

## Phishing Quick Guide

### Definitions and How to Protect Yourself

#### Overview

Banks and credit unions are experiencing an increased number of phish email attacks. Phish attacks request the email recipient to link to a phony website and submit personal account information. Elevations Credit Union has reports of phishing emails and websites and is working to shut these sites down.

#### Definitions

**Phishing (fish'ing) (n.) Also known as "Spoofing"** – The act of sending an email in an attempt to get the recipient to visit a fraudulent website and enter sensitive personal information. Phish emails and websites try to fool the recipient by mimicking a legitimate business. Any information collected by the phisher is then used to steal the recipient's money or identity.

**Sensitive personal information** - Any information about an individual that can be used to verify their personal financial information or identity. This includes: Social Security Number (SSN), credit card, account or PIN numbers, usernames and passwords, birthdates, passport and visa documentation.

#### Phish emails typically:

- Copy a legitimate company's logos and graphics
- Appear to come from a legitimate business (Example from an email: "From: [service@elevationscu.com](mailto:service@elevationscu.com)")
- Include a generic greeting or subject (Example: "Dear Elevations Credit Union Member", "Dear Member" or "Important Information About Your Account")
- Have an urgent tone for quick action (Example: "Ignoring this message will result in a suspension of your account within 24 hours")
- Contain links that resemble the Credit Union's web address (Example: <http://bank-uofcfcuonline.com/>)
- Contain links that appear to be legitimate in the email, but go to a fraudulent phish website. This type of link is called a "masked" or "embedded" link (Example: "Please visit <http://www.uofcfcu.com/security>" - this link actual goes to a fraudulent website address such as "<http://uofccu-security.com/>" or "[http://202.52.132.5:82/www.uofcfcu.com/secure/forms/link24\\_locked\\_out.cfm](http://202.52.132.5:82/www.uofcfcu.com/secure/forms/link24_locked_out.cfm)" )
- Depend on the recipient taking action by clicking on a masked link and entering sensitive personal information into the fraudulent website.

#### To ensure the protection of your sensitive personal information:

- 1) **Be cautious.** YOU control the information you give out. Be careful when searching the internet and don't give out any information if you can't verify or trust the source.
- 2) **Be aware.** Always verify the addresses of websites where you do business. The only website address you should use to login to our Link24 Online Banking site is: <https://www.ElevationsCU.com>. Only send sensitive personal information on an encrypted, secure website that you trust. Secure websites show a padlock symbol on the bottom right of the browser to verify the security and authenticity of the site.
- 3) **Be proactive.** If you have clicked on a link in a phish email, it does not mean you have a virus or have compromised your sensitive personal information. However, if you **entered any sensitive personal information into a suspicious website**, contact the legitimate business immediately.
- 4) **Know that we're here for you.** You can contact us directly at 303.443.4672 if you are suspicious about any request for sensitive personal information appearing to come from Elevations Credit Union. Please report any suspicious emails or security questions to [security@ElevationsCU.com](mailto:security@ElevationsCU.com).

For more questions on security please visit: <http://www.ElevationsCU.com/security/>

#### Note about Elevations Credit Union's Email Messaging

Elevations Credit Union will never ask you for any sensitive personal information including any account information or social security number via email. Email is a responsible way to deliver relevant product and service offers, regulatory information and rate updates, **NOT** to gather confidential member information. For more questions please visit: <http://www.ElevationsCU.com/emailmessaging>