SYNOVUS®

COVID-19 Financial Fraud Awareness

April 2020

COVID-19 is driving its own fraud

There are specific scams that fraudsters are using to steal money and personal information during the pandemic.

Email

Spam email is the leading means of committing COVID-19 fraud at 94.9% as of April 8, 2020.[1]

- Includes fake CDC and WHO emails
- Stimulus check fraud

Spear-phishing emails, which target specific organizations or individuals, increased 667% since February 2020.[2]

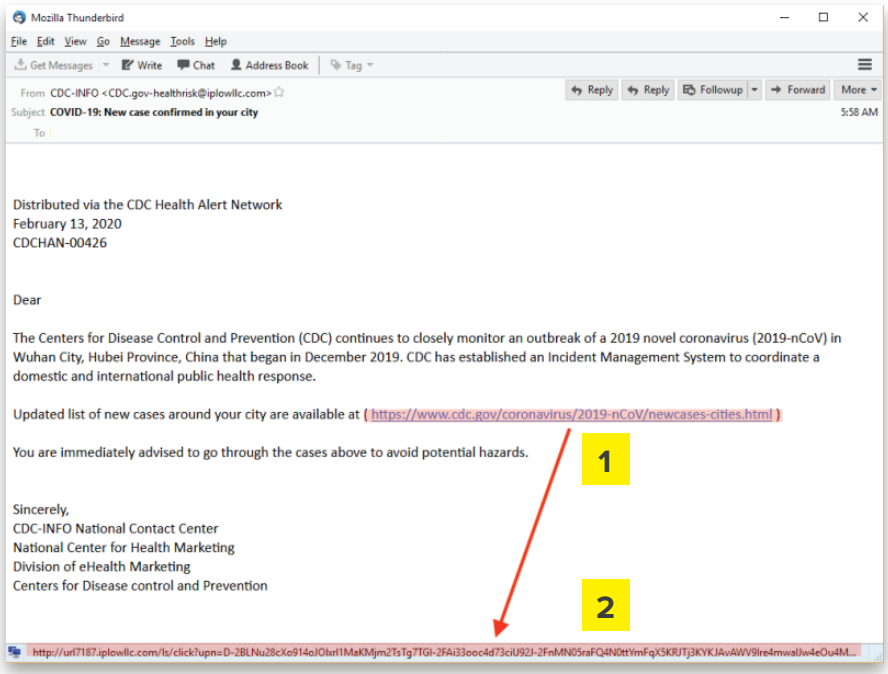
- There were 467,825 spear-phishing emails March 1–23.[2]
- Of those, 9,116 related to COVID-19 (2% of the attacks).[2]
- COVID-19 spear-phishing email themes include:[2]
  - Scamming (77%)
  - Brand impersonation (22%)
  - Business email (1%)

Sources:
(1) Trend Micro, "Developing Story: COVID-19 Used in Malicious Campaigns," Updated April 8, 2020
(2) Barracuda Networks, "Threat Spotlight: Coronavirus-Related Phishing," March 26, 2020

This email appears to be from the World Health Organization, but the numerous spelling and grammatical errors indicate it is a fake.

Source: Sophos Security, "Coronavirus "safety measures" email is a phishing scam," February 5, 2020

Examples of phishing emails

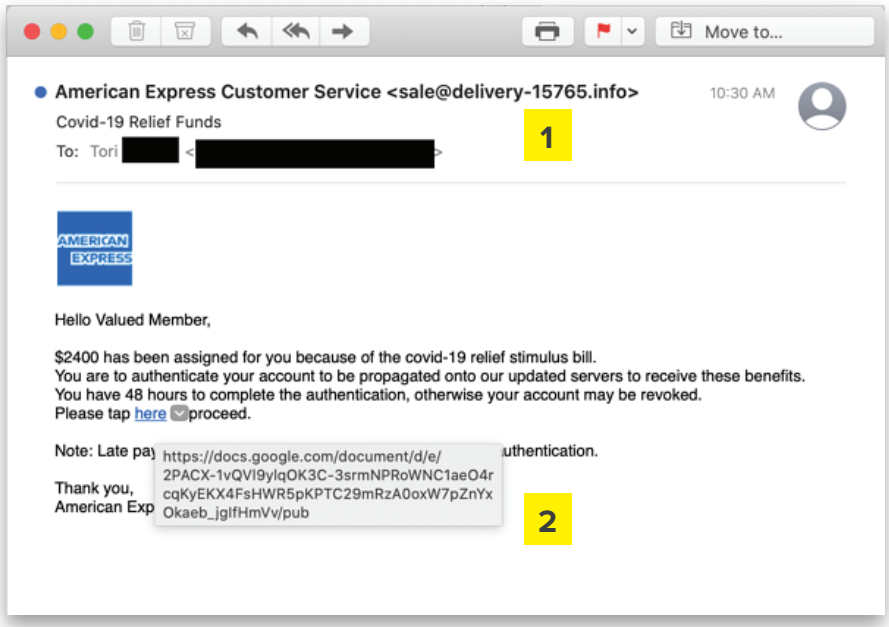


This is an example of phishing with malicious links.

1 The email body contains a URL that appears to display a legitimate link to the CDC's website.

2 When hovering over the link, however, the actual link to a scammer's website appears.

Source: Business Insider, "Email Scammers are Taking Advantage of Coronavirus Fears to Impersonate Health Officials and Trick People into Giving up Personal Information," March 9, 2020



This example uses the CARES Act stimulus as bait.

1 This example appears to be from American Express, but a check of the sender's email address reveals it is not.

2 Hovering over the link in the body of the message reveals a link to a Google Docs file that is likely to be malicious.

Source: KnowBe4, "They're Here! COVID-19 Stimulus Check Phishes Finally Arrive," April 2, 2020

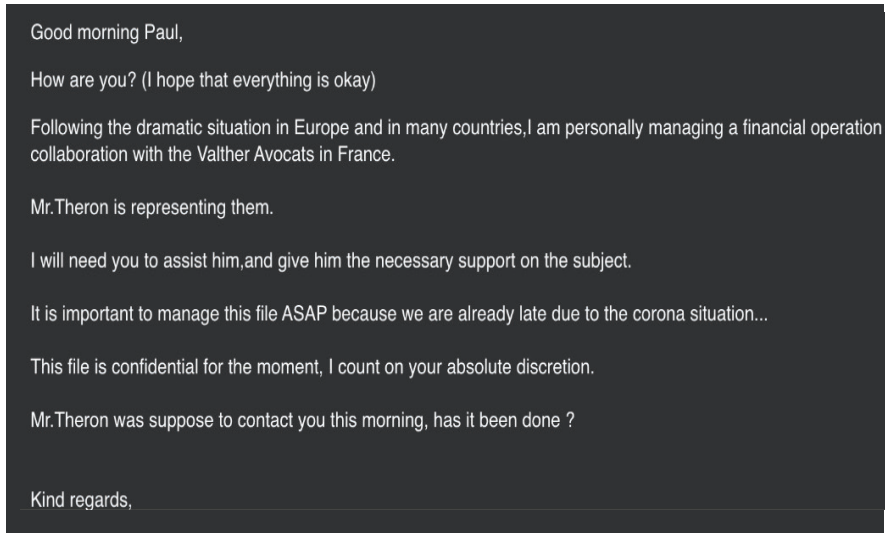
Types of COVID-19 fraud

Business Email Compromise (BEC)

The FBI anticipates a rise in BEC schemes related to the COVID-19 pandemic.

- BECs target anyone who performs legitimate funds transfers.
- There has been increased targeting of municipalities purchasing protective equipment or other medical supplies.
- COVID-19 related BECs often request funds be sent to a new account or that standard payment practices are altered due to the coronavirus outbreak.

Source: Federal Bureau of Investigation, "FBI Anticipates Rise in Business Email Compromise Schemes Related to the COVID-19 Pandemic," April 6, 2020



This BEC scheme requests the recipient take urgent action—likely a financial contribution.

Source: Trend Micro, "Developing Story: COVID-19 Used in Malicious Campaigns," April 8, 2020

Types of COVID-19 fraud

Phishing and Spear-Phishing Emails

Phishing emails may solicit:

- Charitable contributions
- Crowdfunding
- General financial relief
- Airline carrier or other refunds

Beware of phishing emails requesting verification of your personal information in order to receive an economic stimulus check from the government.

Government agencies are not sending unsolicited emails seeking your private information in order to send you money.

Source: Federal Bureau of Investigation, "Public Service Announcement, Alert Number I-032020-PSA," March 20, 2020

Fake Websites

- Phony URLs represent five percent of COVID-19 fraud tools. [1]
- Nearly 40,000 fraudulent websites related to COVID-19 were created in March. [2]

Sources:
(1) Trend Micro, "Developing Story: COVID-19 Used in Malicious Campaigns," April 8, 2020
(2) Atlas VPN , "Over 35,500 Coronavirus-Related Websites Reported as Scams," April 3, 2020

Types of COVID-19 fraud

Money Mules

Money mules conduct illegal financial transactions on behalf of others. These might include:

- Allowing others to illegally use a bank account to receive and “process” or “transfer” funds via wire, ACH, mail or money service.
- Opening a separate account on behalf of a fake business.

Work-from-Home Schemes

Work-from-home schemes are being used to recruit money mules. Tactics might include:

- Online job postings and emails (easy money-little effort).
- Suspicious “employers” who use Gmail, Yahoo, Hotmail and other services that are normally for personal use.

Source: Federal Bureau of Investigation, “FBI Warns of Money Mule Schemes Exploiting the COVID-19 Pandemic,” April 6, 2020

Combatting COVID-19 fraud

Primary Security Measures

- Be suspicious of:
  - Requests for advanced payment of services when not previously required.
  - Last minute changes in wire instructions or recipient account information.
  - Employee requests for changes to direct deposit.
- Perform daily reconciliation of all banking transactions.
- Set up dual-approval for ACH and wire transfers.
- Reduce daily limits for ACH and wire transactions if they are not being used.
- Train all employees who perform online banking transactions on basic Internet security.
- Dedicate a computer to performing online banking transactions.
- Install firewalls and update anti-virus, anti-spam and anti-spyware programs regularly. Update other software regularly with new security patches.

Combatting COVID-19 fraud

Other Tips to Consider

- Be wary of sudden changes in established communication platforms or email account addresses.
- Do not use public “hot spots” for online transactions.
- Limit Internet banking access to a few trusted employees.
- Use strong passwords with a combination of upper/lower case letters, numbers and special characters.
- Ensure employees don’t share passwords.
- Delete unexpected, incoming e-mails that have suspicious attachments or provide web links.
- Beware of e-mails that appear to be sent from well-known companies with file attachments. These often house viruses.
- Never share employee or customer information if you cannot confirm the identity of the caller.
- Verify the web address of legitimate sites and manually type them into your browser.
- Check for misspellings or wrong domains within a link.
- Verify any changes and information via the contact on file. Don’t use the number or link in the email to contact the vendor.
- Ensure the URLs in emails are associated with the business indicated in the communication.
- Require security tokens for online banking access.
- Lock up security tokens when not in use and report lost/stolen tokens immediately.
- Don’t use primary administrative login to perform transactions, only for system setup.
- Don’t share usernames and passwords with users via the same email. Send them separately.
- Consider online fraud insurance coverage.
- Beware of refusal to communicate by any means other than email.
- Remove employee access immediately upon separation from the company.
- Consider hiring security professionals to design a program for your company.
- Shred sensitive business documents.

Available resources

FBI Internet Crime Complaint Center (IC3)

https://www.ic3.gov/default.aspx

U.S. Small Business Administration (SBA)

https://www.sba.gov/managing-business/cybersecurity

Federal Communications Commission (FCC)

https://transition.fcc.gov/cyber/cyberplanner.pdf

U.S. Department of Homeland Security –U.S. Computer Emergency Readiness Team

https://www.us-cert.gov/ccubedvp/smb

Synovus Safety and Security

https://www.synovus.com/contact-us/safety-and-security/

Synovus Personal Resource Center

https://www.synovus.com/personal/resource-center/#security

SYNOVUS®