8 TIPS FOR PROTECTING YOUR DENTAL PRACTICE FROM PHISHING ATTACKS

by Darby TechForce

You get hundreds of emails every day. Patients, suppliers, and insurance companies are constantly infiltrating your inbox to request appointments and solicit payment for supplies and services. Most of the time you're good at quickly scanning the list of senders and subject lines to see which emails warrant your attention and which ones you can delete without opening. But sometimes, it's not so easy to distinguish a real message from a malicious one.

Phishing attacks trick you into clicking on a link or attachment that infects your computer with malware or takes you to a website that looks legitimate, but isn't. All it takes is opening a single infected email to give a cyber criminal access to all of your patient and practice information. Unfortunately, phishing attacks are extremely common, and the consequences can be devastating for your business.

According to a 2017 report from Accenture and the American Medical Association (AMA), 55% of healthcare professionals said they had experienced a phishing attack. With the average cost of a stolen healthcare record ringing in at $380, protecting your patients' information is critical not only for their safety, but for your practice's bottom line.

While it's impossible to prevent hackers from attempting to steal your sensitive information, you can train your front office staff how to identify fake emails and how to respond in the event of an attack. Here are eight tips for protecting your dental practice from phishing attacks.

1) Listen to your gut
It may sound new age, but experts recommend listening to your intuition when it comes to avoiding phishing scams. If an email looks sketchy and feels off, it probably is. Don't open it and click delete. A legitimate sender will follow up if he or she doesn't hear back from you.

2) Check the source
Sophisticated hackers can take over someone's email address and send messages that look like they're from a trusted source. If the email address is legitimate but the text seems sketchy, reach out to that person separately and ask if he or she sent you an email.

3) Take extra precautions
Use a password manager to create strong, unique, random passwords with letters, numbers, and symbols. Be sure to enable multi-factor authentication on all accounts that offer it. The extra steps may seem tedious, but they could protect your practice from being hacked.

4) Inspect the subject line
Cyber criminals are smart marketers. Phishing emails will often use exciting or threatening subject lines to appeal to your emotions. Be very suspicious if an unknown sender tries to get you to act quickly or submit personal information by clicking on a link.

5) Carefully read the email
Phishing emails often use generic greetings like "Dear Sir or Madame." A legitimate organization would not address their customers this way. Scroll down to the footer to see if there is a physical address or "unsubscribe" button. If one or both are missing, it might be a fake email.

6) Check for spelling
One of the most common signs an email is a phishing attack is the presence of grammar mistakes. Look for improper capitalizations and misspellings. If the email is from a legitimate organization, they will proofread their emails before sending them out.

7) Keep your operating system up to date
Failing to update your computer with the latest version of your operating system leaves it vulnerable to phishing attacks. If you're still using Windows 7, now is the time to start upgrading your computers to Windows 10. Microsoft will soon stop providing security patches for Windows 7.

8) Hover, but don't click
If you open an email that looks suspicious, hover your mouse over one of the links in the message to view to the URL it will send you to. If you don't recognize the website, do not click on the link and delete the email.

As careful as your staff is to avoid phishing attacks, mistakes can happen. In the event of a successful phishing attack, an offsite backup like DataSafe may be the only way to restore the files that keeps your practice running.

At Darby TechForce, our HIPAA compliant backup service goes beyond just storing your most important data. Our tech experts monitor and manage your backups to make sure they're always working, and we fix them if they're not. Should a phishing attack lock you out of your practice management software, we can help get your data back in a matter of hours with Rapid Restore.

For more information about protecting your practice from phishing scams, check out our whitepaper: How to Avoid Phishing Attacks in Your Dental Office.