

Dual Authentication Tapped in Phish Fight

SEPTEMBER 5, 2006 | Researchers at Carnegie Mellon University have built a tool that protects users from phishing attacks -- even if they take the bait.

The Phoolproof Phishing Prevention tool provides two-way authentication between the user and the Web server via the user's mobile device: a cell phone or PDA, for instance. The Java-based tool operates atop SSL and uses a key pair that authenticates the user and the Websites visited.

That way, even if a user mistakenly tries to go to a phishing site posing as his bank, for example, the tool will prevent him from accessing it. And he won't be able to inadvertently give away or compromise his credentials, which are stored in the mobile device. The mobile device talks to the user's Web browser and only shows its authentication key to a legitimate Website.

CMU researchers say their prototype is more effective against phishing than existing anti-phishing tools. "A lot of prior approaches try to get the users to just recognize when they arrive at a phishing Website," says Bryan Parno, a graduate student and member of the project's research team at CMU's CyLab. "But the fundamental problem is users are still going to make the wrong decision."

Parno says studies show users still click through and enter their personal data even when their toolbar warns them about a site.

The catch: Both the user and Websites must deploy the Phoolproof Phishing Prevention technology for it to work, so consumers, businesses, and financial institutions, for instance, would all have to be in the loop.

"I like the idea of including another means to authenticate, and handsets are one alternative," says Dan Hubbard, vice president of research at Websense and a research fellow with the Anti-Phishing Working Group. However, "I'm not sure about the scaling of such a solution," he says.

Plus, it adds some complexity and costs for the organizations deploying it, Hubbard says. "And this wouldn't potentially stop plain-Jane social engineering asking a user for a username and password," either.

But CMU's Parno says all it would take is "small tweaks" to server configurations to store the user account key as well as some changes to the SSL setup. Websites would likely deploy it side by side with existing username and password authentication on their sites, for example, he says.

The CMU CyLab's prototype runs on a Nokia smart phone, but it could be used on any mobile device, Parno says. "When you want to log on to Amazon.com, for example, your mobile device communicates with your PC and launches your browser to make sure it's the right site. Then it authenticates on your behalf using the key, and you enter your user name and password," Parno explains.

The mobile device manages the keys, so the organization or user doesn't have to. "What's nice about this setup is the key never leaves your mobile device, and it never discloses it," Parno says, so there's no chance of giving away your identity to the wrong guy. And even if your cell is lost or stolen, your keys are useless without your username and password, he says.

CMU is working with some financial institutions and mobile phone companies that are interested in the tool, Parno says, but he can't name names. It's unclear yet just how CMU will distribute the tool -- or whether it will charge for the tool or make it freeware -- but the research team is working on making the prototype more robust and reliable in the meantime, he says.

Phishing experts say there's no single solution for killing phishing attacks available today. Peter Cassidy, secretary general of the APWG and director of research for Triache, says there are 130 different brands being phished each month, with small banks and credit card companies becoming major targets of these schemes as well. Cassidy notes that IM, interactive voice response systems, and blended media attacks are becoming more common with phishing attacks, too, so there are just too many attack venues for a single solution to protect. "Phishing is a many-splendid thing," he says.

"There's nothing in the near-term that's a silver bullet," Websense's Hubbard says. "One of the biggest gains we could get is mass education of the problem to help with the low-hanging fruit attacks -- just making sure users are aware of the mass amount of fraud that's happening online."

— Kelly Jackson Higgins, Senior Editor, [Dark Reading](#)

- [Anti-Phishing Working Group](#)
- [Websense Inc.](#) (Nasdaq: [WBSN](#) - [message board](#))