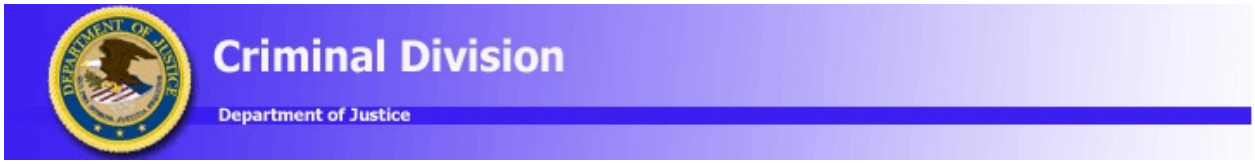

SPECIAL REPORT ON "PHISHING"

Background

During 2003 and early 2004, law enforcement authorities, businesses, and Internet users have seen a significant increase in the use of "phishing." "Phishing" is a general term for criminals' creation and use of e-mails and websites – designed to look like e-mails and websites of well-known legitimate businesses, financial institutions, and government agencies – in order to deceive Internet users into disclosing their bank and financial account information or other personal data such as usernames and passwords. The "phishers" then take that information and use it for criminal purposes, such as identity theft and fraud.

A growing number of phishing schemes are using for illegal purposes the names and logos of legitimate financial institutions, businesses, and government agencies in North America, Europe, and the Asia-Pacific region. One industry organization, the Anti-Phishing Working Group (www.antiphishing.org) has reported that in January 2004, there were 176 unique phishing attacks reported to it – an increase of more than 50 percent over the number of reported phishing attacks in December 2003.

The Department of Justice is issuing this Special Report to inform Internet users about the risks of responding to phishing e-mails and websites, whether phishing schemes violate federal criminal laws, and the steps that Internet users should take when they see possible phishing e-mails or websites.

What Are The Risks of Responding to Phishing E-Mails?

At first glance, phishing e-mails, and the websites associated with such e-mails, may appear completely legitimate. One recent phishing attempt falsely used the names of the Federal Deposit Insurance Corporation (FDIC) and two of its officials, as well as the Department of Homeland Security. What Internet users may not realize is that criminals can easily copy logos and other information from legitimate businesses' websites and place them into phishing e-mails and websites.

In addition, if the e-mail recipient clicks on the link in the e-mail, even the window of the Internet browser he or she is using may contain what looks like the true Uniform Resource Locator (URL) of a legitimate business or financial institution. Unfortunately, some phishing schemes have exploited a vulnerability in the Internet Explorer browser. This vulnerability

allows phishers to set up a fake website at one place on the Internet, but make it look like the Internet user is accessing a legitimate website at another place on the Internet.

Most phishing e-mails include false statements intended to create the impression that there is an immediate threat or risk to the bank, credit-card, or financial account of the person who receives that e-mail. In the case of the false FDIC e-mails mentioned above, the text of the e-mails falsely claimed that the Secretary of Homeland Security had advised the FDIC to suspend all federal deposit insurance on the recipients' bank accounts. Other recent phishing e-mails have falsely claimed that the recipients' Visa credit card was being used by another person, or that a recent credit-card transaction had been declined.

In some cases, phishing e-mails have promised the recipients a "prize" or other special benefit. Although the message sounds attractive rather than threatening, the object is the same: to trick recipients into disclosing their financial and personal data.

People who receive phishing e-mails also may not realize that the senders may have used "spamming" (mass e-mailing) techniques to send the e-mail to thousands and thousands of people. This means that many of the people who receive that spammed e-mail do not have accounts or customer relationships with the legitimate business or financial services company that the e-mails purport to come from. The people who create phishing e-mails count on the fact that some recipients of those e-mails will have an account or customer relationship with that legitimate business or company, and may be more likely to believe that the e-mail has come from a trusted source.

Ultimately, people who respond to phishing e-mails, and input the requested financial or personal information into e-mails, websites, or pop-up windows, may be putting their accounts and financial status at risk in three significant ways. First, phishers can use the data to access existing accounts of those Internet users, and withdraw money or buy expensive merchandise or services. Second, phishers can use the data to open new bank or credit-card accounts in the victims' names, and use the new accounts to cash bogus checks or buy merchandise. If the phishers open those new accounts with the victims' names, but use addresses other than the victims', the Internet users may not realize that they have become victims of identity theft until they are contacted by creditors or they check their credit reports. Third, some recent phishing schemes have involved the use of computer viruses and worms to disseminate the phishing e-mails to still more people.

Can Phishing Violate Federal Criminal Laws?

Because they use false and fraudulent statements to deceive people into disclosing valuable personal data, phishing schemes may violate a variety of federal criminal statutes. In many phishing schemes, the participants in the scheme may be committing identity theft (18 U.S.C. § 1028(a)(7)), wire fraud (18 U.S.C. § 1343), credit-card (or "access-device") fraud (18 U.S.C. § 1029), bank fraud (18 U.S.C. § 1344), computer fraud (18 U.S.C. § 1030(a)(4)), and the newly enacted criminal offenses in the CAN-SPAM Act (18 U.S.C. § 1037). When a phishing scheme also uses computer viruses or worms, participants in the scheme may also violate other

provisions of the computer fraud and abuse statute relating to damage to computer systems and files (18 U.S.C. § 1028(a)(5)). Finally, phishing schemes may violate various state statutes on fraud and identity theft.

Each of the federal criminal offenses mentioned above carries substantial penalties. Sentences can range as high as 30 years imprisonment under the wire fraud and bank fraud statutes, 15 years imprisonment for identity theft and credit-card fraud, and 5 years imprisonment under the CAN-SPAM Act. In addition, federal judges can impose substantial fines, which can be as high as $250,000 for an individual, and require forfeiture of a defendant's property. The Department of Justice has successfully prosecuted a number of criminal cases involving phishing, and will vigorously prosecute phishing schemes in appropriate cases in the future.

What Should Internet Users Do About Phishing Schemes?

The Department of Justice recommends that Internet users follow three simple rules when they see e-mails or websites that may be part of a phishing scheme: ***Stop***, ***Look***, and ***Call***.

1. ***Stop***. Phishers typically include upsetting or exciting (but false) statements in their e-mails with one purpose in mind. They want people to react immediately to that false information, by clicking on the link and inputting the requested data before they take time to think through what they are doing. Internet users, however, need to resist that impulse to click immediately. No matter how upsetting or exciting the statements in the e-mail may be, there is always enough time to check out the information more closely.

2. ***Look***. Internet users should look more closely at the claims made in the e-mail, think about whether those claims make sense, and be highly suspicious if the e-mail asks for numerous items of their personal information such as account numbers, usernames, or passwords. For example:
   - If the e-mail indicates that it comes from a bank or other financial institution where you have a bank or credit-card account, but tells you that you have to enter your account information again, that makes no sense. Legitimate banks and financial institutions already have their customers' account numbers in their records. Even if the e-mail says a customer's account is being terminated, the real bank or financial institution will still have that customer's account number and identifying information.
   - If the e-mail says that you have won a prize or are entitled to receive some special "deal," but asks for financial or personal data, there is good reason to be highly suspicious. Legitimate companies that want to give you a real prize don't ask you for extensive amounts of personal and financial information before you're entitled to receive it.

3. ***Call***. If the e-mail or website purports to be from a legitimate company or financial institution, Internet users should call or e-mail that company directly and ask whether the e-mail or website is really from that company. To be sure that they are contacting the real company or institution where they have accounts, credit-card accountholders can call

the toll-free customer numbers on the backs of their cards, and bank customers can call the telephone numbers on their bank statements.

A number of legitimate companies and financial institutions that have been targeted by phishing schemes have published contact information for reporting possible phishing e-mails, as well as online notices about how their customers can recognize and protect themselves from phishing. This list will be periodically updated as appropriate.

Company	Telephone	E-mail/Notice
America Online (AOL)	800-827-6364	http://www.aol.com
Bank of America	Call customer service number on bank statement	*Notice*: http://www.bankofamerica.com/privacy/index.cfm?template=privacysecur_personal_family&statecheck=DC
Bank One	1-877-226-5663 [Personal Accounts] 1-800-404-4111 [Business Accounts] 1-888-745-0091 [Credit Cards]	*Notice*: http://www.bankone.com/answers/BolAnswersDetail.aspx?top=all&segment=ABO&topic=Promotion&item=BankOneCustomerAlert
Citibank	800-374-9700 800-788-0002 [TTY]	http://www.citibank.com
EarthLink	800-327-8454	*E-Mail*: fraud@abuse.earthlink.net [Forwarded e-mails] *Live Chat*: http://support.earthlink.net/chat *Notice*: http://support.earthlink.net/mu/1/psc/img/walkthroughs/other/policy_procedure/8492.psc.html
eBay	--	*E-Mail*: spoof@ebay.com [Note: Forwarded messages only] *Notice*: http://pages.ebay.com/help/confidence/isgw-account-theft-spoof.html
FleetBoston Financial	800-841-4000	*Notice*: http://www.fleet.com/home.asp
PayPal	--	*E-Mail*: spoof@paypal.com [Note: Forwarded messages only] *Notice*: http://www.paypal.com/cgi-bin/webscr?cmd=p/gen/email-security-outside
US Bank	1-877-595-6256 [toll-free]	*E-Mail*: fraud_help@usbank.com *Notice*: http://www.usbank.com/cgi_w/cfm/promo/personal/fraud_email_info_and_help.cfm

Note: Internet users who want to e-mail, or go to a website for, one of the companies listed above should type in the e-mail address exactly as it appears above. Typing in the address is the only way to be certain that a browser will go to the legitimate company's website. No one should ever rely on any information that appears in a phishing e-mail.

In addition, people who use the Internet Explorer browser should immediately go to the Microsoft Security home page -- http://www.microsoft.com/security/ -- to download a special patch relating to certain phishing schemes. This URL should be typed into the browser window to make certain that the browser will go to the real Microsoft Security website.

The Department of Justice asks the public to report possible phishing schemes promptly to law enforcement. The sooner that law enforcement and legitimate businesses learn about new phishing e-mails and websites, the sooner those e-mails and websites can be shut down and appropriate law enforcement action taken.

If you may have disclosed your personal information to a possible phishing e-mail or website, you should immediately file an online complaint with the Internet Crime Complaint Center (a joint project of the FBI and the National White Collar Crime Center) at http://www.ic3.gov. Because that disclosure of personal information may put you at risk of becoming a victim of identity theft, you also should go to the Federal Trade Commission's identity theft website, at http://www.consumer.gov/idtheft, and follow the directions there for reporting information to credit bureaus, credit-card companies, and law enforcement.

If you have received a possible phishing e-mail, but have not yet responded to it, do not respond. Instead, send copies of the e-mail to the Federal Trade Commission at uce@ftc.gov and the Anti-Phishing Working Group at reportphishing@antiphishing.org.

Further Information

- ***Phishing***: Read the Federal Trade Commission's publication, "How Not to Get Hooked by a 'Phishing' Scam," at http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm.
- ***Identity Theft***: Visit the Department of Justice's webpages at http://www.usdoj.gov/criminal/fraud/idtheft.html and http://www.usdoj.gov/criminal/fraud/idquiz.html, and the Postal Inspection Service's website at http://www.usps.com/postalinspectors/id_intro.htm.
- ***Cybercrime***: Visit the Department of Justice's website at http://www.cybercrime.gov.

* * *