

CITIZENS STATE BANK WARNS CONSUMERS ABOUT PHISHING SCAMS

Citizens State Bank is warning consumers not to fall victim to phishing scams. Phishing is a new twist on an old telemarketing scam, but uses e-mail. These criminals send e-mails to millions of people hoping that even a few will give away valuable information.

To avoid becoming the victim of a phishing scam we offer the following tips:

- **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** 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. Most secure Internet addresses, though not all, use "https".
- **Report suspicious activity** to the [Internet Crime Complaint Center](#), 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 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 website](#).