

## Beware of Phishing Scams

Phishing is an online scam that seeks to steal credit card numbers, account information, Social Security numbers, passwords, and other sensitive information by using fake e-mails, fraudulent Internet addresses, imposter websites, and "pop-ups" to impersonate your financial institution and trick customers into disclosing their personal data.

Be suspicious of any email with urgent requests for personal financial information unless the email is **digitally signed**, you can't be sure it wasn't forged or 'spoofed'. Phishers typically include upsetting or exciting (but false) statements in their emails to get people to react immediately. They typically ask for information such as usernames, passwords, credit card numbers, social security numbers, date of birth, etc.

Phisher emails are typically NOT personalized, but they can be. Valid messages from your bank generally are personalized, but always call to check if you are unsure. Don't use the links in an email, instant message, or chat to get to any web page if you suspect the message might not be authentic or you don't know the sender or user's handle. Instead, call the company on the telephone, or log onto the website directly by typing in the Web address in your browser.

Avoid filling out forms in email messages that ask for personal financial information. You should only communicate information such as credit card numbers or account information via a secure website or the telephone, always being positive about who you are communicating with.

Here are some guidelines from the Anti Phishing Working Group.

### **If you have given out your credit or debit or ATM card information**

- Report the theft of this information to the card issuer as quickly as possible
  - Many companies have toll-free numbers and 24-hour service to deal with such emergencies.
- Cancel your account and open a new one
- Review your billing statements carefully after the loss
  - If they show any unauthorized charges, it's best to send a letter to the card issuer describing each questionable charge.
- Credit Card Loss or Fraudulent Charges (FCBA).
  - Your maximum liability under federal law for unauthorized use of your credit card is \$50.
  - If the loss involves your credit card number, but not the card itself, you have no liability for unauthorized use
- ATM or Debit Card Loss or Fraudulent Transfers (EFTA).
  - Your liability under federal law for unauthorized use of your ATM or debit card depends on how quickly you report the loss.
  - You risk unlimited loss if you fail to report an unauthorized transfer within 60 days after your bank statement containing unauthorized use is mailed to you

### **If you have given out your bank account information**

- Report the theft of this information to the bank as quickly as possible
- Cancel your account and open a new one

### **If you have downloaded a virus or Trojan**

Some phishing attacks use viruses and/or Trojans to install programs called "key loggers" on your computer. These programs capture and send out any information that you type to the phisher, including credit card numbers, usernames and passwords, Social Security Numbers, etc. In this case, you should:

- Install and/or update anti-virus and personal firewall software
- Update all virus definitions and run a full scan
- Confirm every connection your firewall allows
- If your system appears to have been compromised, fix it and then change your password again, since you may well have transmitted the new one to the hacker
- Check your other accounts! The hackers may have helped themselves to many different accounts:
  - Check your eBay account, PayPal, your email ISP, online bank accounts, online trading accounts, Amazon.com and other e-commerce accounts, and everything else for which you use online password

### **If you have given out your personal identification information**

Identity theft occurs when someone uses your personal information such as your name, Social Security number, credit card number or other identifying information, without your permission to commit fraud or other crimes. If you have given out this kind of information to a phisher, you should do the following:

- Report the theft to the three major credit reporting agencies, Experian, Equifax and TransUnion Corporation, and do the following:
  - Request that they place a fraud alert and a victim's statement in your file.
  - Request a FREE copy of your credit report to check whether any accounts were opened without your consent.
  - Request that the agencies remove inquiries and/or fraudulent accounts stemming from the theft.
- Major Credit Bureaus
  - Equifax - [www.equifax.com](http://www.equifax.com)
    - To order your report, call: 800-685-1111 or write: P.O. Box 740241, Atlanta, GA 30374-0241
    - To report fraud, call: 800-525-6285 and write: P.O. Box 740241, Atlanta, GA 30374-0241
    - Hearing impaired call 1-800-255-0056 and ask the operator to call the Auto Disclosure Line at 1-800-685-1111 to request a copy of your report.
  - Experian - [www.experian.com](http://www.experian.com)
    - To order your report, call: 888-EXPERIAN (397-3742) or write: P.O. Box 2002, Allen TX 75013
    - To report fraud, call: 888-EXPERIAN (397-3742) and write: P.O. Box 9530, Allen TX 75013 TDD: 1-800-972-0322
  - Trans Union - [www.transunion.com](http://www.transunion.com)
    - To order your report, call: 800-888-4213 or write: P.O. Box 1000, Chester, PA 19022
    - To report fraud, call: 800-680-7289 and write: Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92634 TDD: 1-877-553-7803
- Notify your bank(s) and ask them to flag your account and contact you regarding any unusual activity:
  - If bank accounts were set up without your consent, close them.
  - If your ATM card was stolen, get a new card, account number and PIN.
- Contact your local police department to file a criminal report.
- Contact the Social Security Administration's Fraud Hotline to report the unauthorized use of your personal identification information.

- Notify the Department of Motor Vehicles of your identity theft.
  - Check to see whether an unauthorized license number has been issued in your name.
- Notify the passport office to be watch out for anyone ordering a passport in your nameFile a complaint with the Federal Trade Commission.
  - Ask for a free copy of "ID Theft: When Bad Things Happen in Your Good Name", a guide that will help you guard against and recover from your theft.
- File a complaint with the Internet Fraud Complaint Center (IFCC)
  - <http://www.ifccfbi.gov/index.asp>
  - The Internet Fraud Complaint Center (IFCC) is a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C), with a mission to address fraud committed over the Internet.
  - For victims of Internet fraud, IFCC provides a convenient and easy-to-use reporting mechanism that alerts authorities of a suspected criminal or civil violation.
- Document the names and phone numbers of everyone you speak to regarding the incident. Follow-up your phone calls with letters. Keep copies of all correspondence.