

News

Mobile devices to defend against phishing

[Liz Tay](#) 05/09/2006 15:11:13

Researchers at the Carnegie Mellon University have developed a new antiphishing tool to address the growing problem of fraud.

The university says the Phoolproof Phishing Prevention system provides an additional layer of security at sensitive sites, such as banks, e-commerce and investment sites, by leveraging a mobile device, such as the user's mobile phone or PDA.

Phishing fraud typically occurs through fraudulent e-mails requesting sensitive information, such as passwords and credit card details, which may then be used to plunder financial accounts, make purchases, or apply for additional credit cards.

There were 28,571 unique cases of phishing fraud in June 2006, according to an [Anti-Phishing Working Group](#) report. This nearly doubles the number of reports from a similar period a year ago.

"While it is difficult to collect accurate data about the extent of phishing fraud, what data we do have suggests that phishing is a growing problem," said Carnegie Mellon researcher Bryan Parno. "Estimates suggest that millions of consumers have been affected by phishing attacks, while businesses have lost billions of dollars."

And it appears phishing is a problem for Web surfers of all levels. A separate [study](#), conducted by researchers at Harvard University and the University of California Berkeley earlier this year, found that a well-designed fraudulent Web site fooled 90 percent of participants, Internet newbies and 'Web savvy'-types alike.

The prevention system eliminates the risk of a user being fooled, through the use of a secure electronic key that is stored on the user's mobile device. The device communicates with the Web browser, and will only reveal its authentication key to the appropriate Web site, researchers said.

"The Phoolproof Phishing Prevention system rests on the observation that users should not be authenticated based on information that they can readily reveal to others," Parno said. This way, phishers will not be able to access a user's accounts, even if they obtain information about the user.

The system also defends against keyloggers and other malicious software on the user's computer, the researchers said. And even if the mobile device is lost, the finder will still require the username and password to access accounts.

"An attack on the device itself will not produce enough information to allow an attacker to access the user's accounts," Parno said. "Beyond that, we expect mobile devices to adopt many of the defence techniques currently employed on desktops.

"In the long-term, mobile devices will include hardware support for enhanced security measures, and we can leverage these to enhance the security of our system."

Researchers do not expect there to be many additional costs in adopting the system. It was deliberately designed to be as simple as possible for both users and businesses to implement, Parno said.

The system uses the standard SSL protocol to minimize changes to a business' existing infrastructure. After being adopted, the system also allows legacy clients to authenticate as they normally would, which means that the system could be rolled out gradually without affecting too many customers.

Complicating the concern for more secure financial sites is a looming deadline for new security guidelines from the US Federal Financial Institutions Examination Council, a group of government agencies that sets standards for financial institutions. Last year, the council set a December 31 deadline for banks to add online security measures beyond just a user name and password. Failure to meet that deadline could result in fines, the council said.

Enterprise IT Buyer's Guide | Vendors relevant to this article

[GFI](#) , [SonicWALL](#) , [3Com](#)

More about [Financial Institutions](#), [Mellon](#), [Harvard University](#), [Carnegie Mellon University](#)



Copyright 2006 IDG Communications. ABN 14 001 592 650. All rights reserved. Reproduction in whole or in part in any form or medium without express written permission of IDG Communications is prohibited.

IDG Sites: [PC World](#) | [GoodGearGuide](#) | [Australian GamePro](#) | [CIO Australia](#) | [CSO Online](#) | [LinuxWorld.com.au](#) | [Australian Reseller News](#)