

# THE TECHNOLOGY BYTE

NEWSLETTER FROM YOUR TECHNOLOGY GUIDE:  
ACE TECHNOLOGY GROUP



## OVERVIEW:

**Dental Month**

**Tech Tips**

**Chris's Corner**

**Latest in Cyber Security**

**Recent Security Breaches**

**Reminder**

**New in Technology**

**ACE Employee Spotlight**

**Power Commands**

## DENTAL PRACTICES AND CYBER RISKS

**May is Dental Care Awareness Month** so we decided to focus this month's newsletter on dental care awareness in the form of cyber security.

Dental offices are often small businesses with limited time to focus on cyber security. Yet, dental offices hold personal, sensitive information that cybercriminals are just waiting to sink their teeth into. Cyber security can be confusing, and many small businesses think a cybercriminal wouldn't waste their time hacking their business to steal such a small amount of data. That is the complete opposite. Dental offices face multiple types of cyber attacks every day.

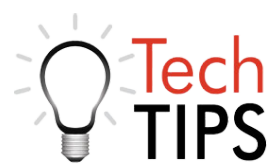
### Cyber Risks for Dental Offices

- Email fraud is a BIG problem. In 2019, the American Dental Association (ADA) was the target of a well-manicured phishing attack. The cyber criminals used the ADA logo and the signature of the ADA President to send emails to members in order to gain access to sensitive information.
- Dental practices rely on devices and applications that connect to online computer networks. That includes dental software, electronic patient records, and digital X-ray machines. Plus, personal devices that staff use. Each could be a compromised source and used by cybercriminals.

Dental practices cannot afford to ignore the risks of cyber threats, and they can't incur a cyberattack that leaves a bad taste in their patient's mouths.



## RECENT SECURITY BREACHES IN THE U.S.



### **American Dental Association**

Exploit: Ransomware



### **CashApp**

Exploit: Data Breach



### **Bob's Red Mill Natural Foods**

Exploit: Data Breach

## THREE KEYS TO AVOID PHISHING EMAILS AND RANSOMWARE ATTACKS

Here are three simple, practical cybersecurity awareness training tips you can use to identify and avoid malicious emails:

1. **Stop Skimming and Start Studying** - We receive so many emails that we've conditioned ourselves to skim messages and make quick decisions. But when we do this, we take unnecessary risks. That's because there can be clues both on the surface and just below the surface of the message that can alert us to things that aren't right
2. **Think It Through** - After you read an email, take a moment to digest it. What you want to do is give yourself the space to act thoughtfully, rather than just reacting at the moment.
3. **Verify, Verify, Verify** - It's critical to remember that, with phishing scams, things are never what they seem. The reality is that a message can look and even sound legitimate but still set off a warning bell.

It takes just a minute to confirm a questionable message, whether it comes from a coworker, internal department, financial institution, or other sources. [Read More.](#)

## Who's Responsible for HIPAA Violations?



## CHRIS'S CORNER

Monthly Expert Advice From The Owner

Most healthcare organizations cannot avoid HIPAA Rules. Those working in or with the healthcare industry must comply with HIPAA standards to protect the patient and build trust. Patients provide intimate details of their lives to healthcare professionals. If a patient's Protected Health Information (PHI) is exposed it can not only have a long-lasting impact on their health but on their finances and their safety as well. Failure to comply with HIPAA can have compelling consequences, professionally, personally, and even financially for healthcare professionals too.

Unintentional HIPAA violations can result from a lack of training and knowledge. While Covered Entities are required to train employees on policies and procedures related to the healthcare industry, they may not have the resources to provide training for every possible scenario. Taking responsibility for unintentional violations is not easily accepted by Covered Entities.

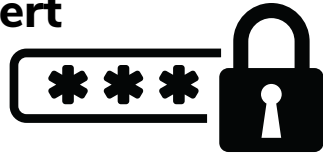
Acknowledgment implies failure to conduct thorough risk assessments, overlooked threats to Protected Health Information (PHI), or failed compliance monitoring of policies and procedures.

The best way to protect your career, improve your job prospects, and get the most out of your vocation, is to take responsibility for your own knowledge of HIPAA. Take advantage of HIPAA training courses that provide in-depth knowledge in areas of your role and situations and scenarios you may encounter in your work day.

For our HIPAA compliant customers, we offer PHI training, security risk assessments, and Phishing stimulations. When you receive these training courses, take advantage of the knowledge and information to increase your skillset and benefit your career as a healthcare professional.

# LATEST IN CYBER SECURITY

## Google Issues Alert to Billions of Chrome Users



In late April Google issued an alert to BILLIONS of Chrome users that the browser was targeted by hackers... and they succeeded. The attack revealed 30 new security flaws, seven of which pose a "high" threat to users.

Use-After-Free (UFA) attack is a memory exploit that has broken through Chrome security more than 65 times since the beginning of 2022. Chrome appears to be vulnerable to a new type of hack, "zero-day". A zero-day hack means the cybercriminals know vulnerabilities in a platform before a company can deploy a patch.

Google has since released an update to fix bugs, which impact Windows, macOS, and Linux. To manually check for the update, click the three dots in the top right corner of the browser and navigate to *Settings > Help > About Google Chrome*. The last critical step: *restart your browser*.

The attack on Chrome poses a real security threat to users who save their passwords in Chrome's password autofill feature. Experts warn against the use of storing passwords in Chrome, especially for those working remotely and storing passwords in web browsers. While the Chrome autofill is convenient it is not safe against cyber attacks.

### To turn off autofill

- **On Chrome**, select the three-dot "More" button in the top right > then Settings > then Show advanced settings > then uncheck "Enable Autofill to fill out web forms in a single click" listed under "Passwords and forms."
- **On Safari**, select Preferences > AutoFill > then deselect all of the information types that you want Safari to automatically fill.

If you used Chrome to save your passwords you can wipe them without too much difficulty. But before you wipe them from Chrome you'll want to download a CSV file of your passwords that can be imported into a password manager, like LastPass.

We highly recommend using a password manager to store your passwords. While it can get a little clunky using autofill with password managers, they offer a safer solution.

Click for Chrome Update Support

 <https://support.google.com/chrome/answer/95414?co=GENIE.Platform%3DDesktop&oco=1>

## How to Back Up Chrome Passwords

Export a CSV File of Your Stored Passwords from Chrome

### STEP 01

Visit

[passwords.google.com](https://passwords.google.com)



### STEP 02

Settings

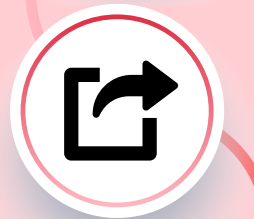
Tap the Settings in the top right



### STEP 03

Export

Click export next to export passwords



### STEP 04

Confirm

Confirm you want to export a CSV file.  
\*Note: you will need to verify ID

*File will download immediately*




## CYBERSECURITY TERMS TO KNOW

### HIPAA - HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

noun; Health Insurance Portability and Accountability Act of 1996: U.S. government legislation that ensures a person's right to buy health insurance after losing a job, establish standards for electronic medical records, and protects the privacy of a patient's health information. (Dictionary.com)



## REMINDER

REFER A FRIEND - WE'LL GIVE YOU A \$25 GIFT CARD FOR EACH REFERRAL AND ANOTHER GIFT CARD, UP TO \$250 IF WE WIN THEIR BUSINESS. [DETAILS HERE](#) 

# NEW IN TECHNOLOGY

## Digital Dentistry Gives Us Something to Smile About

Digital technology is transforming our world daily, that includes the dental industry. Digital advancements in dentistry have made office visits safer, faster, reliable, and more comfortable. Digital dentistry utilizes technology in dental procedures rather than electronic or traditional mechanical tools. Dentists are using digital dentistry to analyze and treat patients in multiple ways.



Since the pandemic, teledentistry has become a popular alternative to visiting dentist offices. Teledentistry provides dental consultations and even a basic examination without the stress and anxiety visiting a dentist's office can bring. By using digital tools such as synchronous or asynchronous video, dentists can determine if an emergency office visit is necessary or if the patient can wait until their next regular check-up.

We've all been in the dentist's chair watching a TV in the corner of the room. For many of us that TV did very little to distract us from the scraping and drilling sounds happening around us. Many dental practices have invested in virtual reality (VR) headsets to provide a more augmented reality for patients. Patients report that VR helped reduce pain and helped them to relax during procedures.

Remember those tiny mirrors dentists use to see every angle of your teeth? Dentists are now using tiny cameras to magnify and explore parts of the mouth. The cameras provide images of hard-to-see places in the mouth that help dentists provide accurate oral care. Those images also allow for 3D models of teeth to be made for crowns or other oral devices.

The benefits of new dental technology gives us all something to smile about!

## Get to know your friendly ACE team!

### EMPLOYEE SPOTLIGHT: AMANDA

*After a brief hiatus, we are thrilled to have Amanda back on our ACE Team!*

Sr. System Architect; Radnor, PA native; Delaware County Community College Graduate; wife to Pete, mom of two boys, two dogs, three cats, and one bunny.

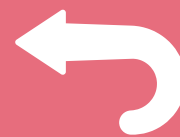


Has a diverse background with over 20 years of IT work experience, more than 10 of which have been in the MSP field. Amanda is known for her ability to truly understand the clients' needs and for finding solutions to even the most difficult challenges.

While she started with computers on her grandfather's Leading Edge Model D in the mid-'80s, her first PC was a Pentium 75 she received for Christmas in 1994. Computers have been a lifelong love for Amanda, and she considers herself lucky to pursue a career based on a passion.

When she's not at work, Amanda enjoys spending her time with family as well as various hobbies. She enjoys aquascaping, pyrography, woodworking, and when the seasons permit, gardening.

## POWER COMMANDS



Undo your previous command

**For Windows:** Ctrl + Z

**For Mac:** Command + Z



Redo your previous undo command

**For Windows:** Ctrl + Y

**For Mac:** Shift + Command + Z



[Meet the Rest of the ACE Team](#) ✨



Find us on [LinkedIn](#) ✨