Be Alert for Cybercrime Scams

Cybercriminals often boost their efforts to take advantage of people and businesses during times of uncertainty. Know what to watch for to reduce the chance of being a victim.

Does the pandemic create additional risks of cybercrime that might harm a dental practice? What can I do to minimize the chances of my practice being a victim of a cyber scammer?

Cyber criminals are enterprising, opportunistic, and amoral. For example, they are aware that COVID-19 is on our minds, and they take advantage of that to trick people. They are aware that large numbers of employees are working from home, and that functions previously performed solely in the workplace are now being performed remotely. Functions like processing payments. Like handling protected health information (PHI). Often by workers not used to performing these tasks remotely, and even sometimes using family computers that may lack antivirus or other safeguards present in dental office software. The criminals and fraudsters are already on the job: the Federal Trade Commission has already provided several alerts about coronavirus scams, including "FTC: Coronavirus scams, Part 2" and "Avoid Coronavirus Scams." An alert from the newly formed Virginia Coronavirus Fraud Task Force cautioned about various scams, including:

- "**Phishing scams:** Scammers posing as national and global health authorities, including the World Health Organization (WHO) and the Centers for Disease Control and Prevention (CDC), are sending phishing emails designed to trick recipients into downloading malware or providing personal identifying and financial information." https://www.justice.gov/usao-wdva/covid-19-fraud

Another warning plays on expectations of government relief checks:

- "**Government relief check scams**: Scammers send you a message make a social media post claiming you qualify for a COVID-19 government grant and just need to click a link to fill out the "necessary" personal information. In the process, your identifying information is stolen.

  What to do: [If the message is unexpected or seems suspicious]… don't click! In addition to taking your money, these sites can also download malware to your device and use your information for identity theft." https://www.whsv.com/content/news/These-are-the-coronavirus-scams-you-should-look-out-for-568969131.html

- With respect to the government contacting you, be very wary of anyone who claims to be contacting you (by telephone, text, or via social media) from the government. Some guidance on this is available in the FTC's resource "How to avoid COVID-19 government imposter scams."

The Cybersecurity and Infrastructure Security Agency (CISA), which is part of the Department of Homeland Security, recently warned that a malicious cyber actor was sending phishing emails "spoofing" the Small Business Administration (SBA) COVID-19 loan relief webpage. Email spoofing occurs when a scammer deliberately falsifies the sender address in order to mislead the email recipient to believe the email comes from a trusted source. Telephone scammers can also use spoofing to deliver misleading information to your caller ID to disguise their identity. For more information on telephone spoofing, see the Federal Trade Commission.

Phishing may also come by text message (SMS). SMS phishing often uses lures involving financial themes, such as government payments or tax rebates.

On March 25 the FTC posted Seven Coronavirus scams targeting your business and urged "…sharing this information with your employees and social networks…"

How can I minimize the chances of being a victim of attacks and scams like the above?

Phishing emails[1] are a prime way that hackers enter, and these are almost certain to increase. Caution your staff to be particularly vigilant during this crisis. Watch out for emails and texts that try to use the COVID-19 public health emergency to trick you into clicking on a link. For example, the message could be "click here to see the location of

[1] Some ways to recognize phishing:
- Sender will want you to take immediate action (e.g. will ask for an urgent payment)
- Sender may send a fake invoice as an attachment (e.g. bill past due, delivery invoice)
- Sender may claim there is a problem with your account and ask you to send a payment
- Sender may include "Click Here" URLs and ask for your username and password
- Sender may invite you to a meeting on a teleconferencing platform

Be Alert for Cybercrime Scams

COVID-19 cases in your neighborhood" or something similar. Before clicking on any link, take a very close look at the message. Better to be safe than sorry.

Look carefully, even if a message appears to come from a trusted source such as the ADA, your bank, or a governmental entity (such as the Small Business Administration – scammers know that small businesses may be seeking information about SBA loans). These messages may be spoofed or forged so that they appear to come from the entity in question. They may instruct you (or your staff member) to click on a link, open an attachment, provide a username, password or other sensitive information, or send money. Your staff may receive an email that appears to be from their supervisor, asking them to buy gift cards or something else for emergency use.

The attackers know that for many of us, working circumstances have changed, and that we may getting unusual (but sometimes legitimate) requests. Attackers hope unexpected or unusual emails may be more likely to be accepted at face value.

If you receive an email that looks unfamiliar, or asks you to do something unusual, or asks you to do something quickly, be sure to take a very good and skeptical look at it before proceeding with any instructions. If an email that purports to come from an individual or entity that you know but seems suspicious, check with the purported "sender" (but don't hit "reply" – reach out to the sender using confirmed contact info like their known email address or phone number). Hovering over an email senders name will display the sender information. In addition, hovering over any URL link in the email will display the URL for the link. If it looks suspicious do not take any action. You can also check with someone whose judgment you trust before clicking on the link or taking any other action requested in the email. Two heads scoping out a suspicious email are better than one.

The Federal Trade Commission, recognizing that more of us will be working from home, during the pandemic, recently posted Online security tips for working from home which also provides valuable reminders for cyber security while performing tasks remotely. This may be an opportune time to review (yourself and with your staff) the FTC's guidance regarding Malware. Some attackers exploit vulnerabilities in teleworking technologies. Before deploying new technology, assess the security risks and implement appropriate safeguards. If patient information is involved, the risk analysis and safeguards should be documented in compliance with HIPAA, if applicable.

Attackers also attempt to exploit communications platforms such as teleconferencing services. The Office for Civil Rights recently shared a warning from the Federal Bureau of Investigations, FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic, that offered safeguards to help secure use of teleconferencing platforms. Another helpful resource to reduce the likelihood of "hijacking" that may occur when using platforms, such as "ZoomBombing," is available through the company's blog, see ZoomBlog, *A Message to Our Users*, April 1, 2020.

There is no denying that these are difficult times for dental practices; there is also no denying that things could get even worse if your practice is victimized by a phishing or malware scam. Alert your staff to take precautions.

For more information, see:

- CISA, *Alert (AA20-099A) COVID-19 Exploited by Malicious Cyber Actors,* April 8, 2020