Security focus

April 2, 2020

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

CORONAVIRUS SCAMS
INFORMATION AND TIPS FROM THE FTC

UNDELIVERED GOODS:
Online sellers claim they have in-demand products, like cleaning, household, and health and medical supplies. You place an order, but you never get your shipment. Anyone can set up shop online under almost any name — including scammers.

What to do:
Check out the seller by searching online for the person or company's name, phone number and email address, plus words like "review," "complaint" or "scam." If everything checks out, pay by credit card and keep a record of your transaction. If you're concerned about the pricing of products in your area, contact your state consumer protection officials. For a complete list of state Attorneys General, visit naag.org.

FAKE CHARITIES:
When a major health event — like the Coronavirus — happens, you might be looking for ways to help. Scammers use the same events to take advantage of your generosity. Some scammers use names that sound a lot like the names of real charities. This is one reason it pays to do some research before giving. Money lost to bogus charities means less donations to help those in need.

What to do:
Use the organizations at the provided link to help you research charities. When you give, pay safely by credit card — never by gift card or wire transfer.

Link: https://www.consumer.ftc.gov/features/how-donate-wisely-and-avoid-charity-scams

FAKE EMAILS, TEXTS AND PHISHING:
Scammers use fake emails or texts to get you to share valuable personal information — like account numbers, Social Security numbers, or your login IDs and passwords. They use your information to steal your money, your identity, or both. They also use phishing emails to get access to your computer or network. If you click on a link, they can install ransomware or other programs that can lock you out of your data. Scammers often use familiar company names or pretend to be someone you know. Other scammers have used real information to infect computers with malware. For example, malicious websites used the real Johns Hopkins University interactive dashboard of Coronavirus infections and deaths to spread password-stealing malware.

What to do:
Protect your computer by keeping your software up to date and by using security software, your cell phone by setting software to update automatically, your accounts by using multi-factor authentication, and your data by backing it up.

ROBOCALLS:
Scammers are using illegal robocalls to pitch everything from scam Coronavirus treatments to work-at-home schemes.

What to do:
Hang up. Don't press any numbers. The recording might say that pressing a number will let you speak to a live operator or remove you from their call list, but it might lead to more robocalls, instead.

MISINFORMATION AND RUMORS:
Scammers, and sometimes well-meaning people, share information that hasn't been verified.

What to do:
Before you pass on any messages, and certainly before you pay someone or share your personal information, do some fact checking by contacting trusted sources. For information related to the Coronavirus, visit *What the U.S. Government is Doing* at the provided link. There you'll find links to federal, state and local government agencies.

Link: https://www.usa.gov/coronavirus

For the complete FTC Article, visit:
https://www.consumer.ftc.gov/blog/2020/03/ftc-coronavirus-scams-part-2

TO LEARN MORE, VISIT:
Coronavirus Scams: What the FTC is Doing at: **https://www.ftc.gov/coronavirus**
Centers for Disease Control and Prevention at: **https://www.cdc.gov/coronavirus/2019-ncov/index.html**

MONTEREY COUNTY BANK
The Business Bank

Your BANK working for YOU
If you have any questions or concerns regarding your account (s), please contact your local Monterey County Bank branch for additional assistance. For branch hours and locations, please visit our *Contact Us* page on *www.montereycountybank.com*.