During these uncertain times, we want to remind our members to remain vigilant when receiving phone calls, emails and text messages. Unfortunately, scammers and fraudsters are using COVID-19 to their advantage by using fear as their tactic to steal personal and private information. Financial institutions nationwide have reported that in some cases, scammers are calling their customers/members and impersonating the Centers for Disease Control (CDC). During the call, the fraudsters are asking people to verify their personal information, including social security numbers and account passwords.

While no Salem VA Credit Union members have indicated they have been recently scammed as a result of the COVID-19 pandemic, we wanted to share with you the below article written by the Credit Union National Association (CUNA) which shares other credit union warnings and experiences.

Please remember, we will never call you and ask for your account number, social security number, or passwords over the phone. If the caller or person on the other end of the email is asking for such information, please call us directly at 540.344.4419 or email us at info@salemvafcu.org.

Shielding members from COVID-19 fraud

Fraudsters use a variety of tactics to exploit fears about the coronavirus.

March 13, 2020 | Ron Jooss

Fraudsters are leveraging fears over the coronavirus as an opportunity to scam financial institutions and consumers. Credit unions are taking steps to warn and protect their members.

Wright-Patt Credit Union, Beavercreek, Ohio, yesterday alerted members to watch out for scammers who are taking advantage of concerns over COVID-19.

Fraudsters are posing as the CDC Health Alert Network to steal personal information, according to an email Wright-Patt sent to its members.

Sidney (N.Y.) Federal Credit Union also is sounding warnings about a scam where members receive phone calls and text messages that appear to be from the credit union asking for personal and online banking information.

In a message on its Facebook page, the credit union tells members not to reply to these messages because caller ID can be "spoofed" and isn't a reliable way to identify a caller.

City of Boston Credit Union posted a message on its website that hackers and scammers are using the potential public health crisis to take advantage of unsuspecting businesses and consumers.

The message explains that fraudulent emails have surfaced claiming to be from the Center of Disease Control and Prevention (CDC) and the World Health Organization (WHO), directing unsuspecting recipients to harmful websites that load malware or other harmful applications under the ruse of offering important pandemic information.

In response to these and other campaigns, WHO and CDC have issued alert warnings to consumers to be on the lookout for individuals posing as the organizations.

“The best practice in avoiding scams and hackers is to not click on any links in emails you were not expecting or you did not request,” the message says. “Just delete the email.”

Opportunistic hackers are employing other tactics to take advantage of consumers.

One of the phony maps fraudsters use is Corona-Virus-Map.com, according to PaymentSource. This website claims to provide an up-to-date coronavirus map similar to another map from Johns Hopkins University.

The malicious website produces a map that nearly matches the university’s graphics. The fraudulent map contains software that steals usernames, passwords, credit card numbers and other data stored in the user’s browser.

The Corona-Virus-Map.com Trojan is distributed through infected email attachments, malicious online ads, social engineering, and software vulnerabilities, according to PCRisk.com.

Fraudsters also target consumers through a more common tactic: phishing email attacks.

Phishing emails will use the virus as a lure in the subject line. The email’s text may contain false news about the COVID-19.

Some emails claim to be from CDC or WHO, and others offer a link to coronavirus map of the recipient’s neighborhood, or an update on how many people have been infected.

The emails attempt to trick users into enter personal information or click on a link that will download malware on user’s computer.

Wright-Patt Credit Union offers members this advice to protect themselves from scanners:

- Use only reputable sources when searching for information about the coronavirus.
- Be aware of phishing emails and never click unknown attachments or links.
- Be cautious of emails and phone calls offering unexpected information and asking for personal information.

Pacific Northwest Credit Union, Portland, Ore., posted Fraud & Scam Resources for members on its website.

CUNA is following developments of the coronavirus disease and will provide updates as information and materials become available.