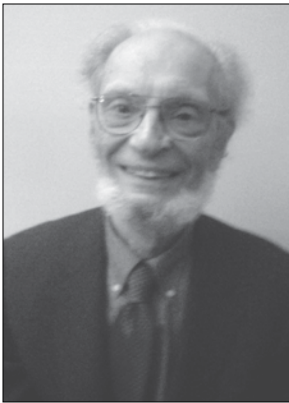


## Spear-Phishing

by Jerome Trupin, CPCU, CLU, ChFC



**Jerome Trupin, CPCU, CLU, ChFC**, is a partner in Trupin Insurance Services, located in Briarcliff Manor, N.Y. As an “outsourced risk manager,” he provides property-casualty insurance consulting advice to commercial, nonprofit and governmental entities. Trupin regularly writes articles on insurance topics for industry publications and is the co-author of several insurance textbooks published by the AICPCU/IIA. Trupin has been an expert witness in numerous cases involving insurance policy coverage disputes, has spoken on insurance topics across the country, and has taught many CPCU and IIA courses. He can be reached at [cpcuwest@aol.com](mailto:cpcuwest@aol.com).

**S**pear-phishing isn't the name of a sport for phonetically-challenged scuba divers; it's a refinement on the all-too-common Internet blight known as “phishing.” A phisher casts a wide net; a spear-phisher sends a message directly to a specific recipient. (It's easy to get e-mail addresses of people in, for example, the finance department of a large corporation, either by bribing an employee for a list or searching for names on the Internet and then formatting their e-mail addresses using the firm's standard e-mail name-format.) An actual spear-phishing loss occurred as follows:

Late on a Friday afternoon, Sue Mark (name changed), an employee in the finance department of a large firm, received an e-mail, addressed directly to her, appearing to be from the firm's bank. The message said that there had been a number of unsuccessful attempts to log in to the firm's bank account and directed Sue to the bank's Web site.

The Web site appeared to be legitimate. It asked that she send a reply message containing the firm's bank account number and password. According to the message, this information was needed so the bank could be sure that she was someone in the firm rather than the person attempting to access the account. The message said that the bank would then change the password and let her know the new one. The Web site appeared identical to the bank's actual Web site. It was, of course, run by the spear-phisher. Sue took the bait, and by Monday morning the spear-phisher had withdrawn \$650,000 from the firm's bank account.<sup>1</sup>

Could the firm collect for the \$650,000 loss under its employee fidelity coverage? Is there any other crime coverage that might apply?

There are two basic types of employee fidelity coverage available today. The Insurance Services Office (ISO) and some other insurers provide what's known as “employee theft” coverage. Employee theft is, logically, a theft by an employee. Theft is defined as “unlawful taking to the deprivation of the insured.” In order to trigger coverage, Sue's act would have to be unlawful and she would have to be the one who had done the “taking.” Because her actions do not meet that standard, there's no coverage. Sending the account number and password was stupid, but probably not illegal. If stupid acts were illegal, we'd probably all be indicted at one time or another.

*Continued on page 2*



# Spear-Phishing

Continued from page 1

The other type of employee fidelity coverage is known as “employee dishonesty.” The American Association of Insurance Services (AAIS) and the Surety & Fidelity Association of America (SFAA) make employee dishonesty forms available, as do some independent insurers; at one time ISO offered employee dishonesty coverage. The basic requirement under these forms is that the employee’s act be dishonest, not necessarily unlawful. Employee dishonesty forms, however, contain what’s referred to as a “dual trigger.” The dual trigger requires that the employee manifest an intent to cause the insured to sustain loss and obtain financial benefit for the employee or another person whom the employee designates. The benefit must be something other than salaries, commissions, bonuses, promotions, profit sharing, etc. Since Sue didn’t intend to cause a loss to her employer and since she didn’t expect any financial benefit, there’s no coverage under employee dishonesty coverage either.

It appears that Sue’s employer would also be unsuccessful in seeking coverage under its employee fidelity insurance, whichever form (employee theft or employee dishonesty) is used. Is there a coverage that might apply?

There is coverage available under an ISO coverage known as “Computer Fraud.” The computer fraud insuring agreement reads as follows:

## 6. Computer Fraud

We will pay for loss of or damage to “money,” “securities” and “other property” resulting directly from the use of any computer to fraudulently cause a transfer of that property from inside the “premises” or “banking premises”:

- a. To a person (other than a “messenger”) outside those “premises;” or
- b. To a place outside those “premises.”<sup>2</sup>

This appears to be a coverage that

would protect Sue’s firm. We don’t know exactly how the spear-phisher obtained the funds. Depending on the exact way that the spear-phisher communicated with the bank, coverage might be found under ISO Crime Funds Transfer Fraud coverage instead. It reads as follows:

## 7. Funds Transfer Fraud

We will pay for loss of “funds” resulting directly from a “fraudulent instruction” directing a financial institution to transfer, pay or deliver “funds” from your “transfer account.” “Fraudulent instruction” means: An electronic, telegraphic, cable, teletype, telefacsimile or telephone instruction which purports to have been transmitted by you, but which was in fact fraudulently transmitted by someone else.<sup>3</sup>

Because it recognizes the possible overlap between these coverages, the ISO Computer Fraud coverage form excludes any claim that qualifies as Fund Transfer Fraud claim and the Fund Transfer Fraud coverage excludes any claim that qualifies as Computer Fraud. To avoid this overlap, some insurers combine the two coverages into one insuring agreement.

Spear-phishing may be the most exotic, but it’s far from the only way that criminals can help themselves to a firm’s bank account. A front page story by **John Markoff** in the Dec. 5, 2008, issue of *The New York Times* starts out: “Internet security is broken, and nobody seems to know quite how to fix it.” The story goes on to point out that credit card thefts, bank fraud and other scams rob computer users of an estimated \$100 billion a year. Amazingly, the author writes that “a Russian company that sells fake antivirus software that actually takes over a computer pays its illicit distributors as much as \$5 million a year.”<sup>4</sup>

The most common source of computer and fund transfer fraud losses are employees. The CFO of the American Cancer Society’s Columbus, Ohio, office, who had wired \$7 million from the

Cancer Society’s bank account to one in his name in an Austrian bank, was arrested just as he was boarding a plane to flee the country. An employee’s thefts would be covered under fidelity coverage — another argument for high limits for that coverage. But the Internet has given criminals worldwide the opportunity to invade a firm’s bank accounts. To protect against those losses, Computer Fraud and Fund Transfer Fraud coverages with high limits are vital for virtually every enterprise. ■

## References

1. Based on a presentation by George N. Allport, Chubb Insurance, at the Westchester CPCU Chapter/Westchester Community College seminar on Nov. 21, 2008.
2. ISO Properties Inc., CR 00 20 05 06 Commercial Crime Coverage Form © 2005.
3. ISO Properties Inc., op. cit.
4. Markoff, John. “Thieves Winning Online War, Maybe Even in Your Computer.” *The New York Times*: Dec. 5, 2008. In case the term phishing is new to you, here’s information about it from Wikipedia: “In the field of computer security, **phishing** alludes to baits used to “catch” financial information and passwords. It is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social Web sites (YouTube, Facebook, MySpace), auction sites (eBay), online banks (Wells Fargo, Bank of America, Chase), online payment processors (PayPal), or IT Administrators (Yahoo, ISPs, corporate) are commonly used to lure the unsuspecting. Phishing is typically carried out by e-mail or instant messaging,<sup>1</sup> and it often directs users to enter details at a fake Web site whose URL and look and feel are almost identical to the legitimate one. Even when using SSL with strong cryptography for server authentication, it is practically impossible to detect that the Web site is fake. Phishing is an example of social engineering

techniques used to fool users,<sup>2</sup> and exploits the poor usability of current Web security technologies.<sup>3</sup> Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness and technical security measures.”

1. Tan, Koon. “Phishing and Spamming via IM (SPIM).” Internet Storm Center. <<http://isc.sans.org/diary.php?storyid=1905>> Accessed on Dec. 5, 2006.
2. Microsoft Corporation. “What is social engineering?” <<http://www.microsoft.com/protect/yourself/phishing/engineering.aspx>> Accessed on Aug. 22, 2007.
3. Jøsang, Audun et al. “Security Usability Principles for Vulnerability Analysis and Risk Assessment.” (PDF) Proceedings of the Annual Computer Security Applications Conference 2007 (ACSAC’07). <<http://www.unik.no/people/josang/papers/JAGAM2007-ACSAC.pdf>> Accessed in 2007.