

Don't get reeled in by 'phishing' scams

Do these messages sound familiar?

- *We could not verify your account information. Click here to update and verify your information.*
- *We have detected unauthorized transactions on your account. Click below to confirm your identity.*
- *Your billing information is outdated. Please follow the link below to update your billing information.*

The above messages are common tactics used in phishing scams. Phishing is a type of electronic fraud used to obtain personal information from its victims.

Here's how the scam works

'Phishers' send a mass e-mail to their targets, masquerading as a trusted business or organization. Credit unions, banks, online payment services and Internet service providers are institutions commonly imitated in phishing scams. In the e-mails, phishers request personal information from their targets, such as credit card numbers, bank account information, social security numbers and passwords. The e-mails often contain a link to what appears to be an official webpage of the organization, asking the target to disclose sensitive material. Victims of phishing may then become victims of identity theft.

The Federal Trade Commission offers these tips to avoid phishing scams:

- If you get an e-mail or pop-up message that asks for personal or financial information, do not reply or even click on the message. Legitimate companies will never ask for this information via e-mail.
- Use anti-virus and anti-spyware software, as well as a firewall, and update them all regularly.
- 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 e-mails you receive, regardless of who sent them. These files can contain viruses or other software that can weaken your computer's security.

If you have received an e-mail that is 'phishing for information,' forward it to spam@uce.gov and the company impersonated in the e-mail. If you have received an e-mail impersonating Northern Federal Credit Union, please forward the e-mail to marketingdept@northernfcu.com. You can also file a complaint at the Federal Trade Commission's website, www.ftc.gov.

Watertown (Downtown)

120 Factory Street
Watertown, NY 13601
(315) 782-0155

Watertown

1180 E. Commerce Drive
Watertown, NY 13601
(315) 785-5600

Adams

10924 US Route 11
Adams, NY 13605
(315) 232-2990

Gouverneur

145 East Main Street
Gouverneur, NY 13642
(315) 287-0356

Lowville

5801 Number 4 Road
Lowville, NY 13367
(315) 376-7303