

How Not To Get Hooked by a “Phishing” Scam

Dear Matanuska Valley Federal Credit Union Customer, _____

At Matanuska Valley Federal Credit Union, the highest interest to our customers is the safekeeping of confidential information you have entrusted to us and using it in a secure manner. A fundamental element of safeguarding your confidential information is to provide protection against unauthorized access or use of this information. We maintain physical, electronic and procedural safeguards that comply with federal guidelines to guard your nonpublic personal information against unauthorized access.

At this time we need you to confirm your e-mail address with our existing database. As soon as our database will be updated we need to make few important announcements to our customers so please update your contact information with no delay.

<https://www.mvfcuonline.org/cgi-bin/mcw000.cgi?MCWSTART>

Our database will be instantly updated.

We are committed to the secure use and protection of customer information on our website. If you have any questions regarding our services, please check the website or call our customer service.

Best Regards,
Matanuska Valley Federal Credit Union Online Department.

Have you received email with a similar message above (actual email “phish”)? It’s a scam called “phishing” — and it involves Internet fraudsters who send spam or pop-up messages to lure personal information (credit card numbers, bank account information, Social Security number, passwords, or other sensitive information) from unsuspecting victims.

Phishers send an email or pop-up message that claims to be from MVFCU or, a business or organization that you may deal with - for example, an Internet service provider (ISP), bank, online payment service, or even a government agency. The message may ask you to “update,” “validate,” or “confirm” your MVFCU account information. Some phishing emails threaten a dire consequence if you don’t respond. The messages direct you to a website that looks just like a legitimate organization’s site. But it isn’t. It’s a bogus site whose sole purpose is 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.

MVFCU doesn’t have customers; we have members and always refer to you as such.

MVFCU doesn’t need to confirm, nor will we ever ask you to confirm personal financial information via an email.

Never, ever click a link on any email message that asks for your personal financial information. The link is usually typed correctly, but the actual hyperlink will take you to a “bogus” website.

Phishing is a scam where fraudsters call, send spam or pop-up messages to lure personal and financial information from unsuspecting victims. To avoid getting hooked:

- Don’t reply to **phone calls**, email or pop-up messages that ask for personal or financial information, and don’t click on links in an email message. Don’t cut and paste a link from the message into your Web browser - phishers can make links look like they go one place, but that actually send you to a different site.

- If you are concerned about your account, contact the organization using a phone number you know to be genuine, or open a new Internet browser session and type in the company’s correct Web address yourself.

- Use anti-virus software and a firewall, and keep them up to date.

- Don’t email personal or financial information.

- Review credit card and bank 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.

- Forward spam that is phishing for information to: **spam@uce.gov** and to the company, bank, or organization 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: **www.consumer.gov/idtheft**.

How To Spot A Rotten “Phish”



The best anti-fraud device for your computer or telephone is FREE and is sitting on top of your shoulders!

See tips and examples inside.



Building Better Financial Futures Since 1948!
745-4891 • www.mvfcu.coop • 694-4891