

Target for new COVID scam: Small business owners

January 13, 2021

by

Lesley Fair

Attorney, Division of Consumer and Business Education, FTC

There's a new coronavirus-related scam making the rounds, but this time the crooks are targeting small businesses. It starts with an email that claims to come from the "Small Business Administration Office of Disaster Assistance." It says you're eligible for a loan of up to \$250,000 and asks for personal information like birth date and Social Security number. Let's do a CSI-style investigation to spot clues that the email is a fake.

Clue #1. You got an email or phone call out of the blue that claims to be from the IRS, the Social Security Administration, or – in this case – the Small Business Administration. The FTC has warned about [government imposter scams](#) like this.

Clue #2. You were told that you're automatically eligible for a big loan. Real lenders never do this.

Clue #3. You're asked to hand over your date of birth and Social Security number. This is a tip-off that the sender is trying to steal your personal information.

Phishing attempts aren't the only scam that business owners are reporting. We've heard from people who have applied for loans through websites pretending to be part of the SBA's Economic Injury Disaster Loan program, which has been extended to December 31, 2021. And other people report they've been contacted to repay loans they never took out. The likely culprits? Criminals who illegally applied for loans in their name.

Here are steps you can take to help protect yourself.

Check your credit report. The worst time to learn that someone has taken out a loan in your name is when you're applying for a loan yourself. So check your credit report first at www.annualcreditreport.com, the authorized source for the free reports

consumers are guaranteed by law. In addition, the three major credit bureaus are offering free weekly online reports to consumers through April 2021. If you're not in the market for credit or a loan, [freezing your credit](#) offers an extra – and free – measure of protection.

Look for reliable sources of information. Looking for a loan? Don't click on a link in an unsolicited email and be careful with online search engine results. Scammers often bait their online traps with sound-alike names and URLs, phony endorsements, and professional-looking websites. For small business owners looking for COVID-relief programs, always start at www.sba.gov, the official site of the Small Business Administration. Or reach out to a trusted financial institution in your community.

Check out lenders before sharing personal information. Scammers who impersonate lenders have the perfect excuse to ask you for lots of personal information that can be used to steal your identity. Don't leave a trail of personal information exposed by filling out lots of applications online with lenders you don't know. Investigate lenders first and if you spot something amiss, stop. And then file a report at ReportFraud.ftc.gov.