



## A Matter of Convenience

Let's say you enjoy visiting the neighborhood bank teller and see no reason to bother with the Internet. But what if you need to travel on business, or get laid up from an automobile accident or fall ill for an extended period? What about the busy mother who misplaces her checkbook or is out of postage stamps and bill payments need to get off in the mail today? Wouldn't it be easier to jump online and take care of your banking needs from the convenience of the kitchen, study or home office?

That's the great thing about online banking—the ease and convenience of it all. Plus, when it comes to paying bills online, you can schedule when those payments need to be made so you save money on late fees or other charges, plus you save \$8 to \$12 a month or more on postage stamps and your taste buds by avoiding those nasty tasting envelopes.

Another great advantage about online banking is that you can access information that's not easily available at your branch. You can check, view and print account activity for any date range you specify—no more waiting around for a monthly statement. Online banking also allows you to transfer funds, re-order checks and pay bills—whenever you want.

Getting started is easy. Log onto the website of your bank or credit union and go from there. Signing up usually involves providing basic information like your address and bank account number, signing a privacy agreement and agreeing to pay any fees associated with the account. Typically, if you have enough money in your account, there are no fees. Otherwise, you may have to pay a monthly fee for the bank's online bill-paying service. This varies from bank to bank.

## The Benefits and Risks of Online Banking

One of the most significant and convenient advantages made available to public with the advent of the Internet is online banking. Virtually every banking and credit union organization across the United States now offers such services, which means you can check your account balances, transfer money from checking to savings and vice versa, make mortgage and car payments, and pay your bills—whenever and wherever you have access to a computer and the Internet.

Unfortunately, with such online convenience come certain cyber-risks, which means it's important to educate yourself about how unauthorized access to your financial information occurs, and the steps you can take to protect yourself. This issue of Dollars & Sense provides helpful information for online banking consumers designed to help you gain and retain control of well-being by changing the age-old saying "A penny saved is a penny earned" to "A penny saved is a penny kept." ■

### Begin with Online Bill Pay

If you're considering making the leap to online banking, the best place to start is with online bill pay. With it

*(Continued on page 2)*

### A Matter of Convenience (continued from page 1)

you can pay virtually any company or person in the U.S.—your credit card company, electricity bill, cable bill, or dentist. You can even use bill pay to send money to friends and family. Most banks and credit unions have similar procedures for setting up online bill pay:

**1. Set up your payee.** Your bank credit card or loans are typically already set up for you as payees when you enroll. To set up your other payees, you'll need your bill to find the company address and your account number.

**2. Schedule your payment.** Indicate the amount you want to pay, and when you want the money to be taken out of your checking account. The system lets you know how much time to allow for each payee—it's

usually up to three to five business days before you want the money to get there.

**3. Your payment is sent.** The money is deducted from your account and sent to the recipient as you instructed. If you choose, you can also receive an email confirming that the payment has been sent.

You can also use online bill pay to keep track of your payment history, so you can look back as much as a full year to monitor how much and when you paid each of your payees.

#### What to Look For

If you do decide to begin banking online, here are four suggestions of things to look for:

• **Low fees**—All banks allow you to

check your account activity online for free. Should there be a fee for bill-paying services, find out what it is and if you can save money by going with a different bank or credit union.

• **Customer service**—In case you encounter trouble, make sure it's easy to reach a real person at the bank or the bank's service or help center. Some banks have 24/7 customer service reps on call, others promise to respond to emails within 24 hours.

• **Privacy policy**—The key to knowing how your bank will use your personal information is to read their Privacy Policy. Most such policies state that the financial institution won't sell your information to third parties but they will pass it along to their "affiliated companies"—usually sellers of insurance and investments. Ideally, you want a policy that allows you to disallow the passing of your information to any company, affiliated or not. ■

### Don't Ever Send Personal Information Inside an Email

Most people today can't live without their personal email accounts, because they make connections with friends and family so much easier than the post office trips and interrupting phone calls of past decades. Unfortunately, most spammers and phishers know this too...and they take full advantage of the medium. It's no longer scams like the exiled African princess asking you to send her help until her father's billions are released from a holding bank that can draw people in. These types of email lies are easy to recognize and a swift click of the delete icon will easily remove the nuisance email from your inbox. Today shadow spammers are sending emails masked as your local bank or utility company. Many of these emails are difficult to tell from the real thing. They are becoming more and more convincing, and harder to spot.

#### Common problem emails often come from spammers posing as one of the following companies:

Ebay, PayPal, the IRS, Chase Bank, Citibank, Bank of America, Capital One, and just about any other local bank, financial institution and/or company that issues bank or credit cards like Sears and others.

Many of these emails will show up in your inbox as activity alerts, or warnings that your online account has been compromised. It is important to evaluate each one of these emails individually. First ask yourself, "Do I even have an account with these people?" Eighty percent of the time, you won't even have a reason to associate with that organization. Next, do not ever click on links presented in these emails. Many of them will simply take you to a fake off-shore site hoping to get your personal information from you. Some, however lead to nasty computer virus downloads, or spyware. Save yourself the headache and ignore the email. Last, if you are worried about the potential warning, call your bank directly or visit their website by typing the address directly into the browser. Many institutions have been alerted to phishing emails that use their names and will have information on their site explaining the false email and steps to take to avoid problems. Remember, don't EVER send personal information in response to one of these emails! ■

# Tips for Safe Online Banking

As explained by US-CERT ([www.us-cert.gov](http://www.us-cert.gov)) when it comes to online banking, there is no way to absolutely guarantee your safety. However, good practices do exist that can reduce the risks posed to your online accounts. Consider these helpful suggestions to increase the chances that best practices are being followed and implemented:

Review your bank's information about its online privacy policies and practices. By law, banks are required to send you a copy of their privacy policies and practices annually; you may also request a copy of this information. Bank websites should also have this information. As you read it, pay particular attention to any mention of the methods used for encrypting transactions and authenticating user information. Also, check to see if the bank requires additional security information before authorizing a payment to a business or individual that has never received a payment before.

Before setting up any online bill payment, check the privacy policy of the company or service you will be sending payment to. You have the right to limit the information an online bank shares with both its parent organization and any other financial institutions. Be aware that some online banks may have separate procedures for handling each of these requests. You may also want to use a service such as the Better Business Bureau to view any existing history of outstanding consumer complaints about privacy violations.

For security purposes, choose an online personal identification number (PIN) that is unique and hard to guess. Be sure to change your PIN regularly. Do not choose a PIN that contains personal information such as your birthday or Social Security number; an attacker might be able to guess these. Regardless of the circumstances, never give someone access to your current PIN number.

Install antivirus, firewall, and anti-spyware programs on your computer and keep them up to date. Installing and updating this software protects your computer and its contents against unauthorized access. You should turn on automatic updates for these programs or, if prompted, always agree to download system updates as soon as they are available.

Regularly check your online account balance for unauthorized activity. Timing is a factor in your response to unauthorized electronic fund transactions. If you receive a paper account balance, make sure that you reconcile it with your online balance.



Use a credit card to pay for online goods and services. Credit cards usually have stronger protection against personal liability claims than debit cards. Some credit cards limit personal liability for unauthorized transactions to \$50. Personal liability for debit cards can be higher. According to the Federal Reserve's Regulation E, if you report an electronic fund transaction problem involving debit cards to a bank or financial institution in the first two days, you are only liable for \$50. Reporting that same incident between 3 and 60 days increases your personal liability to \$500. After 60 days, there are no financial restrictions placed on your personal liability.

Avoid situations where personal information can be intercepted, retrieved, or viewed by unauthorized individuals. You should conduct online bank transactions in locations that are not

subject to public monitoring. When you are entering login information, you should avoid using unsecured or public network connections (for example, at a coffee shop or library). As a general rule, you should avoid using any computer that other people can freely access; the end result could be unauthorized access of your financial information. Remember, it is possible for your account information to be stored in the web browser's temporary memory.

If you receive email correspondence about a financial account, verify its authenticity by contacting your bank or financial institution. You should not reply to any email requests for security information, warnings of an account suspension, opportunities to

make easy money, overseas requests for financial assistance, and so forth. Also, links found in these suspicious emails should not be clicked. Forward a copy of the suspicious email to the Federal Trade Commission at [uce@ftc.com](mailto:uce@ftc.com) and then delete the email from your mailbox.

If you have disclosed financial information to a fraudulent website, file reports with the following organizations:

- Your bank
- The local police
- The Federal Trade Commission: [www.ftc.gov](http://www.ftc.gov)
- The Internet Crime Complaint Center: [www.ic3.gov](http://www.ic3.gov)
- The three major credit bureaus: Equifax, Experian, and TransUnion

### With the Convenience Comes Some Risk

Now that you've gotten a feel for the benefits of online banking, keep in mind that we don't live in a perfect world. Without question, the popularity of online banking also presents some risks and challenges to your financial security and personal privacy.

As recommended by the United States Computer Emergency Readiness Team (US-CERT), ([www.us-cert.gov](http://www.us-cert.gov)), if you are going to use online banking to conduct financial transactions, you should make yourself aware of the risks and take precautions to minimize them. US-CERT is a partnership between the Department of Homeland Security and the public and private sectors. Established in 2003 to protect the nation's Internet infrastructure, US-CERT coordinates defense against and responses to cyber attacks across the nation.

#### Attacks that Target Online Banking

Several types of electronic fraud specifically target online banking. Some of the more popular types to be aware of include:

**Phishing attacks**—Use fake email messages from an agency or individual pretending to represent your bank or financial institution. The email asks you to provide sensitive information (name, password, account number, etc.) and provides links to a counterfeit website. If you follow the link and provide the requested information, intruders can access your personal account information and finances. In some cases, pop-up windows can appear in front of a copy of a genuine bank website. The real web site address is displayed; however, any information you type directly into the pop-up will go to unauthorized users.

**Malware**—The term for maliciously crafted software code. Special computer programs now exist that enable intruders to fool you into believing that traditional security is protecting you during online banking transactions. In fact, it is possible for this type of malicious software to perform the following operations:

**Account information theft**—Malware can capture the keystrokes for your login information, plus it can also monitor and capture other data you use to authenticate your identity (for example, special images that you selected or "magic words" you chose).

**Fake website substitution**—Malware can generate fake web pages that replace your bank's legitimate website. Such a "man-in-the-middle attack" site enables an attacker to intercept your user information. The attacker adds additional fields to the copy of the web page opened in your browser. When you submit the information, it is sent to both the bank and the malicious attacker without your knowledge.

**Account hijacking**—Malware can hijack your browser and transfer funds without your knowledge. When you attempt to log in at a bank website, the software launches a hidden browser window on your computer, logs in to your bank, reads your account balance, and creates a secret fund transfer to the intruder-owned account.

**Pharming**—Pharming attacks involve the installation of malicious code on your computer; however, they can take place without any conscious action on your part. In one type of pharming attack, you open an

email, or an email attachment, that installs malicious code on your computer. Later, you go to a fake website that closely resembles your bank or financial institution. Any information you provide during a visit to the fake site is made available to malicious users.

#### All of These Attack Types Require You to Provide Information

All the attack types just described share one characteristic; in order to succeed they need you to provide information:

- In phishing attacks, you must provide the information or visit links.
- With malware, you may be tricked into performing actions you would not normally do. You would have to install the malware on your computer either by running a program, such as an email attachment, or by visiting a website through email or instant message link. Then, you would have to submit your bank login information. Your financial information would be at risk only after you performed all these steps.
- With pharming attacks, you must open an email, or email attachment, to become vulnerable. You then visit a fake website and, without your knowledge, provide information that compromises your financial identity. ■

### Family Financial Education Foundation

ACCESS EDUCATION SYSTEMS

724 Front Street, Suite 340

Evanston, WY 82930

contact: (888) 292-4333

[www.ffef.org](http://www.ffef.org) | [info@ffef.org](mailto:info@ffef.org)



**If you know of someone who would benefit from this information, please pass this newsletter along.**

*This publication is the property of Family Financial Education Foundation. All rights are reserved. For more information about our services or how we can help you with your debt management program, please contact Family Financial Education Foundation at [www.ffef.org](http://www.ffef.org).*