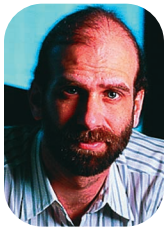
Customers, Passwords, and Web Sites

Criminals follow money. Today, more and more money is on the Internet: millions of people manage their bank, PayPal, or other accounts—and even their stock portfolios—online. It's a tempting target—if criminals can access one of these accounts, they can steal a lot of money.



Bruce Schneier
Counterpane Internet Security

And almost all these accounts are protected only by passwords.

You already know that passwords are insecure. In my book *Secrets and Lies* (published way back in 2000), I wrote: "…password crackers can now break anything that you can reasonably expect a user to memorize."

On the Internet, password security is actually much better than that, because dictionary attacks work best offline. It's one thing to test every possible key on your own computer when you have the actual ciphertext, but it's a much slower process when testing remotely. And if a Web site's creators are halfway clever, the site would shut down an account if there were too many incorrect password attempts in a row.

This is why criminals have turned to stealing passwords.

Phishing is now very popular with attackers, and it's amazingly effective. Think about how the attack works. You get an email that seems to be from your bank; it has a plausible message, and contains a URL that seems legitimate and opens a window containing your bank's Web site. When the site asks for your username and password, you type it in. Okay, maybe you or I are aware enough not to type it in. But the average home banking customer doesn't stand a chance against this kind of social engineering attack.

In June 2004, a Trojan surfaced that captured passwords. It looked like an image file, but it was actually an executable that installed an add-on to Internet Explorer, monitoring and recording outbound connections to the Web sites of several dozen major financial institutions. It then sent usernames and passwords to a computer in Russia. Using SSL didn't help; the Trojan monitored keystrokes before they were encrypted.

Banks are increasingly fielding calls from customers who have fallen victim to these attacks. But even though the security problem has nothing to do with the bank, and customers are at fault, banks must make good on customers' losses. It's one of the most important lessons of Internet security: sometimes your biggest security problems are ones that you have no control over.

The problem is serious. In a May survey report, Gartner estimated that approximately 3 million Americans have fallen victim to phishing attacks. "Direct losses from identity theft fraud against phishing attack victims—including new-account, checking-account, and credit-card account fraud—cost US banks and credit-card issuers about $1.2 billion last year" (in 2003). Keyboard sniffers and Trojans will push this number even higher in 2004.

Even if financial institutions reimburse customers, the inevitable result is that people will begin to distrust the Internet. The average Internet user doesn't understand security; he thinks that a gold lock icon in the lower-right-hand corner of his browser means that he's secure. If it doesn't protect him—and we all know that it doesn't—he'll stop using financial Web sites and applications.

The solutions are not easy. The never-ending stream of Windows vulnerabilities limits the effectiveness of any customer-based software solution—digital certificates, plug-ins, and so on—and the ease with which malicious software can run on Windows limits other solutions' effectiveness. Point solutions might force attackers to change tactics, but won't solve the underlying insecurities. Computer security is an arms race, and money creates very motivated attackers. Unsolved, this type of security problem will change the way people interact with the Internet. It'll prove that the naysayers were right all along—the Internet isn't safe for electronic commerce. □

Bruce Schneier *is one of the world's foremost security experts and chief technical officer of Counterpane Internet Security. His most recent book is* Beyond Fear: Thinking Sensibly about Security in an Uncertain World. *You can subscribe to his email newsletter,* Crypto-Gram, *at www.schneier.com.*

Ed. note: Another version of this column appears in Schneier's Crypto-Gram *newsletter.*