

Risk Alert - American Bankers Association Warns Consumers Of Phishing Scams

The ABA recently warned consumers not to become victims of the sudden nationwide increase in phishing scams. The ABA indicated that perpetrators are using automated dialers, text messages or e-mails to inform consumers their accounts have been closed due to fraud. Consumers then are prompted to enter their card information, including the expiration date and three-digit CV code on the card's back to reactivate their accounts. Those who fall for the scam risk having their information used to fraudulently purchase goods and services or to obtain credit, the Association said.

Below are several tips provided by the ABA to help CU members avoid becoming a victim of such phishing scams.

- Never give out your personal or financial information in response to an unsolicited phone call, fax or email, no matter how official it may seem.
- Do not respond to email that may warn of dire consequences unless you validate your information immediately. Contact the company to confirm the email's validity using a telephone number or Web address you know to be genuine.
- Check your credit card and bank account statements regularly to look for unauthorized transactions, even small ones. Some thieves hope small transactions will go unnoticed. Report discrepancies immediately.

Whenever you submit financial information online, first look for the padlock or key icon which may appear at the bottom of your Internet browser or in the address at the top. Also, many secure Internet addresses, though not all, use "https."

Report suspicious activity to the Internet Crime Complaint Center (<http://www.ic3.gov/complaint/default.aspx>) a partnership between the FBI and the National White Collar Crime Center.

If you have responded to an email, contact your bank immediately so they can protect your account and your identity. For information on identity theft, visit ABA's Consumer Connection. For more information on phishing, visit the following: Federal Deposit Insurance Corporation, the Anti-Phishing Working Group, the National Consumers League, the OCC Consumer Protection News and the OCC Consumer Complaints and Assistance Web site.