

Phishing...

**Don't become the catch of the day.
Be the one that got away.**

Phishing is a new twist on an old telemarketing scam; however, instead of the phone, scam artists use the computer e-mail system.

Phishing (FISH-ing), refers to how thieves steal victims' personal financial information. They're phishing for information. Phishing con artists pretend to represent a trusted source, like a bank, and then scare the consumer with threats if they don't act quickly.

These scammers steal credit card, bank account and Social Security numbers. They also seek passwords and any sensitive financial information.

Phishing scams are constantly evolving and your bank offers the following tips so you don't become a victim:

- Never give out your personal financial information over the phone or the computer, unless you called them first. Banks will never ask you to "verify" your financial information or ask you to click on a special site link.
- Do not respond to an e-mail that may warn of dire consequences. Always confirm these e-mails separately with the bank or company.
- Check your credit card and bank account statements regularly and look for unauthorized charges, even small ones. Report these discrepancies immediately.
- When submitting financial information to a web site, look for the padlock or the key icon at the bottom of your browser and make sure the address begins with "https". This is no guarantee, but the lack of these icons or "https" does indicate that the web site is not secure.
- Report suspicious activity to the Internet Crime Complaint Center at www.ic3.gov.
- If you do respond to a fraudulent e-mail, contact your bank immediately so they can help protect your account and identity.

For more information on phishing or identity theft go to www.antiphishing.org or www.consumer.gov/idtheft. Each year, phishing con artists convince 5 percent of the public to fall for their scams. Make sure it's not you.