

# Protecting Yourself Against E-mail Fraud

Internet “phishing” scams are one of the fastest-growing frauds today. Phishing typically involves a bogus e-mail message that uses legitimate materials, such as a credit union or other organization’s Web site graphics and logos—the “look and feel”—in an attempt to entice e-mail recipients to provide personal financial details, such as account information, credit card and Social Security numbers.

Financial institutions, government agencies, retailers, credit card companies and many other organizations have seen their Web site graphics, including corporate logos and other materials “stolen” by fraudsters intent on tricking individuals into divulging personal financial information by responding to an official-looking, but entirely bogus, e-mail.

Like many cons and scams, phishing preys on the unwary. Here’s how credit union members can fight back against this fraud.

## TAKE SOME SIMPLE PRECAUTIONS.

- ✓ Never respond to an unsolicited e-mail that asks for personal financial information.
- ✓ Report anything suspicious to the proper authorities. Alert the credit union or government agency identified in the suspect

e-mail through a Web address or telephone number that you know is legitimate.

- ✓ Contact the Internet Crime Complaint Center at [www.ifccfbi.gov](http://www.ifccfbi.gov)—a partnership between the FBI and the National White Collar Crime Center—if you think you have received a phishing e-mail or have directed to a phishy-looking Web site.

## “STOP, LOOK AND CALL”

The Department of Justice advises e-mail users to “stop, look and call” if they receive a suspicious e-mail.

- ✓ **Stop.** Resist the urge to immediately respond to a suspicious e-mail—and to provide the information requested—despite urgent or exaggerated claims.
- ✓ **Look.** Read the text of the e-mail several times and ask yourself why the information requested would really be needed.
- ✓ **Call.** Telephone the organization identified, using a number that you know to be legitimate.

## IF YOU’VE BEEN “PHISHED...”

If you believe that you have provided sensitive financial information about yourself through a phishing scam, you should:

- ✓ Immediately contact those organizations for which you provided the information.
- ✓ Contact the three major credit bureaus and request that a fraud alert be placed on your

credit report. The credit bureaus and phone numbers are: Equifax, 1-800-525-6285; Experian, 1-888-397-3742; and TransUnion, 1-800-680-7289.

- ✓ File a complaint with the Federal Trade Commission at [www.ftc.gov](http://www.ftc.gov) or 1-877-382-4357.

Credit union members should never provide their personal information in response to an unsolicited telephone call, fax, letter, e-mail or Internet advertisement.

The bottom line: **Don't get hooked by fraudulent phishing attempts.**



Presented by the National Association of Federal Credit Unions, an independent trade association representing federally chartered credit unions nationwide.

© 2004 FINANCIAL EDUCATION CORPORATION

**INTERNET FRAUD**

# Don't Get Phished

**Simple Precautions Can  
Keep You from Getting  
Hooked by Internet  
'Phishing' Scams**