

www.constructionnews.net ★ (210) 308-5800 ★ Volume 23 ★ Number 6 ★ JUNE 2020

ACCOUNTING



Don't Fall for COVID-19 Money Scams

Steven Bankler, Owner Steven Bankler, CPA, Ltd. San Antonio, TX

Millions of dollars and valuable personal information have been lost to money scams and the problem is only increasing during the COVID-19 pandemic. If you're a business owner, you need to be extra careful right now

because scams involving federal stimulus money and relief loans are increasing by the day. Criminals are counting on fear and compassion—two powerful emotions that are in large supply during a crisis—to trick you. Your best defense is to be vigilant and arm yourself with the latest news. Be on the lookout for the following common scams:

Fraudulent PPP and emergency relief loans

With the trouble businesses have had securing PPP and other Small Business Administration (SBA) loans, fraudsters have stepped in to fill the void. Many of these scams show telltale signs that they aren't what they seem. Offers appear to come from the U.S. Treasury Department or SBA offering loans or grants in exchange for your personal financial information. But here's what happens: They take that information and apply for the loan on your behalf, while you A) are on the hook to pay it back and B) lose your one chance to apply. Other scams promise a faster or guaranteed loan for a fee.

As the federal government opens additional funds for loans, it's important to note: these loans don't cost anything and they can't be fast-tracked or guaranteed to go through. Your safest course of action is to work with a financial institution you know or with whom you already have a relationship.

COVID-19 PPE scams

Getting crews back to worksites involves securing additional personal protective equipment (PPE) and medical equipment—from masks to contactless thermometers and hand sanitizer—to protect them. Scammers have emerged by the thousands to take advantage of businesses needing these supplies. The FBI warns of several schemes involving PPE procurement that borrow from old scams, including a requirement for wired funds upfront and email phishing scams spoofing legitimate company email addresses to secure payment information.

Be on the lookout for unapproved vendors and those that are difficult to verify. If the seller contacts you, verify with the manufacturer that the seller is a legitimate distributor of their product. Don't overlook unusual payment terms or a sudden request to reroute payments. Follow your instincts and ask questions.

Social Security scams

The IRS is warning taxpayers to be on the lookout for a new twist on a scam re-

lated to Social Security numbers. The scam usually originates with a caller claiming to be able to suspend or cancel the victim's Social Security number due to an overdue tax bill. Don't fall for it.

First, your SSN is not affected by your tax bill, and it doesn't need to be reactivated or confirmed to remain valid. The immediacy of the call is also a red flag. The IRS would never threaten to immediately bring in local police or other law enforcement groups to have a taxpayer arrested for not paying. Plus, the IRS would never demand taxes be paid without allowing the taxpayer to question or appeal the amount owed. A series of letters will almost always arrive before any other form of communication is initiated.

Charity fraud around major disasters

Unfortunately, criminals often strike along with major disasters like fires, floods, and outbreaks like COV-19. According to the IRS, these fraudulent schemes usually start with unsolicited contact by telephone, social media, email, or even in-person. Bogus websites or phone number masking might make the soliciting "nonprofit" appear legitimate. The scammers may even claim to be working for or on behalf of the IRS to help victims file casualty loss claims and get tax refunds.

Be careful when being generous. Research the organization and get their legitimate contact information from the Tax Exempt Organization Search at IRS. gov or through a charity evaluator like CharityNavigator.org. Never give or send cash (it's better to give in a way that's traceable, like a check or credit card), and don't give out personal financial information to anyone who contacts you for it.

Fraudulent tax reminders

Last summer, the IRS detected a new email scam with subject line variations that include "Automatic Income Tax Reminder" or "Electronic Tax Return Reminder." The emails have links that show an IRS.gov-like website with details that appear to be about the taxpayer's refund, electronic return or tax account. The emails contain a temporary or one-time password to "access" the files. But when taxpayers click through, it turns out to be a malicious file. The malware allows the imposters to gain control of the victim's computer or secretly download software that tracks every keystroke, eventually giving them passwords to sensitive accounts, such as financial accounts.

The golden rule here is to not click on links within unsolicited emails. The IRS never initiates emails about tax refunds or sensitive information like PINs, passwords, or similar access information.

Protect yourself from these scams. Hang up the phone, don't click on the email, do your research. If it's the IRS that's supposedly contacting you, log in to your account at IRS.gov, call the IRS back directly (don't use the number the solicitor gives you), or contact your CPA to find out if it's legitimate. The same actions can be taken if the person contacting you claims to be from your bank or financial institution. In these cases, it's better to be safe than sorry.

Steven Bankler has more than 43 years of experience in the accounting industry. Steven's expertise lies in consulting, planning, tax, and asset protection as well as exit strategy services for closely held businesses. He also provides litigation support (both as a testifying expert witness and a consulting expert), business negotiations and estate planning. Visit www.bankler.com for additional tax strategy tips

and to learn more about Steven Bankler, CPA, Ltd.

Helping employers during COVID-19

When the workers' compensation rates skyrocketed in the late '80s and early '90s, the Texas Legislature created the Texas Workers' Compensation Fund. Years later, Former Governor Rick Perry, changed the fund's name to **Texas Mutual Insurance Company** by signing into law HB 3458 authoring it to operate as a mutual insurance company. Committed to building a stronger, safer Texas, they exist to protect businesses, promote safe environments and help ensure Texas workers get home safely to their families.

As Texas and the rest of the world navigate through the unique situation that the coronavirus is posing, Texas Mutual stands strong in their commitment to those who count on them by supporting their policyholders; stepping in for their communities; helping their agent partners; and keeping employees safe.

For the past 22 consecutive years, Texas Mutual has distributed dividends to reward policyholders who contribute toward keeping employees safe and losses low. When an employer purchases a policy at Texas Mutual, they are not just buying financial security for themselves and their employees. They're also becoming owners of Texas Mutual. As a policyholder, you can improve your chance of qualifying for a dividend by prioritizing safety and putting a return to work program in place.

Texas Mutual paid \$330 million in dividends to 57,000 eligible policyholders in April 2020, bringing the 22-year payout total to over \$3.1 billion. Paying the dividends two months early put funds into the hands of Texas employers when our economy needed it most. Dividend distribution has been at the heart of consistently rewarding their policyholders for sharing in their mission of building safer workplaces. Texas Mutual has also committed \$2 million in grant funding for nonprofit organizations across the state that are vital to COVID-19 relief and recovery.

Furthermore, a number of nonprofit organizations that received workforce development grants from Texas Mutual earlier this year have been released to use those grants not just on specific programs but for meeting the needs they have now, whether that is payroll for staff or supplies to serve those in need.

Texas Mutual has also helped employers settle into new remote work environments by providing tips and safety guidance. As employees have been working remotely from their homes, most people don't have the same type of workstation in their homes as they do at the office. The following tips are recommended best practices to help you work productively and safely at home.

Choose a dedicated workspace:

Designate a spot in your home for working. It should ideally be a space you don't relax in so there's a separation of work and play.

Define a beginning and finishing time:

Pick a definitive start and end time each day to establish a clear balance.

Dress the part:

Dress like you're going to the office; it helps keep a sense of routine and keeps you focused.

Have a plan:

Keep a more structured daily schedule than usual to help you avoid distractions and maintain productivity.

Think about how you're communicating:

Be conscious of how you're commu-



nicating and the different communication methods you're using.

Take clear breaks:

Remember to take breaks when you need to and use this time to get up, stretch and move around.

Consider lighting and space when setting up your workstation:

Make sure you have enough lighting and space to work comfortably.

Ensure walking paths and doorways are unobstructed:

This will help prevent slips, trips or falls and keep paths clear in case of an emergency.

Don't place computers near heat sources:

Computers and other hardware can overheat which could lead to malfunction and could even start a fire.

Maintain a clean and clutter-free workspace:

To minimize the spread of COVID-19, many counties and cities are implementing stay-at-home orders. While you are home and sharing space with your family members, be sure to sanitize your workstation and continue frequent handwashing. You should also keep your space free of trash and other hazards that could cause you to slip, trip or fall.

Use power cord ties:

Cord ties can help you keep your cords organized, preventing trip and fire hazards.

Utilize surge protectors:

Without a surge protector, a power surge can easily damage your computer, effecting your data or your system.

Keep liquids away from electrical equipment:

This includes on the ground and on your desk. You can also keep a coaster on your desk and a lid on your cup to help prevent any spills.

Prevent cybersecurity risks:

You can practice good computer security by utilizing a secured VPN and Wi-Fi, keeping up with company-approved computer updates and being vigilant of phishing scams through email and phone.

Stay hydrated and remember to give yourself a lunch break:

Keep these things in mind as working remotely affects your normal office routine.

Smoke alarms and carbon monoxide detectors:

It's likely that you will already have these in your home so be sure to check their batteries and test them regularly.

First-aid kit:

Accidents can happen at any time so be sure you can quickly find first-aid essentials in your home.

Fire extinguisher:

Familiarize yourself with the fire extinguisher in your home so that if a fire occurs you are prepared to react quickly.

Prevent awkward postures and eye strain by making your workstation setup more ergonomic:

Eliminate sources of glare behind the monitor and try not to face directly into a window.

Follow the 20-20-20 rule by looking at an object at least 20 feet away for 20 seconds every 20 minutes.

Keep your shoulders relaxed with your elbows at your side.

Do not overreach for your keyboard or writing tools.

When in seated position, your hips should be level-to-slightly-higher than your knees.

If your feet don't touch the floor, use a box or footrest to prop them up.

Your elbows should be even or slightly lower than your keyboard.

If possible, use an external monitor, keyboard and mouse.

Take regular stretch breaks throughout the day. -cmw





Steven Bankler,CPA,Ltd.

Our Job is To Put Money in Your Pocket!*



ESBE SBE 213055107

210.530.0062 • FAX 530.0064 MIKE & MARK CRAWFORD P.O. Box 791324 San Antonio, Tx 78279-1324

1-800-ASPHALT

EMAIL: estimating@prolinepaving.com office@prolinepaving.com



CONSIDERING CHANGING ADVISORS?

LOOKING FOR A PROACTIVE CPA?

If you have a family-owned or closely-held business, we're now taking applications for potential clients.

Call to apply for a FREE initial interview.

(210) 691-3133 www.bankler.com

Visit our website and view Client Spotlight for construction client success stories.