

4/4/2005



## **NYS Office for Technology (OFT) Customer Relations Communication**

**Number: CRC-052**

**Date: March 29, 2005**

**Topic: E mail scam targeting Key Bank customers**

**Contact(s):** Your OFT Customer Relations representative, or call  
1-866-789-4OFT

It has been reported that staff have received e-mail messages such as one targeting Key Bank customers, indicating there may be a problem with the customer account and providing them with instructions on how to correct the situation. The instructions direct the email recipient to click on a link that takes them to a web site, prompting for personal information such as a pin number, social security number, bank account number or credit card number. Both the link and web site closely resemble an authentic Key Bank web site.

If you receive an email requesting personal information, from Key Bank, Citibank, or any other bank or business, **do not click on the link**. In some cases, just opening the link may cause malicious software to be downloaded to your computer. One way that you can tell the email is fake is by moving your mouse over the URL (at least in OUTLOOK) and you can see the displayed URL doesn't match the actual URL.

Never give personal information in response to an email requesting it. Any reputable business will not request personal information in this manner. This type of scam is known as 'phishing' (pronounced 'fishing') and has quickly become a popular, and unfortunately successful, social engineering technique that can lead to not only monetary loss but also identity theft.

(Please note that Websense, an OFT Internet filter may identify the email as Phishing and block the user from opening the link.) For more information on how to identify phishing scams, and what to do if you receive one, please see the U.S. Federal Trade Commission's Alert below

### **FTC Consumer Alert**

How Not to Get Hooked by a 'Phishing' Scam

Internet scammers casting about for people's financial information have a new way to lure unsuspecting victims: They go "phishing."

4/4/2005

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

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. 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.

The FTC, the nation’s consumer protection agency, suggests these tips to help you avoid getting hooked by a phishing scam:

- If you get an email or pop-up message that asks for personal or financial information, do not reply or click on the link in the message. Legitimate companies don’t ask for this information via email. If you are concerned about your account, contact the organization in the email using a telephone number you know to be genuine, or open a new Internet browser session and type in the company’s correct Web address. In any case, don’t cut and paste the link in the message.
- Don’t email personal or financial information. Email is not a secure method of transmitting personal information. If you initiate a transaction and want to provide your personal or financial information through an organization’s Web site, look for indicators that the site is secure, like a lock icon on the browser’s status bar or a URL for a website that begins “https:” (the “s” stands for “secure”). Unfortunately, no indicator is foolproof; some phishers have forged security icons.
- 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.

4/4/2005

- 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 get spam that is phishing for information, forward it to [spam@uce.gov](mailto:spam@uce.gov). If you believe you've been scammed, file your complaint at [www.ftc.gov](http://www.ftc.gov), and then visit the FTC's Identity Theft Web site at [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft) to learn how to minimize your risk of damage from ID theft. Visit [www.ftc.gov/spam](http://www.ftc.gov/spam) to learn other ways to avoid email scams and deal with deceptive spam.

If you have any questions, please call your customer relations manager or the Customer Relations main telephone number 1 866 789-4638. Thank you in advance for your continued cooperation.

The OFT Customer Relations Team

OFT Customer Relations  
1-866-789-4OFT (4638) or 402-2537  
[oft.sm.cs.customer.relations](mailto:oft.sm.cs.customer.relations)