Private Communications Corporation, Sherman, Conn., creators of PRIVATE WiFi service.*