Northwest Credit Union Association
Idaho • Oregon • Washington

Fraud Alerts

Federal Trade Commission Reports Rise in Fraud Schemes Related to Small Businesses and to Grandparents

The Federal Bureau of Consumer Protection has recently issued two alerts that we are sharing here:

Small Business Alert

If you own a small business or work for one, you've seen the headlines about financial relief that may be available to some companies through the Small Business Administration (SBA). You've also likely heard about scammers who extract a grain of truth from the news and distort it in an effort to cheat small businesses. Now more than ever, it's critical for small businesses to go straight to the source for accurate information about what's happening at the SBA. That source, of course, is the Small Business Administration's dedicated page.

The SBA's Coronavirus Small Business Guidance & Loan Resources page offers the latest information about the Paycheck Protection Program, Economic Injury Disaster Loans, Loan Advances, SBA Debt Relief, and SBA Express Bridge Loans. Yes, there are legitimate business groups and financial institutions sharing information, too. But given the number of fraudsters out to make a quick buck with bogus websites and phony emails, your safest bet is to go straight to the SBA by carefully typing the URL sba.gov/coronavirus into the address bar at the top of your browser.

Here are more tips to help you avoid scams targeting small businesses.

- **Scammers often mimic the look and feel of legitimate email**. You've heard warnings for years about email phishing attempts. Fraudsters have upped their game in response. They've been known to copy logos of financial institutions and government agencies, including the SBA, and use wording that sounds familiar. They also manipulate email

addresses so that a message looks to be from a legitimate source – but isn't. That's why it's dangerous to respond to those emails. Instead, go directly to the SBA site.

- **Don't click on links**. Say you get an email that says it's from your bank or a government agency. Don't click on any links. It could load malware onto your computer. If you think you may need to respond, pick up the phone and call the office directly, but don't use a number listed in the email. That could be fake, too. Instead, search online for a genuine telephone number or call your banker using the number you've always used. Yes, now is a good time to keep in close contact with your financial institution, but employ the same established lines of communication you used before COVID-19 became a concern.
- **Be suspicious of unsolicited phone calls**. Some scammers may try the personal approach by calling you and impersonating someone from a financial institution or government agency. Don't engage in conversation. If you think you may need to respond, call using a number you know is legit.
- **Watch out for application scams**. Some small businesses report they've received unsolicited calls or email from people claiming to have an inside track to expedite financial relief. The people contacting them may charge upfront fees or ask for sensitive financial information – account numbers, tax IDs, Social Security numbers, and the like. Don't take the bait. It's a scam. Applying for a loan was a step-by-step process before the Coronavirus crisis and it's a step-by-step process now. That's why the SBA's sba.gov/coronavirus site is the safest place for you to start.
- **Alert others to Coronavirus relief check scams**. Most people have read the news about Coronavirus relief checks that many Americans may receive. The FTC Consumer Blog has advice about spotting relief check scams. Share the tips with your co-workers, family, and social networks.

If you spot a potential Coronavirus-related scam, report it to the FTC at ftc.gov/complaint.

Grandparent Scams in the age of Coronavirus

Grandma: I'm in the hospital, sick, please wire money right away." "Grandpa: I'm stuck overseas, please send money." Grandparent scams can take a new twist – and a new sense of urgency – in these days of Coronavirus. Here's what to keep in mind.

In grandparent scams, scammers pose as panicked family members in trouble, calling or sending messages urging you to wire money immediately. They'll say they need cash to help with an emergency – like paying a hospital bill or needing to leave a foreign country. They pull at your heartstrings so they can trick you into sending money before you realize it's a scam. In these days of Coronavirus concerns, their lies can be particularly compelling. But we all need to save our money for real family emergencies.

So, how can we avoid grandparent scams or family emergency scams? If someone calls or sends a message claiming to be a grandchild, other family member, or friend desperate for money:

- **Resist the urge to act immediately** – no matter how dramatic the story is.
- **Verify the caller's identity**. Ask questions that a stranger couldn't possibly answer. Call a phone number for your family member or friend that you know to be genuine. Check the story out with someone else in your family or circle of friends, even if you've been told to keep it a secret.
- **Don't send cash**, gift cards, or money transfers – once the scammer gets the money, it's gone!

For more information, read Family Emergency Scams. And if you get a scam call, report it to the FTC at ftc.gov/complaint.

David Curtis CUCE
Director, Compliance Services
Northwest Credit Union Association
206.340.4785 • 800.995.9064 x151
www.nwcua.org

If your credit union needs to report fraud, please fill out this form.