Federal Trade Commission Offers Tips to Recognize Scams

Unscrupulous scammers and fraudsters see this period of uncertainty as the perfect opportunity to take advantage of small business owners, including dentists applying for Small Business Administration loans. The Federal Trade Commission can help.

I've heard that scammers and fraudsters may try to take advantage of small business owners, like dentists, who apply for government financial relief. What can I do to protect my practice and get credible advice and updates on avoiding scams related to Small Business Administration ("SBA") loans?

The ADA continues to provide guidance to dental practices on the availability of and how to apply for governmental assistance, such as Paycheck Protection Loans and EIDL loans. But scammers are also aware of these programs, and would love to take the opportunity to scam your practice. The Federal Trade Commission continues to provide guidance to avoid these scams, and their information, "*Where small businesses can turn for accurate information about financial relief*," provides the following tips and warnings:

- **Scammers often mimic the look and feel of legitimate email.** You've been warning your employees 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, end the call and call back 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 your employees 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 staffers, family, and social networks.

At present (things remain fluid), for a good SBA source to remain alert to scams related to SBA loans, review the helpful content available at "*BEWARE OF SCAMS AND FRAUD SCHEMES*."

The FTC has also requested that, if you do spot a potential Coronavirus-related scam, you report it to the FTC at ftc.gov/complaint.

Finally, while we're on the subject of fraud, ransom ware remains very much a threat to your practice. The ADA has previously reported on ransomware attacks on dental practices (see, for example, "*Protect Your Practice from Ransomware*".

Now is the time to act proactively to minimize the chances that, even if you become a ransomware target, your practice does not become another victim. Review ADA's previously issued guidance, "*Tips to Safeguard Your Practice from Computer Hackers*," which also suggests immediate actions to take if you suspect that you've been hacked.

Disclaimer. These materials are intended to provide helpful information to dentists and dental team members. They are in no way a substitute for actual professional advice based upon your unique facts and circumstances. ***This content is not intended or offered, nor should it be taken, as legal or other professional advice***. You should always consult with your own professional advisors (e.g. attorney, accountant, insurance carrier). To the extent ADA has included links to any third party web site(s), ADA intends no endorsement of their content and implies no affiliation with the organizations that provide their content. Further, ADA makes no representations or warranties about the information provided on those sites.

© 2020 American Dental Association All rights reserved.