ANNE KANDRA

Banking on the Web: Risky Business?

The reality behind the risks, plus how to keep your online transactions secure.

PHOTOGRAPH: RICHARD TUSCHMAN

AS A PC WORLD READER, you know how the Internet can make your life easier. But when it comes to conducting sensitive financial transactions—such as applying for a loan, paying the mortgage, or trading stocks—are you inclined to close the browser and reach for the phone?

If so, you have lots of company. The TowerGroup research firm reports that only about one in four banking customers use online banking (numbers are a bit higher for customers age 40 and under). While online banking is clearly gaining in popularity—eMarketer estimates 40 million U.S. households will bank online in 2006, with 5 million more coming on board each year thereafter—it's easy to see why folks might think twice. Every day brings reports about hacker attacks, customer-information thefts, and other security breaches. TV ads feature identity theft victims looking hapless as a stranger's voice crows about buying stereos and trips to Maui. It's enough to make you yearn for your old paper passbook.

The American Bankers Association says consumers cite identity theft as their top concern about online banking. And both the Federal Deposit Insurance Corporation and the Gartner research firm say banks don't adequately educate customers about fraud prevention.

But before you log off your bank's Web site for good (or decide never to check it out at all), remember that most experts agree identity theft is still extremely unlikely to occur as a result of using online banking services. A study by Javelin Strategy and Research found that unsecured online transactions were responsible for fewer than 2.5 percent of identity theft cases. The report even recommends canceling paper bills and statements in order to reduce the risk of theft or loss.

SAFER THAN PAPER

BANK OF AMERICA e-commerce executive Sanjay Gupta says less than 1 percent of fraud at the bank occurs via online transaction. Online banking actually helps protect against fraud, he adds, since it allows customers to confirm transactions and check account balances quickly and easily. Still, Gupta says, "There's a perception that when money is in the vault, it's somehow more secure. We want customers to feel that [online banking] is just as safe—or safer."

To this end, Bank of America and other leading banks and financial institutions have recently introduced new security measures. Bank of America's program, called Sitekey, bolsters simple password protection by adding images and secret questions. The bank also touts a "zero liability" promise that protects customers against any unauthorized charges.

Meanwhile, banks are giving customers incentives to go online. Some banks ▶

have eliminated fees for online services, while charging for things like sending cancelled checks. And financial software programs are increasingly tying features to online banking. For example, most new versions of Quicken let you attach electronic images of cancelled checks (available from some banks) to transaction records, even storing them in encrypted form. Sure beats digging through an old shoe box full of paperwork.

Still on the fence? Here are some tips on keeping financial transactions secure.

BEYOND THE PASSWORD

CHECK YOUR BANK'S online security for features that go beyond a single password. If its security seems bare-bones, ask about plans for improvement.

Make sure the banking site you visit is the real McCoy. Research shows that most online banking fraud now results from *phishing*—where you unwittingly give account and other personal data to a convincing copycat site, typically by clicking a link in an e-mail message. Many ISPs offer antiphishing tools; use them.

Never click on an e-mail link to enter a Web site; use a bookmark or manually enter the URL into your browser instead. And look for signs—such as a secure-encryption icon and working links to customer service—that the site is legit.

Never click on an e-mail link to enter a banking Web site.

Clear your browser's cache periodically to delete the trail of Web sites you've visited. To do this in IE, go to *Tools•Internet Options* and click *Delete Files* under Temporary Internet Files. In Firefox, go to *Tools•Options*, click the *Privacy* icon, then click the *Clear* button next to History.

If you use a feature like Google Desktop Search, be sure it's set up to exclude secure pages (those with URLs that start with "https"). To find the setting, right-click the application icon, select *More*, and then click *Preferences*. Enabling the setting will keep others from accessing sensitive Web pages—those holding account numbers, balances, and other information—by simply doing a desktop search.

KEEP IN TOUCH

THE BEST WAY to ensure that all is as it should be with your bank account is to check in regularly. Print or save PDFs of key transactions. If you store electronic statements and payroll check stubs, it's more important than ever to back up your system regularly. Many banks let you set up automatic notifications when unusual transactions take place, if account balances go below a certain level, or for other circumstances. Consider taking advantage of this feature, if available.

While you're monitoring your bank balances, consider checking your credit report for mistakes, or clues to potential fraudulent activity. Federal law allows you to obtain one free credit report annually from each of the three major credit reporting companies: Experian, Equifax, and TransUnion. Download your report in minutes at www.annualcreditreport.com.

PRIVACY WATCH

Wipe Your Cell Phone's Memory Before Giving It Away

IN LAST MONTH'S *Privacy Watch*, I wrote about the best ways to clear data from an old PC's hard drive before you sell or donate it. But trading in a cell phone can pose an even greater privacy threat: People store PINs, passwords, and other sensitive information on them, and are likely to trade them in more frequently than their PCs. Also, wiping data off a cell phone can be extremely difficult.

If your cell phone stores contacts and other information on a removable SIM card, start by taking the card out. The SIM card doesn't necessarily store all the data on your phone, though. It may store only your phone book, while call logs, photos, memos, and other information might reside in the phone's internal memory.

To get rid of everything, you may need to employ multiple reset commands–and those commands aren't always easy to find in a modern cell phone's complex menus. One Samsung phone I looked at requires you to enter ten different commands to delete all data, including text messages, phone numbers, call timers, and logs. But remember, if you want to keep the numbers stored in your SIM card, by all means remove it before you delete anything!

The folks at ReCellular–a cell phone recycling service–have a great solution: The Cell Phone Data Eraser page (find.pcworld.com/50670) lets you choose the brand and model number of your cell phone, and then displays the precise commands you need to delete every piece of data from it. (If you don't know your phone's model number, try checking underneath the battery.) If you can't find the instructions on that Web site, you'll have to find your manual. What do you do if you've lost that page-turner? Fortunately, most cell service providers offer downloadable copies of the instruction manuals for the phones they sell.

If you think you can circumvent the privacy threat by sending your phone back to your service provider, you could be mistaken. According to one report, a Cingular customer who received a refurbished phone as a replacement for one that malfunctioned found the new phone was filled with the previous owner's private data, including account numbers, user names, and passwords. (For the full story, see find.pcworld.com/50674.)

Once you've taken the steps that are supposed to wipe all traces of data from your phone, double-check to make sure your address book, call logs, and other data stores really are empty. When you're sure everything is gone, you can donate your old phone with peace of mind. See find.pcworld.com/50668 for a list of organizations and companies that accept phone donations. *–Andrew Brandt*

ILLUSTRATION: MARK MATCHO

Finally, you've heard it all before, but it bears repeating: Keep your virus protection updated, use a firewall, disable pop-ups, use passwords that contain both letters and numbers, and change the passwords periodically. Consider securing your PC with a biometric fingerprint reader, generally available for about $30.

Crooks will always be out there, just waiting for a chance to mug you through the Web. But with a little education and some protection for your PC, you can safely bank through your browser. ■

Anne Kandra is a contributing editor, Andrew Brandt is a senior associate editor, and Amber Bouman is an editorial assistant for PC World. *E-mail them at consumerwatch@pcworld.com, privacywatch@pcworld.com, or onyourside@pcworld.com. To read previously published* Consumer Watch, Privacy Watch, *or* On Your Side *columns, visit find.pcworld.com/31703, find.pcworld.com/31706, or find.pcworld.com/31709, respectively.*

ON YOUR SIDE

Who Pays for Tech Support Goof?

AFTER WE PURCHASED a Logitech MX1000 Laser Mouse from ZipZoomFly.com, we found out it was not compatible with the Firefox browser. We called Logitech to try to get the problem solved, but the tech support representative we spoke to said the company had no fix for the problem—and he had no idea when one would be available.

We couldn't find any assistance on ZipZoomFly.com, or even an explanation of the incompatibility. But when we called to ask for our money back, the customer service representative said we would have to pay a 15 percent restocking fee. We feel we should not have to pay for a product that doesn't work properly.

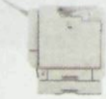
Don and Rita Sutliff
Syracuse, New York

***On Your Side* responds:** Logitech spokesperson Kate Brinks says that contrary to what the company's tech support rep told the Sutliffs, an update that fixes the Firefox incompatibility was available on Logitech's Web site at the time of their call. ZipZoomFly.com says that because of the unusual situation, it has agreed to refund the Sutliffs' $15 restocking fee. However, a ZipZoomFly.com spokesperson pointed out that, like other retailers, it does not provide tech support, and its restocking fee policy is clearly stated on its site.

Bottom line: Be sure to check the product manufacturer's Web site before you phone tech support. That site is the first place to go if you think a product from a reputable vendor is defective.

—Amber Bouman

CL7300D



CL7200

CL4000DN

CL3000e

CL2000N