


[Home](#)
[News / Opinion](#)
[Sports](#)
[Obituaries](#)
[Features](#)
[Entertainment](#)
[Community](#)
[Classifieds](#)
[National News](#)
[Archives](#)
[About Us](#)
[Media Kit](#)
[Current Special Sections](#)
[Upcoming Special Sections](#)
[Subscriber Care](#)

[Fletcher pitches at Pritchard](#)
[Milk drought bringing price hike](#)

Hardin County, Kentucky

THE NEWS-ENTERPRISE

Online

News

Computer users beware: Hackers could be 'phishing' for data

By *BRIAN WALKER*

A recent spike in illegal operations designed to collect personal information about computer-users has gotten the attention of computer watchdog groups and some lending institutions that are trying to protect customers.

The practice is known as phishing — as in fishing for information — and can cost a victim thousands of dollars in credit card debt. The name was invented in 1996 by hackers who successfully got into America Online accounts.

Hardin County officials who follow Internet crimes said they don't know of anyone who has been scammed locally, but such e-mails have popped up unsolicited in some residents' computer mailboxes.

Now, a 6-month-old network of experts is working toward solutions to protect users' information. The Anti-Phishing Working Group, made up of professionals from banking, computer and other industries and the federal government, began meeting Monday in San Francisco to devise ways to combat the problem.

The group has reported increases of known scam Web sites by about 50 percent each of the past three months. Current numbers on its Web site, www.antiphishing.org, show that the organization has identified 282 running scam sites.

The group said users are more savvy than they used to be, but it estimates about six or seven people out of every 1,000 sent a phishing e-mail response with the requested personal information. Officials estimate that about 70 percent of the scams originate in Asia and Europe, making prosecution more difficult.

The practice has become so frequent, the Department of Justice recently issued a special report to inform Internet users about the risks of responding to phishing e-mails and Web sites, whether phishing schemes violate federal criminal laws and the steps that Internet users should take when they see possible phishing messages.

Bank One, which has branches in Hardin County, recently posted an alert on its Web site — www.bankone.com — to warn customers of phishing.

The Cecilian Bank began telling its customers in person about the e-mails, warning them not to respond to the messages. The proactive approach started two weeks ago when the American Bankers Association issued alerts to financial institutions, said Don Wise, president of Cecilian Bank.

He said the ABA specifically warned of e-mails being sent to people that tell

[School Jewels: After 51 years in the classroom, he'd do it all over again](#)

[Computer users beware: Hackers could be 'phishing' for data](#)

[Hospital seeks original staff for a homecoming anniversary celebration](#)

[Ga. fugitive found in Hardin County](#)

them that their FDIC insurance will be cut off unless they provide personal information in an allotted time. But the bank would only seek such information through other forms of communication, such as face-to-face.

"It's a very well designed and guised e-mail for someone who's unsuspecting," Wise said.

The way phishers generally catch users is by sending out bogus e-mail to subscribers of certain online services such as eBay, banks and credit firms. The e-mail appears legitimate and claims to be from the company. It will request current information such as credit card numbers.

"No legitimate business ever works that way," said David Evangelista, executive director of the Radcliff-based United States Internet Crime Task Force Inc. "Nobody contacts you via e-mail to get sensitive information like that."

He said that despite the dangers most computer-users know about, like opening viruses, many people trust a legitimate looking e-mail.

"And they often look like the real thing," Evangelista said.

The Kentucky Better Business Bureau released a report Monday advising business to secure computers by keeping passwords private, using anti-virus software that is up to date, backing up data, making random checks of suspicious activity and educating employees about the dangers of computer usage.

The Anti-Phishing Working Group is working toward better reporting techniques to the Secret Service, scam prevention, projected threats and other concerns.

There are reports of new viruses that install themselves on computers to retain and send out keystroke information. The software is so intelligent, it can remember thousands of individual keystrokes and find patterns like credit card numbers or passwords.

The information is then sent back to the hacker, who uses it to gain access to private information or to steal money from users' accounts.

One hacker recently sent an e-mail to thousands of users claiming to be a representative of Microsoft and warned of the keystroking practice. The supposedly helpful person attached a free software patch that would allegedly protect the user from keystroking.

In reality, users who used the patch merely installed the very virus about which the fake Microsoft employee warned them.

Avoiding scams

- Don't open e-mail from people you don't know.
- Be careful with file sharing services. Hackers often will take more than a song off your hard drive.
- Don't give personal information to anyone who requests it in an e-mail. Hackers will pose as representatives of major companies. No legitimate business e-mails customers wanting this type of data.
- Stay logged off the Internet when not using it.

- Install anti-virus software, and keep it updated.
- If you have your own Web site, install firewall security features to keep hackers out of your system.
- Report frauds to the federal authorities via www.ifccfbi.gov.

Source: www.usict.org, the Better Business Bureau and the Anti-Phishing Working Group.

- Brian Walker can be reached at 769-1200, Ext. 241, or e-mail him at bwalker@mail.the-ne.com.

[Back to top](#)

[Print this story](#)

[Email this story](#)

Copyright © 2004 The News-Enterprise

[Home](#) | [News / Opinion](#) | [Sports](#) | [Obituaries](#) | [Features](#) | [Entertainment](#)
[Community](#) | [Classifieds](#) | [National News](#) | [Archives](#) | [About Us](#) | [Media Kit](#)

408 West Dixie Avenue Elizabethtown, KY 42701
270-769-2312 | ne@mail.the-ne.com
[Contact Us](#)