



## STUDY: 73% USE BANK PASSWORD EVERYWHERE

Posted: Tuesday, February 2 2010 at 06:00 am CT by Bob Sullivan

For years computer security experts have been preaching that users should never share the same password across their connected lives -- at online banking sites, at Amazon, on their Web mail services, even on their cell phones.

Apparently, most people ignore that advice.

A new study by security firm Trusteer found that 73 percent of Web users take their online banking password and use it at other Web sites. And about half of all consumers utilize the same password and user name at online banking sites and other sites.

"I must say I was very surprised," said Amit Klein, chief technology officer of Trusteer. "It is surprisingly sad that such a large portion of users use their banking credentials at other sites. ... It exposes those users to attacks that would otherwise be impossible. I thought that people would take banking credentials more seriously, but it turns out that in this digital age, this is not the reality."

When consumers use the same password across multiple sites, hacking becomes trivially easy. If a criminal breaks into a smaller Web site -- say a site created by a local grocery store -- and grabs a cache of passwords, their next step is always the major banking Web sites. When you consider that 40 percent of U.S. consumers' checking accounts are tied up in the four largest banks, odds are good that the stolen credentials will work for ~~in~~ one of them.

Password overlap also creates an easy end run around sophisticated banking security technology, which is only as strong as the weakest site where the password is used. Banks might enforce strong password creation requirements, for example. But if a consumer uses a bank password ~~#~~ at a poorly defended small site, a hacker can break into the small site, steal the log-in information and essentially crack the bank's high-tech system.

"This is something that should be of huge concern both to banks and to users," said Klein.

Trusteer unearthed the data through use of its Rapport security software, which is designed to warn users when they are about to enter a critical banking password into a site where it doesn't belong -- a phishing site, for example. The tool was used to examine the behavior of 4 million computer users during a 12-month period. During that span, the firm found that 73 percent used their online banking password on at least one non-financial Web site.

And it didn't help much when the banks enforced strict password controls. When a bank allowed consumers to pick a user ID, 65 percent used it on other sites. When a bank assigned a customer ID, 42 percent used it at other sites and 42 percent used both the ID and the password on at least one other site.

### **'They don't think it's worth the trade off'**

Last year, analyst firm Gartner released a survey that reported similar results. It said two-thirds of consumers use the same one or two passwords across all Web sites they access.

But Avivah Litan, who directed the Gartner survey, said that choice might not be as unreasonable -- or as unsafe -- as it seems.

"They are making a choice for convenience over security," she said. "They are using a cost-benefit equation ... and they don't want to try to remember 10 different passwords for everything they do. They don't think the trade-off is worth it, honestly."

While password sharing isn't a safe practice, Litan said, complicating your life with multiple passwords isn't exactly a cure-all.

"The truth is criminals steal your passwords lots of ways, such as recording keystrokes, and if they do that, it doesn't matter whether your password is 15 characters and unique or 7 characters and the same for every site. People have figured this out," she said.

Using multiple passwords is a good idea, but Litan said it is important that consumers understand the risks that remain even if strong passwords are used.

"It is another lock on the door but a lock that is easily picked," she said. "Still, it's always better to put as many blocks in the road you can."

Large banks don't rely on simple user/password combinations to identify users anymore, she added. Numerous technologies are used to prevent fraud through a strategy called "layered security." Device fingerprinting of PCs is a key tool, she said. Web sites tag computer hardware by monitoring unique characteristics, such as exact processor speed or time and date settings. Sites that use device fingerprinting see fraud rates drop 15 to 20 percent, she said.

Banks also look for suspicious behavior, such as attempted transfers to unusual accounts. Another hacker giveaway: clicks through Web sites that occur at high speed, showing an automated PC -- and not a person -- is attempting a transaction. Humans take, on average, about 10 seconds before they click "confirm payment." Computers controlled by hackers racing through stolen login accounts barely wait at all.

"That's best-of-breed security," Litan said. "If you as a bank are relying on passwords for security then you have a poor security system."

#### **RED TAPE WRESTLING TIPS**

It should be comforting to know that your user ID and password are not all that stands between a hacker and your money. Still, that's no reason to let your guard down. Your banking passwords should be handled with great care, and shouldn't be shared with other Web sites.

And remember, many Web firms that store your critical personal information do not use best-of-breed security on their back end -- meaning you are still at risk. A criminal who stole your Facebook credentials **could easily wreak havoc with your life**, so protect those accounts, too.

Klein concedes that the vast majority of computer users will never create unique user/password combinations for all their sites. As a more practical goal, he recommends maintaining three "families" of passwords -- one for critical financial sites, a second for sites that store your personal information, and a third for generic log-ins.

"And you don't want to mix those passwords," he said.

Corporate sneakiness. Government waste. Technology run amok. Outright scams. The Red Tape Chronicles is MSNBC.com's effort to unmask these 21st Century headaches and offer real solutions that save you time and money.

Bob Sullivan covers Internet scams and consumer fraud for MSNBC.com. He is the winner of multiple journalism awards for his coverage of online crime and author of *Gotcha Capitalism: How Hidden Fees Rip You Off Every Day and What You Can Do About It*. and *Your Evil Twin: Behind the Identity Theft Epidemic*.