U.S. EQUAL EMPLOYMENT OPPORTUNITY COMMISSION
Washington, D.C. 20507

Office of
Inspector General
Aletha L. Brown – Inspector General

July 22, 2005

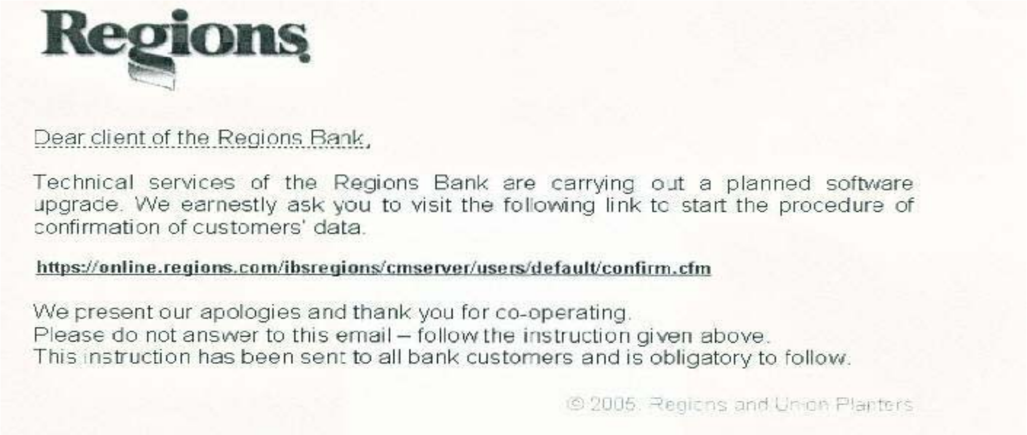
OIG Fraud Alert – "Phishing"

What is "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. "Phishing" is by far the most dangerous form of fraud to hit online commerce, costing U.S. banks alone $1.2 billion in direct losses, increasing insurance rates and eroding consumer confidence in online transactions.[1] According to the *Washington Pos*t "phishing," has become so widespread that one technology consultant estimated that at least 57 million Americans have received these types of e-mails.

According to the *Federal Trade Commission* (FTC), "phishers" send an email or pop-up message that claims to be from a business or organization that you deal with – for example, your Internet service provider (ISP), bank, online payment service, or even a government agency. The message usually says that you need to "update" or "validate" your account information.

[1] 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.



Regions

Dear client of the Regions Bank,

Technical services of the Regions Bank are carrying out a planned software upgrade. We earnestly ask you to visit the following link to start the procedure of confirmation of customers' data.

https://online.regions.com/ibsregions/cmserver/users/default/confirm.cfm

We present our apologies and thank you for co-operating.
Please do not answer to this email – follow the instruction given above.
This instruction has been sent to all bank customers and is obligatory to follow.

© 2005. Regions and Union Planters

Example: "Phishing"

It might threaten some dire consequence if you don't respond. The message directs you to a Web site that looks just like a legitimate organization's site, but it isn't. The purpose of the bogus site? To trick you into divulging your personal information so the operators can steal your identity and run up bills or commit crimes in your name.

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 the websites of legitimate businesses 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 vulnerabilities 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.

The Federal Bureau of Investigations (FBI) calls "phishing" the "hottest and most troublesome" scam on the Internet, and the Department of Justice has created a special unit aimed at identifying and prosecuting the perpetuators of these scams. According to the Anti-Phishing Working Group, banks are particularly vulnerable to "phishing" attacks, with 15 of the top 20 "phishing" scams aimed at the banking industry. "Phishing" is remarkably sophisticated and successful, having fooled nearly 2 million online users into revealing personal and confidential information in the past two years. The most recent "phishing" attacks have targeted non-English speaking countries, such as France and Germany, a prime indication that this type of fraud is getting not only more sophisticated, but has no geographical boundaries.

What Can You Do to Protect Yourself?

The Anti-Phishing Working Group has compiled a list of recommendations below that you can use to avoid becoming a victim of these scams.

- Be suspicious of any email with urgent requests for personal financial information
    - unless the email is digitally signed[2], 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, etc.
    - phisher emails are typically NOT personalized, while valid messages from your bank or e-commerce company generally are
- Don't use the links in an email to get to any web page, if you suspect the message might not be authentic
    - 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 ensure that you're using a secure website when submitting credit card or other sensitive information via your Web browser
    - to make sure you're on a secure Web server, check the beginning of the Web address in your browsers address bar - it should be "https://" rather than just "http://"
- Regularly log into your online accounts
    - don't leave it for as long as a month before you check each account
- Regularly check your bank, credit and debit card statements to ensure that all transactions are legitimate
    - if anything is suspicious, contact your bank and all card issuers
- Ensure that your browser is up to date and security patches applied
    - in particular, people who use the Microsoft 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

[2] A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message, or of the signer of a document. It can also be used to ensure that the original content of the message or document that has been conveyed is unchanged.

The Federal Trade Commission (FTC), the nation's consumer protection agency, suggests other tips to help you avoid getting hooked by a "phishing" scam:

- Review credit card and bank account statements as soon as you receive them to determine whether there are any unauthorized charges. If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.
- Use anti-virus software and keep it up to date. Some "phishing" emails contain software that can harm your computer or track your activities on the Internet without your knowledge. Anti-virus software and a firewall can protect you from inadvertently accepting such unwanted files. Anti-virus software scans incoming communications for troublesome files. Look for anti-virus software that recognizes current viruses as well as older ones; that can effectively reverse the damage and that updates automatically. A firewall helps make you invisible on the Internet and blocks all communications from unauthorized sources. It's especially important to run a firewall if you have a broadband connection. Finally, your operating system (like Windows or Linux) may offer free software "patches" to close holes in the system that hackers or "phishers" could exploit.
- Be cautious about opening any attachment or downloading any files from emails you receive, regardless of who sent them.
- Report suspicious activity to the FTC. If you believe you've been scammed, file your complaint at www.ftc.gov, and then visit the FTC's Identity Theft Web site at www.consumer.gov/idtheft to learn how to minimize your risk of damage from ID theft. Visit www.ftc.gov/spam to learn other ways to avoid email scams and deal with deceptive spam.

What To Do If You Have Given Out Your Personal Financial Information?

"Phishing" attacks are growing quite sophisticated and difficult to detect, even for the most technically savvy people. Also, many people are getting onto the Internet and using email or Web browsers for the first time. As a result, some people are going to continue to be fooled into giving up their personal financial information in response to a "phishing" email or on a "phishing" website. If you have been tricked this way, you should assume that you will become a victim of credit card fraud, bank fraud, or identity theft. Advice given by the Anti- "Phishing" Working Group on what to do if you are in this situation is listed below:

<u>If you have given out your credit card or debit or ATM card information</u>

- 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
    - 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
    - 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

Be careful with your personal information. Protect your identity.

IF YOU HAVE ANY QUESTION PLEASE FEEL FREE TO CALL THE OFFICE OF INSPECTOR GENERAL AT 202-663-4327 OR E-MAIL US AT INSPECTOR.GENERAL@EEOC.GOV