



## **ABA News to Use**

### ***Keeping banking's frontline personnel informed***

#### **Phishing Scams: Don't Take the Bait**

Internet phishing scams, like other forms of fraud, prey on the unwary.

Phishing con artists claim to be from a reputable company and send out thousands of fake e-mails and fake Web page images in hopes that consumers will respond with account information, credit card numbers, passwords or other sensitive information. This information can then be used by the thieves to order goods and services or obtain credit.

A phishing e-mail can look quite convincing, with company logos and banners copied from actual, legitimate Web sites. Often, they will tell recipients that their security procedure has changed or that they need to update (or validate) personal information, and the recipients will be directed to a look-alike Web site. Phishing attempts may also try to impart a sense of urgency to get recipients to respond before thinking through the situation.

Consumers should be vigilant. For more information on phishing, visit the [Federal Deposit Insurance Corp.](#), [Federal Trade Commission](#), [Anti-Phishing Working Group](#), [National Consumers League](#), or [OCC Consumer Protection News](#).

#### **Tips to Thwart Phishing**

- Never give out personal financial information in response to an unsolicited phone call, fax or e-mail, no matter how official it may seem.
- Do not respond to e-mails that may warn of dire consequences unless you validate your information immediately. Contact the company to confirm the e-mail's validity using a telephone number or Web address you know to be genuine.
- Check your credit card and bank account statements regularly and look for unauthorized transactions, even small ones. Some thieves hope small transactions will go unnoticed. Report discrepancies immediately.
- When submitting financial information online, look for the padlock or key icon at the bottom of your Internet browser. Also, many secure Internet addresses, though not all, use "https" to signify that your information is secure during transmission.
- Report suspicious activity to the [Internet Crime Complaint Center](#), a partnership between the FBI and the National White Collar Crime Center.

(Note: For more information, visit ABA's [Phishing Issue Summary](#).

---

For information about ABA News to Use, or to suggest subjects for future articles, please contact ABA's [Brian Nixon](#).