



## **E- SCAM/PHISHING**

### **Consumer Alert: Don't Fall Victim to Online Scams**

Your security is important to us. Here at IDB Bank we want to provide tools and resources to help prevent identity theft and educate you on security.

#### **What is “Phishing”?**

Phishing (FISHing)

Phishing is a high-tech scam that uses spam or pop up messages to attempt to deceive you into disclosing your credit card numbers, bank information, Social Security number, passwords, and/or other sensitive information.

#### **Example Citations**

Phishing is the term coined by hackers who imitate legitimate companies e-mails to entice people to share passwords or credit card numbers.

#### **What is “Spoofing”?**

Pretending to be something it is not, on the Internet, usually an e-mail or a Web site.

#### **How to report Phishing:**

We suggest reporting phishing e-mails or spoofed Web sites to the following groups:

- Forward the e-mail to [reportphishing@antiphishing.org](mailto:reportphishing@antiphishing.org).
- Forward the e-mail to the Federal Trade Commission at [spam@uce.gov](mailto:spam@uce.gov).
- Forward the e-mail to the “abuse” e-mail address at the company that is being spoofed (e.g., spoof@ebay.com).
- When forwarding spoofed messages, always include the original e-mail with its original header information intact.
- Notify the Internet Crime Complaint Center of the FBI by filing a complaint on their Web site: [www.ic3.gov](http://www.ic3.gov).

Recommended Actions if You've Become a Victim of a Phishing Scam

#### **If You Have Given Out Your Credit, Debit, or ATM Card Information**

Report the incident to the card issuer as quickly as possible.



## **E- SCAM/PHISHING**

Report using the toll-free numbers and 24-hour service that many companies have established to deal with such emergencies

Request your card issuer to close your compromised account number and reissue you a new card with a different number.

Monitor you account activity and review account statements carefully after the information loss.

If any unauthorized charges appear, call the card issuer immediately and follow up with a hard copy letter via a traditional delivery such as the U.S. Postal Service (keep a copy for yourself) describing each questionable charge.

### **Credit Card Loss or Fraudulent Charges**

Your maximum liability under federal law for unauthorized use of your credit card is generally \$50. However, that \$50 potential liability probably does not apply for unauthorized telephone and Internet transactions because is “no means to identify the cardholder,” in those cases.

### **ATM or Debit Card Loss or Fraudulent Transfers**

- 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 and unauthorized use is mailed to you for transactions made after that 60-day period.

### **If You Have Given Out Your Bank Account Information**

- Report the theft of this information to the bank as quickly as possible.
- Request your bank close the compromised account and re-open a like account with a different number.



## **E- SCAM/PHISHING**

### **If you have downloaded a Virus or “Trojan Horse”**

Some phishing attacks use viruses and/or “Trojan horses” 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, user names and passwords, Social Security numbers, etc. If this happens, it’s likely you may not be aware of it until you notice unusual transactions on your account. To minimize this risk you should:

- Install and/or update antivirus and personal firewall software.
- Update all virus definitions and run a full scan.
- If your system appears to have been compromised, repair it and then change your password again, since you may well have transmitted the new one to a hacker.
- Check your other accounts! The fraudsters may have helped themselves to many different accounts: E-bay account, PayPal, your e-mail ISP; online bank accounts, online trading accounts and other e-commerce accounts, and everything else for which you use online passwords.

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

If you believe you have given out your personal information such as your name, address, social security number to someone who may use it for fraud:

Contact the three major credit reporting agencies- Experian, Equifax, TransUnion- and do the following:

- Request that the agencies 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.



## **E- SCAM/PHISHING**

### **Major Credit Bureaus**

#### **Equifax – [www.equifax.com](http://www.equifax.com)**

- To order your report, call: 800-685-1111 or write PO box 704201, Atlanta, GA 30374-0241.
- To report fraud, call: 800-525-6285 and write: PO 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 order your report, call: 888-EXPERIAN (397-3742) or write: P.O. Box 9530, Allen, TX. 75013. TDD: 1-800-792-0322.

#### **Trans Union – [www.transunion.com](http://www.transunion.com)**

- To order your report, call: 800-88-4213 or write: P.O. Box 1000, Chester, PA 19022.
- To report fraud, call: 1-800-680-7289 and write: Fraud Victim Assistance Division., P.O. Box 6790, Fullerton, CA 92634 TDD: 1-877-553-7803.



## **E- SCAM/PHISHING**

### **Additional Actions to Take**

- If bank accounts were set up with your consent, close them.
- 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 authorized driver's license number has been issued in your name.
- Notify the passport office to be on the lookout for anyone ordering a passport in your name.
- File 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- and guard against it in the future.
- File a complaint with the Internet Crime Complaint Center (IC3) by visiting their Web site: [www.ic3.gov](http://www.ic3.gov). IC3 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, the Center 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.

### **ID Theft Resources**

<http://www.consumer.gov/idtheft/>

<http://www.identity-theft-help.us/>

<http://www.identitytheft.org/>

<http://www.usdoj.gov/criminal/fraud/idtheft.html>

<http://www.ic3.gov>

<http://www.ftc.gov/bcp/online/pubs/alerts/phishingalrt.htm>



## E- SCAM/PHISHING

### How to Practice Safe Computing

The number and sophistication of phishing and spoofing scams sent out to consumers is continuing to increase dramatically. While online banking is widely considered to be as safe as or safer than in-branch or ATM banking, as a general rule you should be careful about giving out your personal financial information over the Internet. Remember, no reputable financial institution will ever request your personal information via e-mail.

Here is a list of recommendations to follow in order to avoid becoming a victim of scams:

1. **Be suspicious of any e-mail with urgent requests for personal financial information.** Phishers have been known to include upsetting or enticing (but false) statements in their emails to get people to react immediately. More recently, some phishers have toned down their language, as email recipients have become more aware of the use of this tactic. Either way, the e-mail typically asks for information such as user names, passwords, credit card numbers, Social Security numbers, etc.
2. **Be careful of e-mails that are not personalized and /or may contain spelling error and/or awkward syntax and phrasing.** Many phishing e-mails are sent in great bulk, and, therefore are not personalized. If you are suspicious of an e-mail claiming to be from your institution that is not personalized, call your institution before responding. Many also are being sent from other countries from individuals for whom English is a foreign language, thus resulting in misspelled words and awkward syntax and phrasing.
3. **Be careful of personalized e-mails that ask for personal financial information.** Be suspicious of any e-mail that contains some personal financial information, such as a bank account number and asks for other information, such as a PIN. Your bank will never ask for or send you personal financial information by e-mail.



## **E- SCAM/PHISHING**

4. **Do not use links in an e-mail to get to any Web page.** Instead they call the bank on the telephone to confirm the address, or log onto the Web site directly by typing in the Web address in your browser.
5. **Do not complete forms in e-mail messages that ask for personal information.** Your financial institution would never ask you to complete such a form within an e-mail message.