Phishing

Avoid Becoming a Victim

Protect Your Personal Information

How Phishing Works

Criminals are constantly improving their methods of stealing your personal financial information through fraudulent e-mails and Web sites designed to appear as though they were generated from legitimate businesses, financial institutions and even government agencies. This criminal activity is known as "phishing". They are literally fishing for your personal information.

AVOIDING THE SCAMS

- NEVER provide any personal information to an inquiry that is originated by someone else. Do not respond to email inquiries even if they appear to be from a legitimate source. Do not provide social security numbers, account numbers, credit card numbers, passwords, usernames, etc.
- Always use a secure Website when you are submitting credit card or other personal information in transactions you initiate.
- Monitor all bank and credit card accounts. Monitor your credit report at least annually.
- Be suspicious of any email requesting personal information or requiring you to act immediately to prevent negative actions.
- Don't use links that are provided in an suspicious emails.
- Apply security patches and use up to date browsers.
- Signup for the National Do Not Call Registry 1-888-382-1222

ADVICE FOR VICTIMS OF PHISHING

- Contact your financial institution immediately.
- Contact one of the three major credit bureaus and request that a fraud alert be placed on your credit report. Request a free copy of your credit reports. The law allows this free report once a year. The credit bureaus and contact numbers are: Equifax (800) 525-6285; Experian (888) 397-3742; TransUnion, (800) 680-7289.
- Visit www.consumer.gov/idtheft to file a complaint with the FTC and to access a very useable Identity Theft Affidavit form you can use to alert lenders of your situation.
- Review all billings and blank statements immediately for accuracy.
- Close any affected accounts and open new ones.
- Contact the local law enforcement and file a policy report.
- Contact the Social Security Administration (www.ssa.gov) if your SS number has been compro-

FAQs

Q: How will fraudsters contact me??
A: Fraudsters use many different forms of contact including mail, email, social media, malware and popups.

Q: Will the bank ever contact me by email?
A: The bank would not contact you by email normally. However, if you receive an email from a bank employee, please call the bank directly—do not respond to the email.

Q: How will I know if an email is fake?
A: Make clues will help determine if an email is fake. Look for the following signs: Vague subject line, signature doesn't make the email address, poor grammar and misspellings, the body of the email contains a link and hovering over the link with your mouse (without clicking) reveals a totally different site link.

Q: What if I get a check in the mail?
A: First ask yourself, "does this seem too good to be true?" If so, then it probably is. You can bring the check to your bank with any correspondence and have it examined. Make sure to disclose to the bank that the check is suspicious. Whatever you do, do not cash the check and return a portion of the funds to the remitter. If this is a condition of receiving the funds, then it is a scam and you will be liable for any loss!

Other Scams:

- Lotteries or Sweepstakes
- Online Sales Scams
- "Sponsors" or "Charities"
- Money from a "relative" in another country who needs help transferring it to the US.

Found out more about phishing and other crimes at:

www.antiphishing.org *www.flc.gov*

www.idtheftcenter.org *www.microsoft.com/security*

www.earthlink.net/earthlinktoolbar

Report suspicious email or phone activity to www.consumer.gov/idtheft or via phone to 1-877-IDTHEFT