

New twist on how Phishers continue to Phish Credit Union members (posted 7/14/06)

Phishers seek every opportunity to find individuals who are willing to provide information for the criminals to tap into a financial gain. Once you provide the personal and/or financial information, the fraudsters are off and running.

The phishers continue to change their phony e-mails by including false fraud protection techniques as a new twist to convince you the e-mail is from your credit union. Because of everyone's fraud awareness, the phishers lure you to "take action" and provide the information by using an "online banking" log-in which will re-direct this site to the fraudster.

The "take action" the phishers are asking you to perform is:

- Deactivate your card(s) temporarily to guard against fraud.
- Activate your card(s) by having them log on to an "online banking system" where phishers are able to obtain your card information.
- The phishers convince you there is no need to contact your credit union to validate the e-mail or telephone request involving the deactivation and activation process.

Please do not reply to these e-mails. Contact the credit union or see our Loss Prevention Recommendations on the Scam Alert page of our website.