Cybersecurity Reminders

STAY SECURE. STAY SAFE.

PENFED CREDIT UNION

Scammers will use anything as an opportunity to get you!

The COVID-19 (Coronavirus) has affected the lives of millions of people worldwide. Heartless scammers are using this event as another means for getting at you. The scammer's main tool is to play upon the fear and uncertainty that exists within our lives. Coronavirus is no exception.

Cybercriminals are sending emails claiming to be from legitimate organizations, such as PenFed, with information regarding coronavirus. Some of these emails contain attachments; supposed "statistics" on the virus in your area. Some contain other attachments or links. If you click on them, you are likely to download malicious software (malware) onto your device.

The malware could do any number of things from giving remote control of your device to the cybercriminal, to logging your keystrokes, capturing user IDs and passwords, to accessing your personal information, which could lead to identity theft.

How Can I Protect Myself?

- The Center for Disease Control (CDC) or the World Health Organization (WHO) are NOT going to email you information! If you want information, go directly to their web sites.
- If you do get an email, look for typos, misspellings, missing logos, poor quality graphics – Be critical of your review. Real organizations take pains to make their online and email appearances look professional.
- The email will often try to create a sense of urgency – "Buy now, limited supply!" or "click here for information on how to get the cure". Avoid these "Act Now" emails.
- When purchasing items, be sure the web site is secure (look for the lock or HTTPS in the address line. The "S" in HTTPS stands for secure).
- If you think the email is legitimate, and want more information, do NOT use the links provided. Always go to the web site by typing in the address (for example https://cdc.gov). If it is legitimate, the information mentioned in the email can be found on the website without the use of a link.
- Beware of requests for personal information – legitimate government agencies will not ask you for this information.

And Another Thing…

There are groups of these scammers that have taken their tactics out of cyberspace into the real world. They are vishing (phishing via a telephone) folks by impersonating the CDC or other health institutions. Further, other folks are actually going door-to-door.

Protect yourself by:

Phone:

- Understanding that government agencies are NOT going to call you.
- If in doubt, get their name and the name of the agency/organization that they claim to represent. Hang up. Then look them up on line. If it was a legitimate visit, call the organization using a number from their website directly to ask for the information.

At Home:

- Just like the phones, government agencies are NOT going to pay you a visit at home. Do NOT let these folks into your homes.
- Ask for ID.
- Ask for their supervisor's name to contact to "confirm" the visit.
- Again, never call a number that is provided to you, always look them up yourself.
- In any case, never provide personal information!