NORTH COAST
CREDIT UNION

SECURITY TIPS

We take your security very seriously. We use leading edge technology to ensure that your information stays safe. This goes for every system regardless of how you do your banking. Online, Mobile, by Phone or In Branch, your security is our first priority. If you have any concerns about the security of your accounts or your debit/credit cards please call us at 1-800-696-8830, or after hours send an email through our Member Service Contact Center.

First and foremost keep your account information private. If anyone asks for this information respond with a big **NO WAY!**

Never send your account information including member number and password via email. **We will NEVER ask you to do this.**

Never give your password to anyone. **We will NEVER ask for it even when we are speaking with you directly.**

REDUCE YOUR SECURITY RISKS

Switch to strong passwords. It’s worth your time to update all you passwords to contain upper and lower case letters, numbers and symbols. Avoid recognizable identifiers
such as the last four digits of your SSN, your birth date, house number and so on for passwords and PINs.

Refuse requests for personal information. Decline phone and e-mail requests for personal information for your debit/credit card number. They may be scams. If someone calls asking for this information let us know immediately. If you receive an e-mail requesting this information forward to us at our Member Service Contact Center.

We may call you to verify suspicious activity on your debit/credit card. This is a part of our fraud monitoring on your behalf. We will ask you if the suspicious charge is valid.

Traveling outside the US? Please let us know if you plan on traveling. If we know the travel dates and destinations we can make the necessary adjustments to ensure you are not negatively impacted by our fraud monitoring system on your trip. Contact us by calling Member Services at 1-800-696-8830 or stop by your neighborhood branch.

You may receive occasional email from us. Member Bonus emails will include information about special services and products available to our members. If you are suspicious about any email from North Coast call our Member Service Contact Center to verify at 1-800-696-8830.

SECURITY TIPS continued

Protect yourself when banking online. Don't access your account from computers/ devices that are not secure. Be cautious when using public Wi-Fi. Lock your phone, tablet or other web device when you are not using it. Log off when you have finished your online banking.

Keep your firewall/virus protection turned on. A firewall and virus protection helps protect your computer from hackers looking for your personal information. When used correctly, a firewall prevents unauthorized use of and access to your personal information. While firewalls are not perfect protection, they will help to keep your computer safer when you to access the Internet. You will get the best protection if you keep your firewalls and operating system updated.

BE ALERT FOR THESE WARNING SIGNS:

Missing bills or statements:

Be aware if you did not receive your bill or statement as expected in the mail. Many members have moved to eStatements and online Bill Pay to avoid this security threat.

Unexpected charges on your debit/ credit card:

You can check your North Coast Debit/ Credit Card statement daily through Online Banking.

Collection calls or denied credit: Check your credit report immediately if this occurs.

If you suspect fraud or your checks have been stolen contact us immediately by calling our Member Service Center at 1-800-696-8830 or send us an email through our Member Service Contact Center or visit your neighborhood branch.

ONLINE THREATS

Unfortunately as our technology advances so do the methods criminals use to capture your information. By becoming aware of the way criminal attempt to get you information you will be better prepared to spot a scam. Here are some of the ways identity online thieves commit their crimes:

Phishers (pronounced "fishers") create and use emails and websites designed to look like those of legitimate businesses to deceive users into disclosing information. Fraudulent email is designed to get you to click on a link. Clicking on the link may download malware onto your computer or lead you to a fraudulent website.

SECURITY TIPS continued

Misspelled words and bad grammar can indicate a fraudulent e mail. Fake email messages are usually not personalized. Often fraudulent e mails will try to scare you into responding by claiming your account will be closed if you don't respond with personal information immediately. Never include any information in an email that you wouldn't write on a postcard.

To check if a website is legitimate check for the "s". Often, the link to a fraudulent website will have an "s" at the end of it. For example northcoastcu**s**.com. If a website is not familiar to you never click on the link.

Smishers phish via cell phone text messages. The message typically alerts the user of a need for immediate action with a link to a phone site. Instead of replying to these messages or following links, contact the organization directly.

Vishers will reach out to you directly by phone. Vishers can spoof caller ID to make it look like a call is actually originating from North Coast. Remember we will never call and ask you for your account number, PIN numbers or any confidential information. Some Vishers will ask you to go to your computer and log into their website. Hang up on these people.

Pharmers secretly install (or plant) a malicious program in your computer to hijack your web browser. Pharming crimeware misdirects users to fraudulent sites and captures what you enter, such as passwords or account information. To help avoid these turn on your firewall/virus protection, accept security patch updates on your computer.