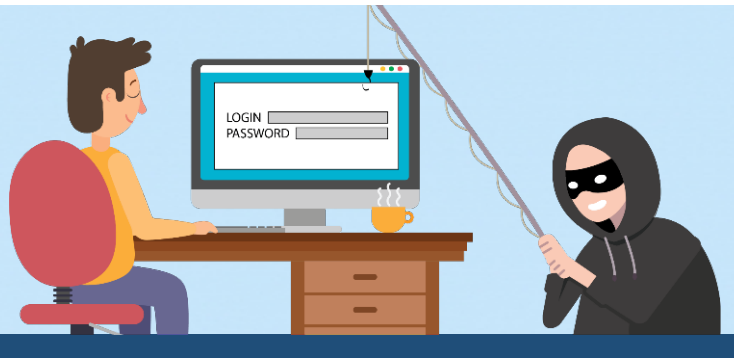
HOW TO AVOID PHISHING ATTACKS IN YOUR DENTAL OFFICE

by Darby TechForce



You would think your email inbox would be the one safe place on the Internet where you could avoid computer viruses. Unfortunately, that's exactly what hackers want you to think. Often, all it takes is opening one infected email to give a cyber criminal access to all of your sensitive information. This is called a phishing attack, and the consequences to your dental practice can be severe. While you can't do much to prevent a phishing attack from happening, there are some important security measures you can take to avoid becoming a victim.

What is a phishing attack?

A phishing attack involves a fake email designed to look like it's coming from a person or organization you trust. The email will usually involve an exciting or threatening statement to trick you or your front office staff into releasing sensitive patient files. In other cases, the sender will attempt to gather information about your practice that can then be used to gain access to protected patient data.

For example, one of your employees could get a phishing email that looks like it was sent from your software provider asking her to reset her password. She clicks the link in the email and is taken to a website that looks familiar. After entering her username and a new password, the hacker can use her credentials to log into the provider's system and access your patients' protected health information. The cyber attacker can also use your employee's contact list to send more phishing attacks, making it appear as though the email was sent from your longtime, trusted receptionist.

Dental practices are at risk for phishing attacks

Think you could never be duped by a hacker? It's dangerous to assume a healthcare phishing scam will never affect your practice. 90 percent of modern data breaches now involve a fake email enticing an individual to click a link or download an attachment that will put malicious files on his or her computer. Phishing attacks have become so sophisticated that a malicious website could look indistinguishable from the login screen you use every day.

How common are these scams? According to a 2017 report from Accenture and the American Medical Association (AMA), 55% of healthcare professionals said they had experienced a phishing attack. A majority of the providers surveyed said that HIPAA compliance alone isn't enough when it comes to securely sharing personal health data. To keep your patients' information safe, it's important to be able to identify fake emails before clicking a link or opening an attachment and train your front office staff to do the same.

How to recognize and avoid a phishing attack

While email is a convenient way to share information, doing so makes dental practices attractive targets for phishing scams. Unfortunately, the spam filter on your inbox can only do so much to sort out unwanted emails. It's important to be able to recognize the signs of a phishing attack to keep your practice and your patients safe. Use the following tips to evaluate suspicious messages and share them with your front office staff so everyone is on the same page.

1. Confirm the identity of the sender. Make sure the name in the "From" field matches the email address between the brackets. Be wary of email addresses that contain typos or unusual capitalization.
2. Check for personalization. Generic email salutations like "Dear Sir or Madame" could be from a cyber attacker. Don't trust impersonal greetings, especially from an organization you do business with.
3. Inspect email links – but DO NOT click on them. Hover your mouse over a link within the email and it will show the full URL it will direct you to. If the destination is not a familiar link or website, don't click it.
4. Inspect the footer. Scroll down past the content of the email to the bottom of the message. If the email footer doesn't include a physical address for the brand or company or an "unsubscribe" button, it's probably fake.
5. If you're unsure, just hit delete. A generic email from an unknown sender asking you to download an attachment may or may not be malicious. If it's legitimate, the sender will email you again or call you for the information.

Boost your cybersecurity to protect your patients' privacy

Unsolicited emails are more than annoying messages clogging up your inbox. Clicking on a link or downloading a suspicious attachment could place malicious software on your computer that deletes important data or holds it for ransom. To avoid losing your patients' health records and other important files, it's important to perform frequent backups. In the event of a successful phishing attack, an off-site backup may be the only way to restore the data that keeps your practice running.

At Darby TechForce, we take the guesswork out of backing up your most important files and keeping them safe. With DataSafe, our dental tech experts will monitor and manage your backups to make sure they're working properly and fix them if they're not. If your practice does suffer a data loss, our Rapid Restore cloud-based disaster recovery service will retrieve your files in a matter of hours with minimal downtime to your dental practice.

To add additional layers of protection, TechForce will set up a firewall and install antivirus software on every desktop in your office. This mitigates the chance of phishing emails getting through to your network. With us in your corner, there's no faster way to protect and recover your data from a healthcare phishing attack.

To learn more about protecting your dental practice with DataSafe and Rapid Restore, give us a call at 800-886-2093 or shoot us an email: connect@darbytechforce.com.