Security Alert

Mobile Devices Pose New Security Hazards

BY LOGAN KUGLER

FROM COFFEE SHOPS to cruise ships, we've become accustomed to having ready access to the Internet—and it's easy to forget how vulnerable that makes us to security threats.

I learned this the hard way recently on a cross-country trip, passing through four cities along the route. Even though I'm well aware of the potential for others to hack into my devices, I'd never had any problems. But there's always a first time: When I got back home, Facebook alerted me to some suspicious activity. I had been hacked!

How to make sure your mobile devices and your data don't get hacked the next time you step out of the house.

Someone in Chicago had logged in to my Facebook account via a Firefox extension—Firesheep (find.pcworld.com/71537)—that can intercept unencrypted cookies from certain Websites on any open Wi-Fi network, making it possible to steal login credentials for sites such as Facebook and Twitter, or even to access your e-mail.

Think it can't happen to you? Think again. Fortunately, a combination of plain old common sense and some technology can protect your devices—quickly and fairly easily.

Tips for Keeping Your Mobile Device Secure

1. Make sure your software is up-to-date: Before every trip, or at least every few weeks, check the manufacturer's Website (or conduct a Google search) to see if a software or firmware update is available. If one is, download it, unless you see a firestorm of negative reviews from early adopters.

2. Employ strong passwords: "Use some combination of letters, numbers, and/or special characters, of 8 characters or more," says Jeremy Miller, director of operations for Kroll Fraud Solutions. "Avoid using dictionary words. Instead, [use] acronyms for things like favorite songs, restaurants, or other items known only to you. And change the password frequently—at least once every six months." If you don't feel clever enough to create your own strong passwords, programs like RoboForm (find.pcworld.com/56186) will do it for you.

3. Don't mess with the security settings: Joe Nocera, an information security expert and a principal with PricewaterhouseCoopers, says that most of the default browser settings in Android, BlackBerry, and iPhone handsets are fairly secure out of the box. "I recommend not going in to change browser security settings—they're pretty good already," he says.

4. Avoid unencrypted public wireless networks: Such networks require no authentication or password for access. In some cases, bad guys set up an open network to snare victims.

Encrypted networks, on the other hand, require an ID or password for access. Such networks are at many hotels that offer Wi-Fi services, and have one of two types of security: WEP (wired equivalent privacy) or WPA (Wi-Fi protected access). The second is more secure—but not invulnerable.

Another precaution: Turn off Wi-Fi when you're not using it. This will prevent you from automatically connecting to networks (and it will also extend your device's battery life).

5. Paying to access a Wi-Fi network doesn't mean it's safe: »

ILLUSTRATION: ANDREW DEGRAFF

PCWORLD.COM

Bad news: Cybercrooks are targeting mobile OSs (find.pcworld.com/71549). Good news: New laws may restrict the use of mobile devices to surreptitiously track your location (find.pcworld.com/71550).

Access fees do not equal security.

6. URLs beginning with 'https:' are safer: When accessing a site where you'll share personal or confidential data—your bank's site, for example—look for *https:* in the URL. The *s* means that you're connected to the site via the Secure Socket Layer (SSL)—so all data transmitted to that site is encrypted.

It's not foolproof, though: On an unencrypted network connection, you may still be subject to a man-in-the-middle (MITM) attack, a form of eavesdropping where the bad guy makes a connection independently with two parties, such that both believe that they are talking directly to each other.

To guard against this, make sure that you are both connected to a secured network and that sites use *https:* when you're entering sensitive information.

Also, says Nocera, most e-mail service providers have both a clear text option (unencrypted data) and an encryption option (SSL). "Make sure you have the SSL option enabled," he advises.

7. Use VPN: If you have access to a virtual private network, use it. A VPN provides secure access to an organization's network and lets you get online behind a secure layer that protects your info.

8. Turn off cookies and autofill: If your mobile device automatically enters passwords and login information into Websites you visit frequently, turn that feature off. (It's a privacy risk.) To get back some of the convenience that autofill offers, try one of the apps (and find more information relating to this article) at find.pcworld.com/71548.

9. Watch your apps: Be selective, Nocera cautions, about the apps you download, particularly in the Android Market, which lacks the strict developer guidelines of Apple's App Store.

10. If you still get hacked: Often you can repair the damage simply by changing your password (to one much stronger) and sending a message via the affected network explaining what happened. And be sure that all your mobile devices have a remote-wipe or autowipe feature, in case one is stolen.

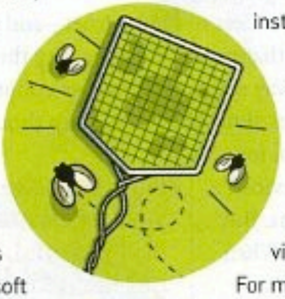
BUGS & FIXES

JAMES MULROY

Microsoft's Latest Updates (and a Fake!)

January's Patch Tuesday proves minor. Plus: new antivirus software updates.

MICROSOFT RELEASED only two security updates in January, an eight-month low. The Patch Tuesday security update of January 11 contains one critical bulletin and another rated important. The updates, MS11-001 and MS11-002, fix vulnerabilities that could allow remote code execution by an attacker.



The critical-rated vulnerability that the company found in Microsoft Data Access Components (a framework for programmers that comes in various Microsoft products, including Windows and Office) could allow remote execution and let the attacker gain the same rights to a PC as the local user—if that user viewed a specially crafted Website that would run malicious code on their computer.

The important-rated vulnerability affects the Windows Backup Manager, which assists users in backing up and restoring a system, including the OS, documents, and settings, in the event of an error. For the system to be harmed, you would have to visit a remote file location and open the file. The file would load into the Windows Backup Manager library, infecting your system and potentially allowing the attacker to gain remote access.

As usual, you should install the updates as soon as possible using Windows Update. To learn more about each one—and to download the two new patches manually—visit find.pcworld.com/71521.

Don't Get Faked Out

While downloading your Microsoft security updates, be sure to avoid a fake update that comes packaged with a computer worm. The fake update seems to have been released intentionally on Tuesday, January 4, in an attempt to coincide with Microsoft's monthly Patch Tuesday.

The update comes attached in an e-mail from no-reply@microsft.com (with Microsoft spelled incorrectly). The message tells the recipient to download the attached file and to follow the instructions on the screen. Microsoft never sends out e-mail messages containing updates. Always follow the standard protocol for updating Microsoft products, and keep your virus definitions up-to-date. For more info, go to find.pcworld.com/71522 and find.pcworld.com/71523.

Antivirus Software Updates

On January 28, antivirus software maker AVG released a number of updates to its virus definitions, its scanner, and many of its modules. If you have AVG software, update it by right-clicking the AVG icon in your system tray and clicking on *Update now*. Or, to update your AVG software manually, visit find.pcworld.com/71524.

McAfee released two Virus Definition Updates, or DATs (database files), on January 27. To update McAfee, right-click on the McAfee icon in the system tray and click on *Update Now*. For more information and to manually update your McAfee software, visit find.pcworld.com/71525.

As for other antivirus tools, Symantec's Norton releases database updates daily and weekly. To download and install the latest security updates, open Norton and select *Run Live Update*. Avast users can receive daily updates by clicking on the Avast icon in the system tray, and then on *Maintenance•Update•Update Engine and Virus Definitions*. For more information and to download the updates manually, visit find.pcworld.com/71526 (Norton) and find.pcworld.com/71527 (Avast).

ILLUSTRATION HARRY CAMPBELL