Be Aware of Phishing and How It Works

Liberty Bay Credit Union will never request your personal or account information via e-mail or phone. If you believe you are a victim of fraud, please contact the credit union immediately at (617)439-6500.

Don't get hooked by scammers out 'phishing'!

Internet scammers casting about for people's financial information have a new way to lure unsuspecting victims: They go "phishing." Also called "carding," phishing is a high-tech scam that uses spam to deceive consumers into disclosing their credit card numbers, bank account information, Social Security numbers, passwords, and other sensitive information.

How it works

The scammers send you an e-mail that appears to be from a business you know. It could be your Internet service provider, online payment service, or credit union, for example. The e-mail says you need to "update" or "validate" your billing information to keep your account active. You are directed to a "look-alike" web site of the legitimate business, further tricking you into thinking you are responding to a valid request.
Unknowingly, you would end up submitting your financial information to the scammers, who would then use it to order goods and services and potentially obtain credit — in your name.

Be aware

The Federal Trade Commission (FTC) urges you to take the following precautions to avoid getting hooked by a phishing scam:

- If you get an e-mail that warns you, with little or no notice, that an account of yours will be shut down unless you reconfirm your billing information, do not reply or click on the link in the e-mail. Instead, contact the company cited in the e-mail, using a telephone number or web site address you know to be genuine.
- Avoid e-mailing personal and financial information. Before submitting financial information through a web site, look for the "lock" icon on the browser's status bar. It signals that your information is secure during transmission.
- 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.

- Report suspicious activity to the Federal Trade Commission. Send the actual spam to uce@ftc.gov. If you believe you've been scammed, file your complaint at www.ftc.gov, and then visit the FTC's Identity Theft web site, www.ftc.gov/idtheft to learn how to minimize your risk of damage from identity theft.

Visit www.ftc.gov/spam to learn other ways to avoid e-mail scams and deal with deceptive spam.