DOLLARS & Sense
FAMILY FINANCIAL EDUCATION FOUNDATION
Family Financial Education Foundation
Edition 5, Volume 6

Personal Information Scams (Phishing)

The most popular and consequently the most dangerous form of e-mail fraud is "Phishing." Phishing is any fraudulent attempt to obtain any of your private information such as your user names, passwords, and credit card details by someone posing as a legitimate organization through electronic messages, most typically e-mail or instant messaging.

The first recorded use of the term "phishing" is thought to be in 1996, although the term also seems to have been used before that. A variant of "fishing," it implies baiting someone to "catch" protected information. Social websites such as YouTube, Facebook, MySpace, Windows Live Messenger; auction sites such as eBay; online banks such as Wells Fargo, Bank of America, Chase; online payment processors such as PayPal; and e-mail services such as Yahoo have all fallen victim to being used by phishers to lure innocent consumers to reveal information that can be used fraudulently.

The main thing phishing e-mail messages have in common is that they ask for personal data by directing you to websites or providing phone numbers for you to call where they ask you to provide personal data. Experiments have shown a success rate of more than 70% for phishing attacks on social networks, and the growth of phishing since 2004 is alarming.

Phishing e-mail messages may appear to be from a legitimate organization, such as your financial institution, or a retailer that you may have done business with previously. These e-mails often direct you to a website that mimics the legitimate website and ask you to "update" or "verify" your personal information, resulting in identity theft. Phishing e-mail often includes official-looking logos and other identifying information taken directly from legitimate websites, and it may include convincing details about your personal information that scammers found on your social networking pages.

Other forms of phishing e-mails include e-mails that warn you there is fraudulent activity on an account of yours and ask you to click through to verify your information, and e-mails that claim you will lose something

(Continued on page 4)

What Is E-mail Fraud and How Can I Protect Myself From It?

Unfortunately, when times get hard, some people look for ways to make it even harder for honest members of the community like you. The United States Secret Service warns that people lose millions of dollars annually due to fraud, and the losses are getting larger all the time.

E-mail is an increasingly popular way to distribute fraudulent messages to potential victims because it is inexpensive and relatively easy to set up. Some of the most common fraudulent messages are hoaxes or chain mails that don't ask for money. Others involve money stories or ask directly for personal information. But all of them are designed to trick you into passing on data that leads to loss for you.

FFEF wants to help you avoid becoming one of the millions of victims of e-mail fraud this year, so in this newsletter you'll find information about various types of e-mail fraud and how you can recognize them in your Inbox. By taking a few precautions, you can reduce your chances of falling unknowingly into the e-mail fraud trap. ■

Nigerian Bank Scams or 4-1-9 Fraud

Another alarming form of e-mail fraud in recent months involves e-mails claiming to be "official orders" from the FBI's Anti-Terrorist and Monetary Crimes Division, most especially from an alleged FBI unit in Nigeria. The latest versions even use the names of several high-ranking executives within the FBI. These are sometimes referred to as advance-fee fraud schemes or 4-1-9 fraud, named such for the section of the Nigerian penal code that deals with fraud schemes.

Nigerian schemers, who pretend to be government officials or bank officials, send e-mail letters to individuals and businesses in the US. The letters state that a reputable company or individual in the US is needed to help the sender deposit an overpayment on a contract. Some e-mails pretend to be the son or daughter of a murdered official pleading for help to deposit his or her inheritance in a US bank. The person who receives the e-mail may be promised a portion of the money in return for his or her help. The e-mail recipient is asked to provide funds to cover bank fees and is asked for personal information such as social security numbers, bank account numbers, and other similar data. If the recipient is sympathetic and provides this information, he or she often soon finds that their bank accounts have been emptied.

Other forms of e-mail fraud claiming to be from the FBI inform recipients they have been named the beneficiary of millions of dollars from an inheritance or a lottery winning. Recipients are told that to claim the large sum of money, they must furnish certain personal information and the e-mail may threaten the recipient with a penalty, such as prosecution, if they don't provide the information. Still others state that the recipient has extorted money and has a limited amount of time to refund the money or face prosecution.

The FBI warns anyone who receives such an e-mail not to respond. The FBI does not send unsolicited e-mails like these. FBI executives do not personally contact consumers regarding such matters. They do not send threatening letters to consumers demanding payments for crimes. You should not respond to any unsolicited e-mails or click on any links within the e-mail as they may contain viruses.

If you receive unsolicited e-mail messages you suspect are fraudulent, you can report them to the Federal Trade Commission. To do so, forward the message exactly as you receive it to spam@uce.gov. Then delete the e-mail message from your Inbox immediately after.

You can report these types of messages to the Internet Crime Complaint Center, which was established to help protect you from such e-mail fraud. The Internet Crime Complaint Center (IC3) is a partnership between the Federal Bureau of Investigation (FBI), the National White Collar Crime Center (NW3C), and the Bureau of Justice Assistance (BJA). It was established to stop Internet crime. An easy-to-use reporting system has been set up that alerts authorities of suspected criminal violations.

The Internet Crime Complaint Center accepts online crime complaints from either the e-mail recipient or from a third party affected by the complaint. If you were to make such a complaint, the Internet Crime Complaint Center needs accurate and complete information from you. You will be asked to provide the following information when filing a complaint:

- Your name
- Your mailing address
- Your telephone number
- The name, address, telephone number, and Web address, if available, of the individual or organization you believe defrauded you.
- Specific details on how, why, and when you believe you were defrauded.
- Any other relevant information you believe is necessary to support your complaint.

The FBI makes the following warnings when assessing the legitimacy of e-mails you receive.

- If the "opportunity" appears too good to be true, it probably is.
- Do not reply to e-mails asking for personal banking information.
- Be wary of individuals representing themselves as foreign government officials.
- Be cautious when dealing with individuals outside of your own country.
- Beware when asked to assist in placing large sums of money in overseas bank accounts.
- Do not believe the promise of large sums of money for your cooperation.
- Guard your account information carefully.
- Be cautious when additional fees are requested to further the transaction. ■

The Latest Alert from the Federal Trade Commission

If the recent changes in the financial marketplace have you confused, you're not alone. The financial institution where you did business last week may have a new name today, and your checks and statements may come with a new look tomorrow. A new lender may have acquired your mortgage, and you could be mailing your payments to a new location. The upheaval in the financial marketplace may spur scam artists to phish for your personal information.

You may receive attention-getting e-mails that look like they're coming from the financial institution that recently acquired your bank, savings and loan, or mortgage. Their intent is to collect or capture your personal information, like your credit card numbers, bank account information, Social Security number, passwords, or other sensitive information. Their messages may ask you to "update," "validate," or "confirm" your account information. For example, you may see messages like:

"We recently purchased ABC Bank. Due to concerns for the safety and integrity of our new online banking customers, we have issued this warning message... Please follow the link below to renew your account information."

"We recently acquired the mortgage on your home and are in the process of validating account information. Please click here to update and verify your information."

"During our acquisition of XYZ Savings & Loan, we experienced a data breach. We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below to confirm your identity."

The messages direct you to a website that looks like the actual site of your new financial institution or lender. But it isn't. It's a bogus site whose purpose is to trick you into divulging your personal information so the operators can steal your identity and run up bills or commit other crimes in your name.

The Federal Trade Commission offers these tips to help you avoid falling victim to a phishing scam:

- Don't reply to an e-mail or pop-up message that asks for personal or financial information, and don't click on links in the message – even if it appears to be from your bank.
- Don't cut and paste a link from the message into your Web browser, either. Phishers can make links look like they go one place, but actually redirect you to another.
- Some scammers send an e-mail that appears to be from an institution and asks you to call a phone number to update your account. Because of the technology they use, the area code you call does not reflect where the scammers are. To reach an institution you do business with, call the number on your financial statements.
- Use anti-virus and anti-spyware software, as well as a firewall, and update them regularly.
- Don't e-mail personal or financial information. E-mail is not a secure way to send sensitive information.
- Review your financial account statements as soon as you receive them to check for unauthorized charges.
- Be cautious about opening any attachment or downloading any files from e-mails you receive, regardless of who sent them. These files can contain viruses or other software that can weaken your computer's security.
- Forward phishing e-mails to spam@uce.gov—and to the institution or company impersonated in the phishing e-mail.

If you've been scammed, visit the Federal Trade Commission's Identity Theft website at ftc.gov/id theft for important information on the next steps to take.

For more tips from the federal government and the technology industry about possible e-mail fraud and to help you be on guard against such fraud, secure your computer, and protect your personal information, visit www.OnGuardOnline.gov. ■

Phishing phrases to watch out for:

"Verify your account"

Legitimate businesses should not ask you to reveal passwords, user names, or social security numbers.

"You have won the lottery"

Lottery scams often include references to big companies, such as Microsoft. There is no Microsoft lottery.

"If you don't respond within 48 hours, your account will be closed."

These messages convey a sense of urgency so that you'll respond immediately without thinking. A phishing e-mail message might even claim that your response is required because your account might have been compromised.

"Click the link below to gain access to your account."

This is an example of a phrase in an e-mail message that directs you to a phishing website. ■

TIPS & TRICKS

Fraudulent IRS E-mails

In recent years, even the Internal Revenue Service has been the victim of phishers attempting to lure innocent consumers to reveal information. E-mails, supposedly from the Internal Revenue Service, have been used to glean sensitive data from U.S. taxpayers. A sample e-mail masquerading as a notice from the IRS appears below. The actual e-mail would also include the same IRS header that appears on the legitimate IRS website.

From: Internal Revenue Service [mailto:admin@irs.gov]

Sent: Wednesday, March 01, 2008 12:45 PM

To: john.doe@jdoe.com

Subject: IRS Notification - Please Read This.

After the last annual calculations of your fiscal activity we have determined that you are eligible to receive a tax refund of $63.80. Please submit the tax refund request and allow us 6-9 days in order to process it.

A refund can be delayed for a variety of reasons. For example submitting invalid records or applying after the deadline.

To access the form for your tax refund, please click here

Regards, Internal Revenue Service

It is easy to see how this could be mistaken for a legitimate e-mail from the IRS so how do you know that it's not? The IRS has provided the following important information to help prevent you from "clicking through" on these e-mails:

- The IRS does not initiate taxpayer communications through e-mail.
- The IRS does not request detailed personal information through e-mail.
- The IRS does not send e-mails requesting your PIN numbers, passwords, or similar access information for credit cards, banks, or other financial accounts.

If you receive an e-mail claiming to be from the IRS or directing you to an IRS site,

- Do not reply.
- Do not open any attachments. Attachments may contain malicious code that will infect your computer.
- Do not click on any links.

If you receive an e-mail or find a website you think is pretending to be the IRS, forward the e-mail or website URL to the IRS at phishing@irs.gov. After you forward the e-mail, delete the message.

The important thing to know is that the IRS will never contact you by e-mail. They will always send you a letter by postal service mail. ■

We have new business hours!

Monday-Friday:
7:00 a.m.-9:00 p.m.
Saturday:
7:00 a.m.-4:00 p.m.

(Continued from page 1)

such as a bank account. Phishing scams attempt to trick you into clicking through immediately by using messages that cause you to panic. Claims like these nearly always indicate a phishing scam as responsible companies and organizations don't take these types of actions by e-mail. If you think the message may be legitimate, type the company's website address into your browser without clicking through from the e-mail, or contact the company by the telephone number on legitimate correspondence you have from the company to see if the e-mail message is legitimate. ■

Protect yourself and your family. Learn more with one of our counselors.

Don't forget to share your wealth of knowledge with friends and family. Our budget planning programs and education are available to everyone. Call today for more information and let us help you clean up your financial life a little this season!

www.ffef.org
www.accesseducation.org

(877) 789-4175

Family Financial Education Foundation

ACCESS EDUCATION SYSTEMS
724 Front Street, Suite 340
Evanston, WY 82930
contact: (877) 789-4175
www.ffef.org | info@ffef.org