COVID-19 Virus Scams

March 2020 Update
from
Downeast Credit Union
Internal Operations

Scammers don’t take a break during a global pandemic…….

Instead they actually RAMP UP their efforts to take advantage of others!!

COVID-19 SCAMS TO WATCH FOR

Unsolicited COVID-19 Testing

This scam includes folks coming to your home, calling or emailing you, claiming to be able to test you for the virus.

They will take your money, even swab you for a test sample and never provide you with results.

If interested in having outside testing done, check with the CDC for valid/approved testing options.

Fraudsters are also looking to “hire” people to conduct the Door-To-Door swabbing – this is not a legit job.

COVID-19 Sanitization

This scam involves people coming to your door, calling or emailing you, claiming they can sanitize your living space or the air in your home to kill off all COVID-19 germs for a “small” fee.

Unsolicited Personal Shoppers

This scam involves people coming to your door or even offering via social media, calls or emails to come and get your money to go out into the public to get the supplies you need.

If you do not know this person, do not give them your money.

What is happening is the victims are left without their necessary supplies and no money to get what they still need.

COVID-19 SCAMS TO WATCH FOR

Fake Media Ads for Unapproved COVID-19 Treatments

There is currently NO CURE for COVID-19.

Often, these folks will state they can treat, cure or give medical advice.

After asking some questions and/or collecting a fee, the scammers can use your personal information provided, including your insurance information, to conduct additional fraud.

All treatment should be provided by your qualified medical team.

Fake Charities

This scam involves collecting donations for people affected by COVID-19.

In reality, the scammers are pocketing the funds.

Do your research before donating: be sure this is a legitimate organization!

Contact with someone carrying COVID-19

There is contact made, claiming you have been in contact with someone with COVID-19.

Some of these calls are made just to scare you, other times it is to sell you an “in-home kit” to be tested for the virus or to sell you a “cure”.

There is currently no in-home testing method approved for COVID-19.

Also, silver, bleach, garlic or bananas will not prevent COVID-19.

COVID-19 SCAMS TO WATCH FOR

Senior “Care Package” or Medical Supply Scams

There are folks that are offering to sell “Senior Care Packages” that include hand sanitizer and even in some instances a purported vaccine, which does not exist.

There have also been reports of people “selling” highly sought after medical supplies such as hand sanitizer, toilet paper or masks that never arrive after placing an order.

World Health Organization/CDC Imposters

There are folks sending malicious emails appearing to come from the W.H.O. or the CDC asking for sensitive information. They also may prompt users to click on suspicious links or open malicious attachments.

This gives access to your computers to obtain information or damage your computer.

Fake COVID-19 “Relief” Checks

This scam includes fraudsters posing as financial institution employees, government officials or health service provides to persuade victims to hand over their sensitive information, including their account numbers or online banking log-in information.

Legitimate sources would never reach out to request this information.

COVID-19 SCAMS TO WATCH FOR

“Frozen Account Scam”

This scam includes being contacted and informed that your assets have been “frozen” due to the COVID-19 outbreak.

This scam can involve the victim giving out personal information to have the funds “moved” to a safe place, including foreign wires.

Or, they may ask for sensitive information to “release” the funds once they “verify” your identity, when really they are stealing your information for personal gain.

FDIC/NCUA Scams

This scam involves being contacted by someone from “NCUA” or “FDIC” claiming that the person’s financial institution is going under.

They urgently request the victim gives up all their information, stating the lending or deposit institution is about to collapse.

Investment Scams

Scammers are offering online promotions on various platforms, including social media, claiming that the products or services of publicly traded companies can prevent, detect, or cure COVID-19, and that the stock of these companies will dramatically increase in value as a result.

These promotions are often styled as “research reports,” make predictions of a specific “target price,” and relate to microcap stocks, or low-priced stocks issued by the smallest of companies with limited publicly available information.

COVID-19 SCAMS TO WATCH FOR

Insurance Provider Scams

This scam involves being contacted by your “insurance provider” and asking if you would like to purchase a kit or even obtain a “Free” testing kit.

The basis of this is for the fraudsters to obtain all your personal information by asking questions to provide your “free” testing kit which never actually arrives.

This *ALSO* could be someone fraudulently calling to sell you “insurance” and offer a policy, which is again is solely for obtaining your personal information.

Small Business Loan Scam

If you have a small business, you could get a call for financial relief (including loans or payment forgiveness) *OR* they may even request to verify that your information with Google is up-to date so your customers can find you.

They will ask all kinds of questions about your business and steal your information.

There could be “processing fees” involved as well.

Mortgage Forgiveness Scams

This call is where the victim is told that by answering some questions, they can be offered mortgage forgiveness *OR* even be offered a new mortgage as the rates are at an all time low!

There may be application fees that need to be paid, but more importantly, if you fall for this one-the scammers have all your personal information.

COVID-19 SCAMS TO WATCH FOR

Social Security Scam

This is a call that comes out to folks stating that due to the virus and/or fraudulent activity, their social security payments have been suspended.

This is likely not the case.

But, if you give them all your information, they will “reinstate” it for you.

Medical Provider Scams

This scam involves being contacted by phone or email by someone who claims to be a doctor or a hospital that has “treated” a family member or friend for COVID-19 and they demand payment for this “treatment”.

Providers will bill you for services rendered as necessary, they will not contact your friends and family.

App Scams

Scammers are even creating and manipulating mobile apps designed to track the spread of COVID-19 to insert malware that will compromise users’ devices and personal information.

SCAMMERS WANT YOUR INFORMATION!

Keep in mind, they are not ALWAYS *just* looking for your money!

Many can access that by obtaining your personal information, such as your date of birth, address, social security number, your Medicare or insurance numbers, your banking information, etc.

This information is then used later to conduct additional fraud.

To Report COVID-19 FRAUD

Call the National Center For Disaster Fraud Hotline

(866) 720-5721 or

disaster@leo.gov

AND/OR.....

To Report COVID-19 FRAUD

The FTC is looking for information on what trends are happening right now in fraud.

So....they made a fun Bingo game that they are asking folks to fill out and share with them what they are seeing! www.consumer.ftc.gov

FTC Scam Bingo

Want to help warn others about scams? Post on your social media (w/ #FTCScamBingo) and play with your friends. Want to let us know what's going on? **When you have bingo, share with the Federal Trade Commission on Facebook (@FederalTradeCommission) or Twitter (@FTC)!**

Got a robocall	Got a scam call	"Lower your interest rate"	"Problem with SSN"	"COVID-19 cure!"
"Treat COVID-19"	"Get COVID-19 test kit"	"Utilities problem"	Blocked a caller	Reported a scam
Fill in your own	"Lower your debt"	FREE SPACE	"Refi your mortgage"	"Forgive student loans"
Call from your own #	Call from similar #	COVID-19 phishing scam	"Get free gov't money"	"Get health insurance"
Call from "tech support"	Pressure to act NOW	Call from "Scam Likely"	Hung up on robocall	Fill in your own

Learn more about spotting and reporting scams at **consumer.ftc.gov**. Sign up for Consumer Alerts at **ftc.gov/subscribe**.

Federal Trade Commission

Content from various sources, including: https://www.justice.gov/usao-wdva/covid-19-fraud

Call your Downeast team at 800.427.1223 if you think you have been affected by a scam or fraud.

downeast

CREDIT UNION