Quaker Oats Credit Union

Protect Yourself From Phishing Scams

QUICK LINKS

[Contact Us](#)
[Loan Rates](#)
[Loan App.](#)
[Up Coming Events](#)

Mobile Banking Is Here!

Download the QO Mobile App NOW!

ANDROID APP ON Google play

Available on the App Store

Want to stay up-to-date on the latest news and information about YOUR credit union?

Like us on Facebook

Join Our Mailing List

We've all come across a phishing email that appeared to be legitimate. Phishers take advantage of the fact that it's difficult to know with absolute certainty whom you're communicating with via email. They use this uncertainty to pose as legitimate businesses, organizations or individuals and gain our trust, which they can leverage to convince us to willingly give up information or click on malicious links or attachments.

Be aware of phishing scams

1) Use a spam filter

Your email provider should provide this spam filter. Keep all of your systems patched and keep your anti-virus software up-to-date.

2) Be vigilant

Watch for any of these telltale signs of a potential phishing email or message:

- Messages from companies you don't have accounts with
- Spelling mistakes
- Generic greetings (such as "Dear user" instead of your name)
- Unexpected messages with a sense of urgency, designed to prompt you to respond quickly without checking the facts
- Attachments with names such as "Resume" or "Unpaid Invoice"

3) Consider these recommendations

- Be suspicious of unsolicited emails, text messages and telephone calls. Never provide sensitive personal information via phone or email.
- If you want to verify a suspicious email, contact the organization directly with a known telephone number. Don't call the number provided in the email. Or, have the company send you something through U.S. mail

(which scammers won't).

- Only open an email attachment if you're expecting it and know what it contains.
- Visit websites by typing the web address into your browser's address bar. Don't follow links embedded in an unsolicited email.
- Use discretion when posting personal information on social media. This information is a treasure-trove to spear phishers who will use it to feign trustworthiness.
- Keep your anti-virus software up-to-date to detect and disable malicious programs, such as spyware or backdoor Trojans, which may be included in phishing emails.
- Know that we will never email, call or text you requesting your member number or passwords. We have everything we need to communicate with you.

If you ever suspect you may have become a victim of financial fraud or identity theft, please contact us immediately! There are several steps we can take to immediately assist you in protecting your accounts.

Source: www.shazam.net