FTC Consumer Alert

Federal Trade Commission ■ Bureau of Consumer Protection ■ Division of Consumer & Business Education

Bank Failures, Mergers and Takeovers: A "Phish-erman's Special"

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 servicer. Procedures for the banking you do online also may have changed. According to the Federal Trade Commission (FTC), the nation's consumer protection agency, the upheaval in the financial marketplace may spur scam artists to phish for your personal information.

Phishers (pronounced "fishers') may send attention-getting emails 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 FTC suggests these tips to help you avoid getting hooked by a phishing scam:

- Don't reply to an email 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 call with a recorded message, or send an email that appears to be from an institution, and ask you to call a phone number to update your account. Because they use Voice

over Internet Protocol technology, 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 email personal or financial information. Email 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 emails you receive, regardless of who sent them. These files can contain viruses or other software that can weaken your computer's security.
- Forward phishing emails to **spam@uce.gov** – and to the institution or company impersonated in the phishing email. You also may report phishing email to **reportphishing@antiphishing.org**. The Anti-Phishing Working Group, a consortium of ISPs, security vendors, financial institutions and law enforcement agencies, uses these reports to fight phishing.

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

For more tips from the federal government and the technology industry to help you be on guard against Internet fraud, secure your computer, and protect your personal information, visit **www.OnGuardOnline.gov**.

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint or to get free information on consumer issues, visit **ftc.gov** or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters consumer complaints into the Consumer Sentinel Network, a secure online database and investigative tool used by hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

FEDERAL TRADE COMMISSION	ftc.gov
1-877-FTC-HELP	FOR THE CONSUMER

October 2008