Does Online Banking Put Your Money at Risk?

Scammers and thieves are out there, but you can protect yourself.
Infamous bank robber Willie Sutton, when asked why banks were his favorite target, responded, "Because that's where the money is."
The modern-day Willie Suttons of the world target bank Web sites for the same reason. With online transactions, money is represented in the form of electronic records of ownership, which means online bank robbers can steal more money, in less time, than by stealing literal currency--and they don't even need a getaway car. But that doesn't mean online banking necessarily has to be a riskier proposition.

"Internet banking is terribly secure," says Brad Adrian, an Internet banking analyst with Gartner. "Financial services providers...make their systems as secure as possible."
But, he says, "unscrupulous people using phishing, keystroke collection, or similar activities" to steal your passwords or account numbers are a growing problem.

Going Phishing

Phishing scams, in which attackers use spoof e-mails and Web sites to lure users into entering personal financial information (such as credit card numbers, bank account information, and passwords), have increased in the last several months. Yet even though public awareness of these scams has grown, people continue to fall victim to them in increasing numbers.
The click-through rate on phishing e-mails is 3 percent, estimates Avivah Litan, vice president and research director at Gartner. That compares with a response rate of about 0.5 percent for spam, he says. One possible reason for this: People take e-mail from their bank very seriously, he says. In part the solution is better customer education, he adds, but banks could also do more to prevent the scams from working in the first place.
Online criminals--including those who phish for a living--have become even more sophisticated, creating fraudulent Web sites and e-mail messages that are harder to detect. Professional phishing criminals even work current events into their attacks to make them seem more realistic: One recent scam, for example, posed as an e-mail soliciting campaign donations.

Protect Yourself

Log on to banks only from a secure computer. Never log on from a public computer in a hotel or cafe, and be careful when logging on to unknown networks with a laptop.
If you get a warning e-mail, call your bank -- don't click on any provided links.
If your computer is acting strangely -- for instance, reacting slowly or getting pop-ups -- avoid using it for online banking until you can get it checked out.

Keep anti-virus and anti-spyware software up to date.
Install and maintain a firewall.
Never respond to any e-mail that requests personal information.
Be leery of fly-by-night, Internet-only banks with high interest rates on savings or checking accounts. Make sure the bank is FDIC-certified and is insured.
And, use a different user name and password for each financial account. The password should be complex, with numbers and symbols, and changed regularly.