THE BRIDGE | News from Delta Dental of Tennessee

Chattanooga, Tenn.

FALL 2018

Smile With a Cybersecure Practice

by Andrew Woodard,
Chief Information Security Officer, Delta Dental of Tennessee

Practical Tips From a Security Pro

These days, it seems like news headlines broadcasting the latest data breaches occur with alarming frequency. Everyone involved in the healthcare industry cringes upon hearing these reports, hoping that their office (or sensitive personal information) will not be impacted.

We're also constantly being barraged with buzz words, like the "Internet of Things" (IoT) or "ransomware." What do these words mean? How do they apply to your dental practice? And what can you do to keep your office more secure?

Delta Dental wants to share some basic cybersecurity recommendations with you. This isn't an exhaustive list, but it's a good start to get you thinking about simple ways you can protect your practice. Many of these concepts apply to your home, as well.

Computers

- Your practice should use a current operating system (OS). For example, if using Microsoft Windows, Windows 10 is the safest option. You want to ensure that the OS you're using is still receiving patches and other updates, and that you can receive support

continued on page 2

The Power of $1

At Delta Dental of Tennessee, we take our financial responsibility seriously. We want our dental professionals and clients to see that the premium dollars they trust to us are being used wisely. For every premium dollar received, here's how it's used:

88¢

Paid Claims

$.88 goes direct to care and is the reimbursement to dental offices for services provided to our members.

6¢

Administration

$.06 covers all of the costs associated with sales and administration of the plans, the processing of claims, and customer service, which is housed in our Nashville headquarters.

3¢

Taxes and fees

$.03 is for premium taxes and broker commission fees.

2¢

Philanthropy

$.02 is our commitment to corporate social responsibility and is contributed back to the communities we serve.

1¢

Reserves

$.01 is deposited into reserves, as required by law, to ensure payment of all future claims.

Security ctd.

when you have any questions or face a technical issue.

• Patching – You should consider enabling automatic patching, which helps make sure your system is always up-to-date. Besides operating system patching for Windows or Mac, patch updates should also be applied to other applications such as Adobe Acrobat and Flash, Java and internet browsers.

• Internet Browsers – Along with current operating systems, internet browsers (such as Microsoft Internet Explorer, Mozilla Firefox and Google Chrome) should be kept current.

• Anti-Virus – You should have an anti-virus software installed on all computers in your office. This should be running in real-time mode and getting daily updates. Sometimes updates come more than once a day.

Wireless Routers and Devices

Securing a transmission – If you use wireless connectivity in your office, you should make sure no one can eavesdrop on the conversation between your computer (or other device) and the wireless router. Failing to secure a wireless connection could allow someone sitting in a nearby building or the parking lot, to tap into the communication. To help prevent this, we recommend the following:

• Configure the router to use WPA2 encryption.

• Set a strong password or passphrase for your office wireless network. If you offer a guest wireless network, make sure the password is different from your staff wireless network password. For more password tips, see the “Passwords” section in this article.

• Change the default password. Manufacturers ship routers with default account names and passwords. For example, the initial account name may be “admin” – short for administrator. And the password would be – you guessed it – “password.” Bad guys know this and when trying to break into your system, they try this and other simple passwords first. Therefore, it is best to change the account name and password when you set up your router.

• Reboot your router regularly. It sounds strange, but the bad guys have figured out how to infect your wireless router in memory, without changing any files on the system. Therefore, the U.S. Department of Homeland Security recommends rebooting your router often, to clear out any potential infection or malware.

• The Internet of Things (IoT) is a phrase describing the fact that these days, many devices in our homes and offices are “smart,” which means they are connected to the Internet. As with the wireless router, change the default account name and password if you can. Depending on the device, security updates may be needed. Also, take a moment to think about ways the device could be used incorrectly – just about any device connected to the Internet has a risk of getting hacked into.

Passwords

• Did you know the man who created complex passwords now regrets it? He realized how difficult it can be for most people to remember combinations of lower and upper case letters, numbers, and special characters, with a minimum of 8 characters, which expires every 90 days! It’s now recommended that people use longer phrases, such as “TodayPasswordsAreNotFun.” It’s even better if you mix up the order of words in a phrase, like “NotPasswordsFunTodayAre,” or are random words which are easier to remember than "TgAz$4m8!"

• In a world where accounts and passwords are everywhere, it is recommended that you keep your personal and work accounts separate. You shouldn't use the same password for your personal email account or social media account that you do for your credit card, online banking sites, or any other site that pertains to your business. If someone gets hold of one, they may be able to access your logins across all sites if you use a common user name and password.

• Password managers are software tools that make life much easier. They keep all of your numerous usernames and passwords secure (and not written on a sticky note in a desk drawer or under your keyboard!). When using a password manager, you only need to remember one password to get into your password manager tool. There are several inexpensive or free solutions available.

Ransomware

What is it? A type of malware that makes all of your files on your computer unreadable by encrypting them. The bad guys then ask for money to give you a "key" to decrypt the files. So how do you protect against it?

• Have up-to-date Anti-Virus and Anti-Malware software, operating system patch automatically, and restrict local administrator access on computers. A user shouldn't be logged in as a local administrator to the computer while answering email or surfing the Internet. This local administrator account should only be used when installing software or modifying settings.

• Be careful when opening attachments and clicking on links in emails.

• Back up your files often. Some ransomware infections will require computers to have the operating system reloaded, and you'll need those backups to restore critical files and keep your office running. Backups can also be extremely valuable in the event of a hardware failure or accidental deletion of critical data.

Dental Office Toolkit (DOT):

When using the Delta Dental Dental Office Toolkit website, we recommend:

• Use a unique account and password for each user. When two or more people share an account and password, it may be very difficult to distinguish one person's activity from another. The question you need to ask yourself is, "if one of the users performs an inappropriate action within the system, how would you determine who did it?"

• Use a password manager (described above) to store your DOT username and password. If the account and password are written down on paper and readily visible, other people can login to that account.

• If someone who has the ability to log in to DOT leaves your office, be sure to manage their access in our system so that they no longer have access.

We hope these tips to help secure your practice have been helpful. Please note, this list is not intended to be an exhaustive or complete set of security controls, but rather a starting point. You may find it helpful to reach out to a computer security company locally or find an IT professional who can be on-call in the event you have any trouble.

Andrew Woodard is the Chief Information Security Officer for Delta Dental of Tennessee, Delta Dental of Michigan, Delta Dental of Indiana, and Delta Dental of Ohio. He is responsible for the overall Information technology security program, including strategic direction and operations. Woodard holds an MBA from New York Institute of Technology as well as two industry security certifications, CISSP and CISA.

What Is PHI?

Although you likely have regular HIPAA reminder sessions, it's helpful to occasionally review what qualifies as Personal Health Information. Simply put, PHI is individually-identifiable information (information that can be tied back to a specific person) which relates to medical care.

Identifiers include:

Full Names (first and last)

Social Security Numbers

Dates of Birth

All geographic subdivisions smaller than a state
(such as a street address)

Driver's license numbers

Telephone or fax numbers

Email addresses

Health plan beneficiary numbers or account numbers

DELTA DENTAL®

Delta Dental of Tennessee
240 Venture Circle • Nashville, TN 37228-1699

Have you signed up for Delta Dental's National EFT program?

Call our Professional Relations department at 800-223-3104 for info!

What's Your Online Reputation?

If you're looking for ways to build your practice, taking a look at what's being said online can be a good way to start. Reviews on pages like Google, Facebook or Yelp can make the difference in whether a new client decides to call or passes you by.

Not sure where to start? You're already giving your clients great service, so why not begin with the people who know you best? Ask existing patients to leave a review on your Facebook page, or a Google review. You can offer an incentive, like an entry into a drawing for a gift card or an electric toothbrush for anyone who leaves feedback (good or bad).

When you get positive reviews, consider sharing them on your social media pages. They're also great morale boosters for staff and a way to get the conversation started if there's something your team needs to improve.

When negative reviews happen, it's important to acknowledge the situation and try to help resolve problems. Potential clients will be able to see that you care about what your patients think and do your best to make it right if there's a problem. Just be careful not to giveaway any PHI in the process (see page 3 for information on what constitutes PHI)!

If there are community Facebook pages for your area, consider joining them (or having someone on staff join them) and search the page for your practice's name regularly. People often post there for recommendations for a dentist before they even search their area, but they will also check reviews for the recommendations before making a decision.

Make sure your website and Facebook pages are up to date with current locations and times, as well as your current phone number and email so that it's easy for new patients to get in touch with you.

338 09/2018 2.2K