Beware of Coronavirus-Related Finance Scams

By Kathleen Doheny
April 14, 2020

The COVID-19 pandemic has brought about not only illness and death, but a wave of coronavirus-related financial scams, as well.

The pandemic and economic fallout have provided a nearly perfect formula for a scammer's success, said Susan Grant, director of consumer protection and privacy at the Consumer Federation of America, a research and advocacy organization based in Washington, D.C.

"Crooks will dust off old scams, figure out a coronavirus angle and deploy them," she said.

John Breyault, vice president of public policy, telecommunications and fraud at the National Consumers League (NCL), an advocacy organization in Washington, D.C., agreed: "Scammers see this as a golden opportunity."

Many scammers have day jobs, Breyault said, and with the economic downturn, those who have lost their regular employment can now focus on scamming full time.

In March, the NCL, which operates a project called Fraud.org, put out an alert warning consumers of the "coming tsunami" of fraud attempts.

As a manager, you can fight back, first by educating yourself about which scams are likely, then by informing your employees about what to watch out for.

The Latest COVID-19 Cons

Here are the scams that experts predict employees at banks, credit unions and financial consulting offices are likely to hear about in the coming months. Be sure your employees are aware of these possibilities.

"Speed up that economic impact check": The Coronavirus Aid, Relief and Economic Security (CARES) Act is sending economic impact payments directly to the accounts of eligible taxpayers. Those who haven't given direct deposit information to the IRS can wait for a paper check, or they can provide the information in a secure portal on the IRS.gov website. That portal is expected to be functioning by mid-April. Knowing this, a scammer may offer to help a taxpayer get the check more quickly. The scammer might ask for the taxpayer's account information and offer to send an expedited payment—for a fee, of course. But no such service exists.

"Give the IRS your banking information": A scammer could set up a dummy website that claims to be the IRS portal and instructs users to provide their direct deposit information. Taxpayers doing an Internet search could wind up on the dummy site instead of on the actual IRS site.

"Invest in a COVID-19 cure": Scammers are expected to peddle bogus COVID-19 remedies, asking people to invest in them and promising impressive returns. In late March, the FBI arrested a Southern California man, alleging that he sought investments in a bogus company that claimed to market pills to prevent COVID-19 and injections to cure those already affected. His Instagram video promoting the products had more than a million views in three days, the U.S. Department of Justice said.

"Help victims and families": Requests to wire money or otherwise contribute financially to COVID-19 victims and families, posted on social media, may look legitimate. Some may be. Some may not be.

"Your account is missing information": Scammers create letters, e-mail or texts that appear to come from the Federal Deposit Insurance Corp. (FDIC), the government agency that insures bank deposits. Some scammers have fraudulently used the names of actual FDIC employees in the phony correspondence. They may ask for bank account information, claiming an update is urgently needed.

Help Employees Avoid Scams

Scams can also be directed against your own organization's workers, Grant said. A scammer might send an employee an e-mail that looks like it is from the employee's manager, requesting money be sent to an organization, such as a charity for coronavirus victims. The worker, who may be the person who typically handles such tasks, may not think to question the request. "It's not hard to guess someone's e-mail at a company," Grant said.

"Another variation is when the message looks like it is coming from the HR department to employees, saying, 'We need to update your personal information. There's been a glitch in our system, and we need to repopulate your personal information,' " Grant said. The e-mail may explain that the information is needed for payroll, and it often seems legitimate.

Gut Check

Scam or not? Grant suggests using a simple test to determine a request's validity: "If you hear that little voice in your head asking, 'Is this legit?' you better pay attention to that."

You can also stay up-to-date on new scams by checking these reputable websites: Consumer Federation of America, (https://consumerfed.org/) National Consumers League, (https://www.nclnet.org/) Federal Deposit Insurance Corp., (https://www.fdic.gov/) Federal Trade Commission (https://www.ftc.gov/), IRS (http://www.irs.gov/) and U.S. Securities and Exchange Commission (https://www.sec.gov/).

Kathleen Doheny is a freelance writer based in Los Angeles.