

T ECHNOLOGY

Gone Phishin'

Avoid the Lure of Rising E-Mail Scams

Phishing, one of the latest e-mail scams, refers to fraudulent e-mails designed to deceive people into disclosing personal, financial and/or confidential business information to be used for unlawful purposes.

Phishing scams are prevalent and on the rise. Not only have the number of reported phishing sites risen in the last year, but the number of reports of identity theft from phishing also continues to rise.

Research indicates that illegal access to checking accounts, often gained via phishing schemes, has grown into one of the fastest growing forms of consumer theft in the United States. Security vendors and anti-phishing organizations report that targeted phishing attacks on business networks – known as spear phishing – are also on the rise.

All of this results not only in the theft of valuable personal and financial information, but also in the theft of trade secrets, intellectual property and other highly sensitive and confidential business information.

Consumer Phishing

Phishing scams come in different forms and are continuously evolving. Typically, they come in



Maria Recalde

the form of an e-mail that appears to be from a legitimate financial institution, insurance company, retailer or other business using seemingly authentic logos, Web links or graphics to mislead the recipient into believing that the e-mail solicitation is from a legitimate business, perhaps even one with whom the recipient already has a customer relationship.

The e-mail typically contains both a request designed to have the recipient disclose sensitive information (such as a request to verify or update the recipient's personal information or account details) and a statement indicating

that if the information is not provided the account at issue will be closed or suspended.

The communication may also contain suspicious attachments or windows that pop up over a legitimate company's Web site, asking you to enter personal or financial information.

Spear Phishing

In addition to these phishing scams targeted directly at consumers, businesses are reporting increased spear phishing scams that wreak havoc on business networks. Spear phishing is designed to grant access to confidential business data.

Username and passwords to access a company extranet or intranet can be obtained through basic phishing techniques.

Log-in information is often retrieved by first sending an official-looking e-mail to employees of a targeted company. The e-mail generally appears to come from a legitimate company e-mail address (typically from the IT or HR departments) and instructs the recipient to reply with confidential information, such as usernames and passwords and/or logging in to a password-protected area.

Some purport to come from a service provider or supplier of the

T ECHNOLOGY

company. A common e-mail group within the company, such as sales@company.com or marketing@company.com, is often targeted.

A reply by one or more of the employees makes the log-in information needed to access password-protected company data available to the sender.

In some instances, a keystroke-logging program is attached to the e-mail. When an unsuspecting employee opens the e-mail and activates the attachment, the keystroke logger is installed and begins logging everything the employee types. As the employee types in username and password information, these details are sent back to the sender, who can then log in as the employee to access confidential business data.

Scam Avoidance

The Department of Justice, the Federal Trade Commission, and the Anti-Phishing Working Group, APWG, among others, suggest the following tips to help you avoid

getting hooked by a phishing scam:

- Be suspicious of and do not reply to any e-mail or pop-up messages with urgent requests for personal, financial or confidential business information. In addition, do not click on any link contained in the text of the message, or cut and paste the link from the message into your Internet browser.

- Always use anti-virus software and a firewall, and keep them up to date. This will make it harder for anyone to install key loggers, spyware, Trojans or other similar devices intended to retrieve your information, harm your computer or track your activities on the Internet without your knowledge.

- Ensure that your browser is up to date and that applicable security patches are applied.

- Do not e-mail personal, financial or any other sensitive information.

- Regularly log into your online accounts and review your account statements to ensure that all trans-

actions are legitimate.

- Be cautious about opening any attachment or downloading any files from e-mails you receive, regardless of who sent them. These files can contain viruses or other software that can weaken your computer's security. Never open e-mail attachments from unknown sources.

- Do not share IDs/user names and passwords, and change your passwords regularly.

- Consider installing a Web browser tool bar to help protect you from known phishing Web sites.

While these precautions cannot guarantee your protection, making these practices part of your online routine can minimize your risk of being the victim of a phishing expedition.

Maria E. Recalde is a partner at Sheehan Phinney Bass + Green P.A. She is a member of the firm's Business Litigation and Intellectual Property and Technology Practice Groups.