



April 27th, 2020

COVID-19 Fraud Updates

Dear Members,

The FBI is seeing a rise in COVID-19 fraud schemes. A recent FBI alert warns consumers and businesses about coronavirus related schemes to steal money and personal information. We want to remind our members, that nw+|cu will *never* request that you provide us with your personal information. Please be aware that there are a lot of scams going on right now, with the fraudsters trying to take advantage of everyone during these difficult times.

Do not provide the following to anyone that is contacting you:

- Date of Birth
- Social Security Number(s)
- Passwords or PIN numbers
- Mother's Maiden Name
- Zip Code
- Access to login information
- Remote access to devices

NOW is the best time to start using nw+|cu services:

- eStatements
- Billpay
- Personal Branch
- Remote Deposit Capture (RDC)

The FBI has cited three of the most prevalent scams and how to avoid them:

1. Fake CDC emails

Watch out for emails claiming to be from the Centers for Disease Control and Prevention (CDC) or other organizations offering information about the virus.

Don't click links or open attachments you do not recognize. Fraudsters can use links in emails to deliver malware to your computer to steal personal information or to lock your computer and demand payment.



April 27th, 2020

Be wary of websites and apps claiming to track COVID-19 cases worldwide. Criminals are using malicious websites to infect and lock devices until they receive payment.

2. Phishing emails

Beware phishing emails asking you to verify your personal information to receive an economic stimulus check from the government. Government agencies are not sending unsolicited emails seeking your private information to send you money.

Phishing emails may also claim to be related to charitable contributions, general financial relief, airline carrier refunds, fake cures and vaccines, and fake testing kits.

3. Counterfeit treatments or equipment

Be cautious of anyone selling products that claim to prevent, treat, diagnose, or cure COVID-19. Be alert to counterfeit products such as sanitizing products and personal protective equipment (PPE), including N95 respirator masks, goggles, full-face shields, protective gowns, and gloves.

Visit [cdc.gov/niosh](https://www.cdc.gov/niosh) for more information about unapproved or counterfeit PPE. Information also is available from the U.S. Food and Drug Administration and the Environmental Protection Agency.

The FBI advises several ways to practice good “cyber hygiene” and security measures:

Don't open attachments or click links within emails from senders you don't recognize.

Don't provide your username, password, date of birth, social security number, financial data, or other personal information in response to an email or robocall.

Verify web addresses of legitimate websites and manually type them into your browser.

Check for misspellings or wrong domains within a link (i.e., an address that should end in .gov ends in .com instead).