# Technology

# Fend Off Electronic Pickpockets

## *Keeping Devices and Credit Cards Secure in a Networked World*

**BY DANIEL J. SIEGEL**

If you haven't watched the TV show "Scorpion," you may want to. The show focuses on an eccentric genius who forms a team of super-geniuses who use their brilliance and technology skills to solve complicated threats that are presumably beyond the average person's intelligence. In a recent episode, the team went to a gaming convention to find a suspect, but before entering the facility, they removed their wallets to prevent what is called either "electronic pickpocketing" or "crowd hacking." But electronic pickpocketing is far more sophisticated than the pickpocketing in the movie "Oliver."

Here is how electronic pickpocketing works. An estimated 90 million credit and debit cards in the United States contained a radio-frequency identification (RFI) chip as of 2012. It's the chip that allows a customer to scan their cards at stores, restaurants and other facilities. But for less than $100, thieves can purchase a device that scans these chips and steals the account information, including your credit card number and expiration date, stored on them. Thus, your account information may be stolen while sitting at your local Starbucks or walking down the street.

Or, perhaps you are at a hotel or convention center for a conference. You decide to log onto the facility's free Wi-Fi Internet. There's only one problem – you haven't logged onto the facility's network, you have instead signed onto a Pineapple, a hacking device that's available for just $99.99. Once you setup the device, the manufacturer says "all of the Internet traffic flowing through the Pineapple such as email, instant messages and browser sessions are easily viewed or even modified by the Pineapple holder." In other words, the operator of the Pineapple can see all of your keystrokes and information, including logins, passwords and account numbers.

What does this mean for the average person? "Thieves can walk by you at a shopping mall and steal your credit card information right out of your purse or wallet from up to 25 feet away, and you won't even know it," according to Chris Gilpin of the National Crime Stop Program. It also means that attorneys must be careful when they are outside of their offices to prevent revealing confidential client information. While it may be hard, if not impossible, for lawyers to keep up with the evolving world of snooping technology, it is not hard to take reasonable precautions to prevent confidential information from getting into the wrong hands.

First, let's consider smartphones. Out of the box, these devices are not particularly secure. After all, they are designed to access information from many "other" sources, and they do that by transmitting and receiving information in the "cloud." The biggest security concerns smartphone users need to address, regardless whether you have an iPhone, an Android or a BlackBerry, typically fall into one of six categories:

- Password theft
- Viruses and data corruption
- Data theft through line sniffing
- Theft of the device itself
- Mobile code vulnerabilities
- Wireless vulnerabilities

While Apple says its iPhone has hardware encryption (encoding), it remains possible to gain access to the information on these devices. In fact, all of the keystrokes entered on an iPhone could be saved and viewed for up to one year, according to McAfee, one of the leading providers of antivirus software. Android devices also have security concerns, and experts regularly debate whether the iPhone's iOS or the Android's operating system is

more secure. Regardless, each has the potential to reveal various actions you take, including:

- Text messages
- Email
- Recently browsed web pages and the entries you make on them.

Fortunately, there are practical and relatively easy ways to secure your phones. In a white paper entitled "Top 10 iPhone Security Tips," McAfee offers advice to securing an iPhone. These tips, which I have revised slightly, apply to all mobile devices:

### ENABLE A PASSCODE LOCK ON YOUR PHONE

Every phone has the ability to use advanced passwords, or a fingerprint, or some other unique identifier, to prevent unauthorized access to the device. You need to determine the features your phone has or whether you need to purchase a third party app that will enhance the pre-installed device security.

### DISABLE FEATURES THAT COULD BE ACCESSED WITHOUT ENTERING THE PASSCODE

Remember, the SD card (the removable thumbnail size card that stores information on your device), and some apps, do not require passwords. In some cases, you can also place apps on the start screen that appear without the need for passwords. As a result, you should not store secure information on an SD card unless it is encrypted, and should not enable apps that bypass the need for entering a password/passcode.

### ADDRESS PRIVACY ISSUES THAT ARE RELATED TO THE DESIGN OF THE PHONE

Because every phone is different, you should review the owner's manual and determine any security issues, and address them, or have your IT staff do so.

### ERASE ALL THE DATA BEFORE YOU RETURN, REPAIR, OR RESELL YOUR PHONE

Never give your phone to a third party without wiping all of the data. Most manufacturers offer detailed instructions how to accomplish this.

### REGULARLY UPDATE YOUR PHONE'S FIRMWARE

Manufacturers regularly update their firmware (the operating system software on these devices) to address security concerns. You should regularly check to see if your firmware is up to date and, if not, install the latest updates promptly.

### DON'T JAILBREAK/ROOT YOUR DEVICE

Jailbreaking or rooting a device means that you are accessing the entire operating system of your device, even areas not intended for end users. Doing so can create security issues, and may void your warranty. You should avoid rooting your device.

### ENABLE THE PHONE'S PRIVACY AND SECURITY SETTINGS

Make sure that you have enabled the device's security settings. For example, don't allow your device to automatically connect to whatever Wi-Fi is nearby. You should require the phone to ask for permission before it takes any actions with any unknown or outside networks or systems.

### USE BLUETOOTH, WI-FI AND EMAIL SECURELY

As noted above, you do not want to automatically connect to other devices or networks. In addition, you should enable encryption on your email so that prying eyes cannot see your email.

### ENABLE APP RESTRICTIONS

Do not install apps without verifying what information they can access. For example, a flashlight app was recently discovered accessing location information and other completely irrelevant data. Most download screens provide a helpful summary of what information an app will access. When in doubt, do not install the app.

### ENABLE "FIND MY PHONE"

There are many apps that enable locating your device, and remotely disabling it or erasing all of your data. For example, your Google account provides that feature for Androids, and there are many third-party apps that offer similar services. Using one of these is a must.

In addition to securing your smartphone, your firm should also have a written policy for all mobile devices, including:

- An official policy detailing the steps your firm will take in the event of a data breach.
- Having written confirmation that all employees are aware of the policy.
- Requiring staff to only store essential information.
- Avoid storing confidential data such

# Tech BRIEFS

## Philadelphia Lawyer's App Pushes Microphilanthropy

A Philadelphia attorney has created Donafy, a smartphone app that allows users to find, notify and donate to nearby nonprofit agencies that serve people in need of legal, food, housing, medical care, mental health and job assistance.

Creator Nikki Johnson-Huston's app said users can become "microphilanthropists" when they see someone in need and use Donafy. The app notifies nearby organizations or in some cases, street response teams, to provide services to the most vulnerable people in the city. The app is only available for iPhone users. Donafy may add an Android version in the future.

The donations are made directly through PayPal. Johnson-Huston said she's not in the donation-taking business. The money goes right to the organization and doesn't go through the app at all. More than 100 nonprofit organizations are linked to the app, with more being added every day. For now, the app's release has been limited to the Philadelphia area because of Johnson-Huston's connection to the nonprofit community here.

Johnson-Huston is a tax attorney who grew up fighting poverty and homelessness. She serves on the boards of several nonprofit agencies. ■

## Criminal Caseload Dashboards Available

Pennsylvania's judiciary has unveiled criminal caseload "dashboards," the latest in a series of interactive, web-based data visuals that allow the public, court staff and researchers to quickly analyze and interpret data related to criminal cases.

The new dashboards provide a detailed look at statewide criminal caseloads, and an overview of each county's criminal case activity over the course of a calendar year.

All of the dashboards can be found on the judiciary's website at www.pacourts.us. Go to the Research and Statistics page and click on "Interactive Data Dashboards." ■

Of course, these solutions don't necessarily answer the question of how to secure the credit cards you carry with RFI chips.

as client Social Security numbers unless absolutely essential.

- Restrict the use of free Wi-Fi. When communicating about client information, attorneys should only do so on secure networks. One of the best ways to accomplish this is to use a mobile hotspot. Most smartphones include a built-in mobile hotspot function, which allows users to work from virtually anywhere. But phone-based hotspots often rapidly deplete the device's battery. Consider using a separate dedicated mobile hotspot. These hotspots can create an Internet connection for five to ten mobile devices, depending on the device and the area where you are located. With only a few steps, the phone creates its own secure Wi-Fi network, without the need for USB or network cables. But remember that these devices use data, so have an adequate data plan.
- Limit yourself to what you need. Only use the devices you need when and where you need them.
- Backup data to a secure location at regular intervals. Backup programs are available for mobile devices, and you should use them. Devices break, and it is essential that you can restore the information and apps quickly and easily.

Of course, these solutions don't necessarily answer the question of how to secure the credit cards you carry with RFI chips. According to Jay Foley, executive director of the Identity Theft Resource Center, there is "no increased threat of fraud from using the smart technology" because the RFI chip cards contain only an account number and expiration date, and not the three-digit security code that's used to authenticate many transmissions. In addition, because the cards generate a unique card-verification number for each transaction, if a thief scanned your card, the security code would not work on the next transaction. But the thief could use the information to make a purchase at online sites that don't require the three digit code.

If you want to have more protection, "Popular Mechanics" recommends that you put a piece of aluminum foil in your wallet (to prevent scanning the cards) or buy a wallet designed to block all RFID transmissions. Or you could simply carry cash, but who does that nowadays?

In short, there are many stories about how data has been stolen from mobile devices. It is essential that lawyers take appropriate precautions to secure their client and other confidential data. ■

---

*Daniel J. Siegel, (dan@danieljsiegel.com), the principal of the Law Offices of Daniel J. Siegel, is a member of the Editorial Board of The Philadelphia Lawyer.*

Tech UPDATE


Epson WorkForce Pro WP-4540

HP Officejet Pro 8630

**TODAY'S SMALL OFFICES AND HOME OFFICES NEED AS MUCH TECHNOLOGY AS THEY CAN GET.** Multi-function printers from Epson and HP do just that. They also copy, scan and fax. There are options to print wirelessly and you can also network several devices together to use these workhorses. You'll spend close to $400, but it's worth it when everything you need is in one place, rather than scattered throughout your office.

| FEATURES | EPSON WORKFORCE PRO WP-4540 | HP OFFICEJET PRO 8630 |
|---|---|---|
| DEVICE TYPE | FAX/COPIER/PRINTER/SCANNER | FAX/COPIER/PRINTER/SCANNER |
| DISPLAY SIZE | 3.5 INCHES | 4.3 INCHES |
| CONNECTIVITY | USB 2.0, WI-FI, WIRED ETHERNET | USB 2.0, WI-FI, WIRED ETHERNET |
| MAX PRINTING SPEED | UP TO 16 PAGES PER MINUTE | UP TO 21 PAGES PER MINUTE |
| MAX SCANNING ORIGINAL SIZE | 8.5 X 14 INCHES | 8.5 X 14 INCHES |
| PHOTO PRINTING | YES | YES |
| DIMENSIONS | 18.1 X 25.7 X 18.2 INCHES | 19.7 X 25.5 X 15.7 INCHES |
| PRICE | $399.00 | $399.99 |