

## ALERT: BEWARE OF PHISHING!

The number and sophistication of phishing scams sent out to consumers is continuing to increase dramatically. Phishing steals consumers' personal identity data and financial account credentials. Phishing can use 'spoofed' e-mails to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as credit card numbers, account usernames, passwords and social security numbers. Hijacking brand names of banks, e-retailers and credit card companies, phishers often convince recipients to respond. Phishing schemes can also plant **crimeware** onto PCs to steal credentials.

While online banking and e-commerce is very safe, as a general rule you should be careful about giving out your personal financial information over the Internet. Following is a list of recommendations below that you can use to avoid becoming a victim of these scams:

- Be suspicious of emails with urgent requests for personal and financial information.
- Avoid filling out forms in email messages that ask for personal financial information. Most phishing attacks ask for unique pieces of information (user accounts, social security numbers, pin numbers, credit card numbers, etc.).
- Don't use the links in an email to get to any web page if you suspect the message might not be authentic.
- The general tone of phishing e-mails will be upsetting or exciting to the recipient in an attempt to get them to react immediately.
- Always ensure that you're using a secure website when submitting credit card or other sensitive information via your Web browser.

Remember that Hannaford Associates Federal Credit Union will either contact you by mail or phone regarding your account and *not* via e-mail in the event a situation occurs that requires their immediate attention where sensitive information is required. If you have any question about an e-mail you receive, your best bet is to contact the company regarding the e-mail sent. Make sure to call a number that is NOT on the e-mail – find an alternate number in the phonebook or online. If you feel you have received a fraudulent e-mail you can forward the email to [reportphishing@antiphishing.com](mailto:reportphishing@antiphishing.com) or notify the Internet Fraud Complaint Center of the FBI by filing a complaint on their website: [www.ifccfbi.gov/](http://www.ifccfbi.gov/). If you have any questions regarding phishing – please feel free to contact the credit union at 1.800.852.1012 option 5.