Protect Your "Cyber Home" With a Solid Foundation

Simple steps to secure your computers and mobile devices for Internet banking and shopping

Your home has locks on the doors and windows to protect your family and prevent thieves from stealing cash, electronics, jewelry and other physical possessions. But do you have deterrents to prevent the loss or theft of your electronic assets, including bank account and other information in your personal computers, at home and when banking or shopping remotely online?

"Think about all of the access points to and from your computer — such as Internet connections, email accounts and wireless networks," said Michael Benardo, manager of the FDIC's Cyber Fraud and Financial Crimes Section. "These always need to be protected. Otherwise, it's like leaving your front door wide open while you are away so that anyone could come in and take what they please."

Consider these strategies.

For Banking by Computer or Mobile Device

Take extra precautions for logging into bank and other financial accounts. These measures include using "strong" user IDs and passwords by choosing combinations of upper- and lower-case letters, numbers, and symbols that are hard for a hacker to guess. Don't use your birthdate, address or other words or numbers that can be easy for con artists to find out or guess. Don't use the same password for different accounts because a criminal who obtains one password can then log in to your other accounts. Keep your user IDs and passwords secret, and change them regularly. Make sure to log out of financial accounts when you complete your transactions or walk away from the computer.

Consider using a separate computer solely for online banking or shopping. A growing number of people are purchasing basic PCs and using them only for banking online and not Web browsing, emailing, social networking, playing games or other activities that are more susceptible to malicious software — known generally as "malware" — that can access computers and steal information. As an alternative, you can use an old PC for this limited purpose, but uninstall any software no longer needed and scan the entire PC to check for malicious software before proceeding.

Take precautions if you provide financial account information to third parties online. For example, some people use online "account aggregation" services that, from one website, can provide a convenient way to pay bills, monitor balances in deposits and investment accounts, and even keep track of your frequent flyer miles. While these websites may be beneficial, they can also present potential issues related to the security of the account information you have shared with them. If you want to use their services, thoroughly research the company behind the website, including making sure that you're dealing with a legitimate entity and not a fraudulent site. Also ask what protections the website offers if it experiences a data breach or loss of data.

Periodically check your bank accounts for signs of fraud. If you bank online, check your deposit accounts and lines of credit at regular intervals to spot and report errors or fraudulent transactions, just as you would review a paper statement. Online banking makes it easier and faster to monitor your accounts. This is important, because the sooner you can detect a problem with a transaction, the easier it should be to fix.

Federal laws generally limit your liability for unauthorized use of your debit, credit and prepaid cards, especially if you report the problem to your financial institution within specified time periods, which vary depending on the circumstances (see Page 8 for more details). A good rule of thumb is to check your accounts online once or twice a week. Also, many banks make it easier for customers to keep track of their accounts by offering email or text message alerts when balances fall below a certain level or when there is a transaction over a certain amount.

A Message to Readers

The Federal Deposit Insurance Corporation has been publishing ***FDIC Consumer News*** quarterly since 1993 to help people protect their money, including tips in practically every issue about how to avoid financial fraud and theft. A lot has changed over the years, especially consumers' increased reliance on computers and the Internet — the "cyber" world — for everything from shopping and communicating to banking and bill paying. While the benefits of faster and more convenient cyber services for bank customers are clear, the risks posed by these services, as well as the strategies for preventing or recovering from cyber-related crimes, may not be as well-known by the average consumer and small business owner.

That is why the FDIC has produced this special edition of our newsletter — a guide to safe online banking that features precautions to take at home and when banking remotely (using laptop computers, smartphones and other mobile devices). We include tips and information for parents and guardians wanting to protect their children from online fraud and identity theft, and for small businesses needing to secure their computer systems and data. You'll also learn about what banks and bank regulators are doing to protect your money.

Note: This and other issues of ***FDIC Consumer News*** can be read or printed at www.fdic.gov/consumernews. Check back there for versions of this issue for e-readers and portable audio (MP3) players. Single copies of this special edition and articles referenced here are available upon request to the FDIC's Public Information Center (toll-free 1-877-275-3342 or publicinfo@fdic.gov). Our publication also may be reprinted in whole or in part without permission.