WESLA FEDERAL CREDIT UNION

## WHAT IS..

- **VISHING** - Fraudulent practice of making phone calls or leaving voice messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as bank details and credit card numbers.
- **SMISHING** - Short for SMS Phishing, smishing is a variant of phishing email scams that instead utilizes Short Message Service (SMS) systems to send bogus text messages.
- **PHISHING SCAMS**- lure account holders into providing personal or financial information to scammers posing as a legitimate business. Most phishing scams are conducted through email, with messages containing links that ask for your personal data or download spyware to your computer or mobile device. Other phishing scams are conducted by phone call, text messages and social media. Navy Federal will never solicit your personal information via phone or email.

## Don't Be A Victim!!

The number and sophistication of phishing scams sent out to consumers is continuing to increase dramatically. 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. The Anti-Phishing Working Group has compiled a list of recommendations below that you can use to avoid becoming a victim of these scams.

- Be suspicious of any email with urgent requests for personal financial information!
- Phishers typically include upsetting or exciting (but false) statements in their emails to get people to react immediately
- They typically ask for information such as usernames, passwords, account numbers, credit card numbers, social security numbers, etc.
- Phisher emails are typically NOT personalized, while valid messages from your bank or e-commerce company generally are
- Don't use the links in an email to get to any web page if you suspect the message might not be authentic. Instead, call the company on the telephone, or log onto the website directly by typing in the web address in your browser.
- Avoid filling out forms in email messages that ask for personal financial information. You should only communicate personal information (such as credit card numbers, PIN number, social security numbers, or account information) over the telephone or via a secure website. When submitting credit card or other sensitive information via your web browser, always ensure that you're using a secure website.
-

WESLA FEDERAL CREDIT UNION

- Regularly log into your online accounts – don't leave it for as long as a month before you check each account.
- Regularly check your bank, credit and debit card statements to ensure that all transactions are legitimate. If anything is suspicious, contact your financial institution and all card issuers.
- Always report 'phishing' or 'spoofed' e-mails to the following groups:
    - Forward the email to the Federal Trade Commission at spam@uce.gov.
    - Forward the email to the "abuse" email address at the company that is being spoofed.
    - When forwarding spoofed messages, always include the entire original email with its original header information intact

- **IDENTITY THEFT** – Identity theft is a crime in which an imposter obtains key pieces of personal information, such as Social Security or driver's license numbers, in order to impersonate someone else. The information can be used to obtain credit, merchandise, and services in the name of the victim, or to provide the thief with false credentials. In addition to running up debt, an imposter might provide false identification to police, creating a criminal record or leaving outstanding arrest warrants for the person whose identity has been stolen.
- **SKIMMING-** Skimming is a huge problem for financial institutions and its members in the United States. It involves stealing the magnetic strip information off a members debit card and using a hidden camera to gather their PIN number information. The information is then used to make a duplicate debit card. In 2012 alone, criminals were able to use these cards and steal 11.3 billion dollars.

With the advent of EMV chips, criminals are aware that the switch to the more secure card is coming in October of 2015, and are in turn trying to commit as much fraud as they can before that. Because of this, both the member and the financial institutions have to take extra precautions when using ATMs.

In an effort to keep you informed, we have a few tips of what you can look for when using your debit/ATM card.

- Look for changes in the ATM or card reader -extra plastic -bulkier card reader -any pieces that weren't present before - changes in the card reading method
- Look for changes in the keypad look and feel.
- Make sure to look around for any cameras place in a position where your hand can be seen in putting your PIN number. They can be very small or placed in pieces of plastic.
- If you suspect a skimmer is being used, contact the financial institution that owns the ATM or the local police department.
- With your heightened awareness, you are not only helping yourself, but you are helping financial institutions fight fraud all over the country.