



Dental Defense:

Fortifying Your Practice Against Cyber Threats



Monica Martinez
VP of Sales - HTI



Jim Gochis
EVP of Procurement-
Synergy Dental Partners



Cybersecurity attacks are
inevitable. Breaches and
Ransomware are not!

Agenda

- Introduction to High Tech Innovations (HTI)
- What is Ransomware and how is it different from a Breach?
- How Common are Ransomware Attacks?
- Real-world examples of ransomware impacting dental practices
- How Does Ransomware Affect Your Business?
- How Do I Know If My Office is a Victim?
- What to Do If Your Dental Office Gets Hacked
- How to Mitigate Your Vulnerability to Ransomware

High Tech Innovations

Backed by over 27 years of dental IT expertise and proven certifications, HTI delivers first-class IT services to dental practices. We've helped hundreds of offices achieve optimal IT performance and security to focus on what matters most -their patients



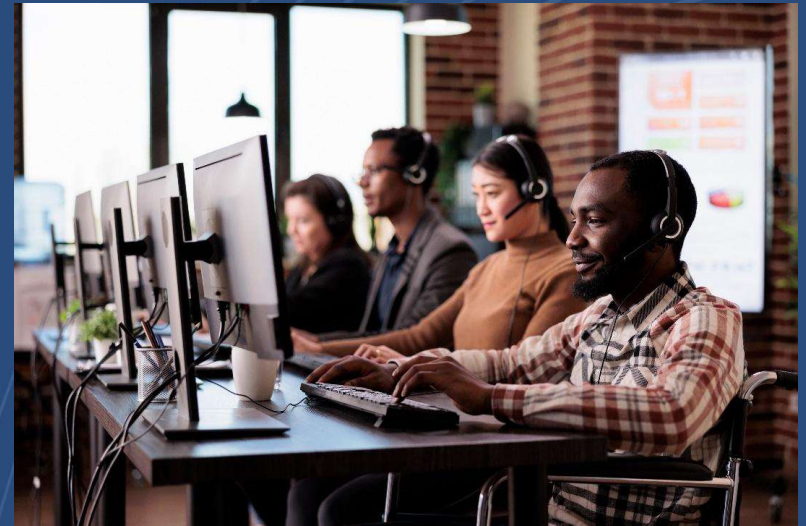
Services Provided

Support (Remote and Onsite)
Monitoring and Maintenance
Cloud based backup
Disaster Recovery
Network Security Services
Vendor Management
Cybersecurity Training
Integration
Computers and Installation
And More



WHAT IS A BREACH?

A security breach is any incident that results in unauthorized access to computer data, applications, networks or devices. It results in information being accessed without authorization.



WHAT IS RANSOMWARE?

To deny access to a device or file until a ransom has been paid



WHAT IS RANSOMWARE?

- A cyber attack with ransomware means an office can lose everything – patient records, clinical files, sensitive data, financial information and practice reputation – in an instant.
- Dental offices are not immune to cyber attacks. In fact, they are a prime target! Cybercriminals are counting on dental offices to have less stringent security measures in place compared to other healthcare entities. Hackers know that one unintentional miss-step from only one employee could make the entire network vulnerable.



CYBER ATTACK COSTS ARE HIGH

- The **average cost** of a data breach in the healthcare sector, including dental practices, was estimated to be around **\$7.13 million in 2023**, a significant increase from previous years. This includes fines, legal fees, credit monitoring services for affected patients, and loss of business due to reputational damage.
- As an example, for a typical 6 office DSO, the ransom is in the range of **\$200,000 to \$600,000**.
- The increase in cyberattacks has led to a more stringent regulatory response, with the OCR enforcing stricter penalties for HIPAA violations resulting from these breaches. In 2023, fines for non-compliance in reported cases ranged from **\$50,000 to over \$1 million**, depending on the severity and scale of the breach.

CYBER ATTACK COSTS ARE HIGH

Penalty Tier	Culpability	Minimum Penalty per Violation	Maximum Penalty per Violation	Annual Penalty Cap
Tier 1	Lack of knowledge	\$137	\$34,464	\$34,464
Tier 2	Reasonable cause	\$1,379	\$68,928	\$137,886
Tier 3	Willful neglect (corrected within 30 days)	\$13,785	\$68,928	\$344,369
Tier 4	Willful neglect (not corrected within 30 days)	\$68,928	\$68,928	\$2,067,813

CYBER ATTACK COSTS ARE HIGH

The Ransom is just the beginning...

- Downtime
- Forensic Investigation
- HIPAA Fines
- Network Restoration
- Credit Monitoring and Repair
- Reputation Hit



HOW COMMON IS RANSOMWARE?

- Rising Incidence of Cyberattacks: According to a report by the American Dental Association, there was a **noticeable uptick** in reported cyber incidents targeting dental offices in 2023.
- Phishing Attacks: The incidence of phishing attacks in the dental sector saw a **40% increase in 2023** compared to the previous year. These attacks often serve as entry points for more damaging exploits, such as ransomware.
- Breaches stemming from hacking which include malware, ransomware and phishing attacks, have soared over the past decade, making up 80% of reported breaches last year. Ransomware attacks have been particularly damaging with the **average ransom demand exceeding \$50,000**.

Patient records exposed in data breaches doubled in 2023

In 2023, more than **112 million** individuals were compromised in healthcare data breaches reported to the HHS Office for Civil Rights (OCR), **48.6 million** impacted individuals in 2022.



FBI Warns Dental Offices on May 7, 2024

FBI warns of cybersecurity threat targeting oral surgery practices

♥ f t in ▶ tT 🖨 ✉
Save Post Tweet Share Listen Text Size Print Email

The FBI issued a warning to the American Dental Association and the American Association of Oral and Maxillofacial Surgeons regarding a credible cybersecurity threat.

The group behind the attacks is threatening to target oral surgery practices, but the FBI believes general dentistry and other specialty practices could be targets in the future, according to a May 7 news release from the ADA.

Attackers often use social engineering scams including phishing, smishing and vishing to gain access to protected health information.



Cyber Insurance Claims Reached Record High in 2023

Record numbers of cyber claims were filed against insurance policies in North America in 2023, according to a recent analysis by the insurance broker Marsh. Last year, more than 1,800 claims were filed with the company from clients in the United States and Canada, more than any other year to date.



Multifactor Authentication Could Have Prevented 9.7 Million-Record Medibank Data Breach

Like the attack on Change Healthcare, the 9.7 million-record data breach at the Australian health insurance provider Medibank could have been prevented if multifactor authentication had been enabled. Medibank was alerted to the security risk two years before the hack.



Cyberattack on Minnesota Radiology Practice Affects 512,000 Patients

The personal and protected health information of almost 512,000 individuals has been exposed in a cyberattack on the Edina, MN-based radiology services company Consulting Radiologists.



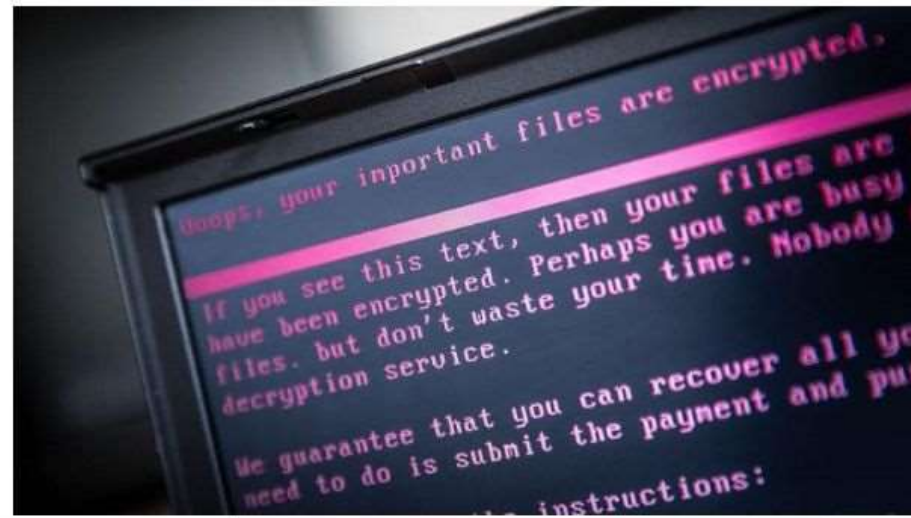
Ransomware Attack Hits 400 Dental Offices Across the US

The attack struck on Monday morning and targeted The Digital Dental Record, a provider of IT software to dental offices. Reportedly, 400 dental practices have been affected nationwide.



By Michael Kan August 29, 2019 12:56PM EST

[f](#) [t](#) [in](#) [p](#) [v](#) [e](#) [m](#) [l](#) [64 SHARES](#)



CHANGE HEALTHCARE

On February 21, Change Healthcare was impacted by a cybersecurity incident that has sent waves through the healthcare industry. Medical and dental providers across the country have experienced disruptions from the cyberattack which took down parts of the company's system. Change Healthcare is one of the largest revenue and payment cycle management providers in the US healthcare system.

The disruption has primarily affected healthcare providers from obtaining insurance approval for procedures leading to delays in claims and insurance payments.

ASPEN DENTAL

Aspen Dental

Thousands of Dental Practices Experience Cyber Attack

05/05/2023 by Oral Health



HOW COMMON IS RANSOMWARE?

- A ransomware attack at Southeastern Minnesota Oral & Maxillofacial Surgery (SEMOMS) last September risked data for an estimated **80,000 patients**.
- A Delta Dental of Arizona employee fell victim to an e-mail-based phishing scam that compromised nearly **13,000 people's** identifying information.
- Affected clinics of an Alabama not-for-profit provider of children's optical and dental services were closed for two weeks after a ransomware attack exposed more than **390,000 patient** records.

HOW COMMON IS RANSOMWARE?

Grove Dental Associates' data breach notice was published on its website. Personal Patient information was accessed by an unauthorized person between March 31 and April 1, 2021, as the result of an email phishing incident.

"The full extent of the potentially affected personal information is not yet known and will vary between persons, but it may include the following: name, address, email address, phone number, dental information, insurance information, Social Security Number, and/or financial account numbers."

The breach was reported to the DHS's Office for Civil Rights, impacting **125,760 patients** in Connecticut, Florida, Georgia, Illinois, Indiana, Massachusetts, Michigan, New York, Texas and Tennessee.

HOW COMMON IS RANSOMWARE?

- **A small 6 practice DSO** was a victim of ransomware, and the demand was **\$2.4 million** to release the decryption key for the practices to recover their data. The ransom demand was only a portion of the cost of this attack. All 6 locations had to rebuild/replace their office networks and all 6 had to lock their doors for 10 business days
- Dallas-based Jefferson Dental & Orthodontics experienced a data breach affecting more than 1 million patients, CBS DFW reported March 18. The DSO which has 72 locations throughout Texas. Up to **1,026,820 patients** could be affected by the breach. This is the largest data breach to be reported to the state's Attorney General since a new state law was enacted Sept. 1, 2021 requiring companies to report data breaches affecting 500 or more Texans.

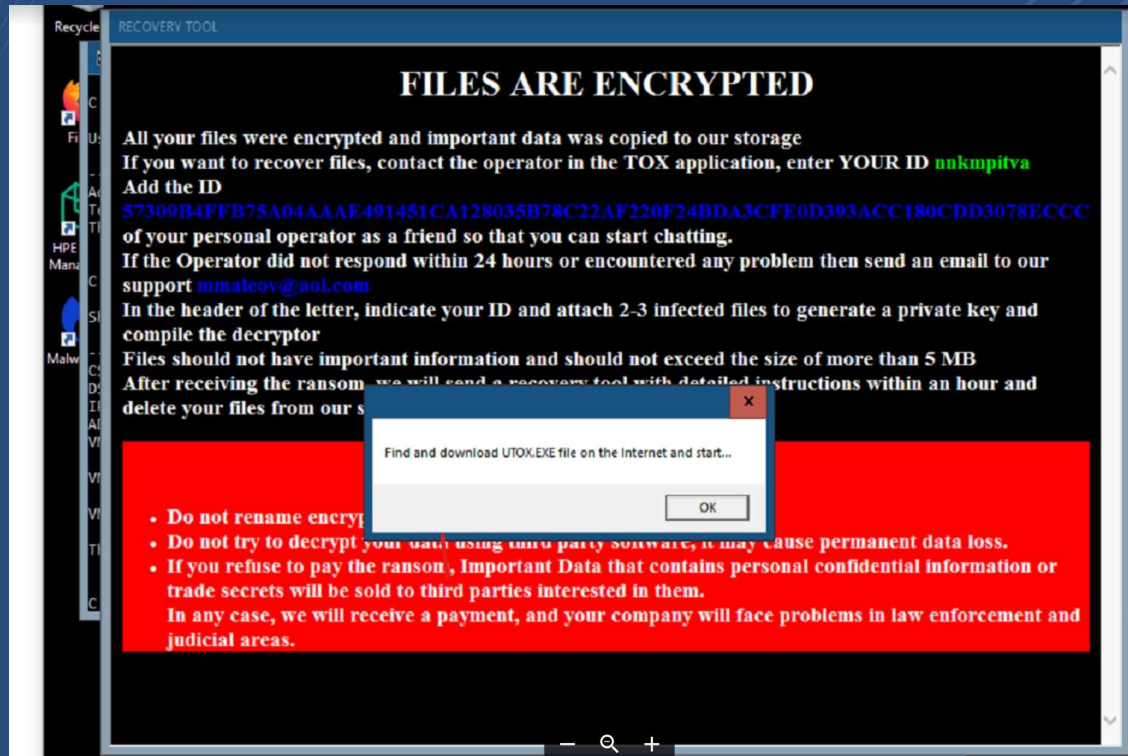
HOW COMMON IS RANSOMWARE?

Over 100 dental practices were victims of a Sodinokibi ransomware attack on November 25, 2019, in Colorado. The cyberattackers issued a **ransomware demand of \$700,000** to provide decryption keys.

A number of the affected practices were able to recover data from their backup data that was securely stored offsite. However, many of the affected dental practices remain without access to systems or data. These practices have been forced to turn patients away because of ongoing system outages stemming from the attack.

Some of the dental practices attempted negotiating with the attackers to obtain the keys needed to unlock their own data. **However, even those practices that paid a ransom have recovered only a portion of their encrypted data.** As a result, these covered entities have had to pay additional money for additional keys to unlock the encrypted files. **One dental practice, which had 50 encrypted devices, received over 20 ransom notes. As a result, the practice had to make multiple payments to recover patient records.**

Real Ransom Attack Alert in Dental Office



How do I know if I am a victim of Ransomware?

- Loss of access to common files or “corrupted” message.
- Warning message of file lock.
- Countdown Clock with Instructions.
- Unfamiliar Open Window that can’t be closed.
- All Files have been replaced with

HOW_TO_DECRYPT_FILES.TXT

DECRYPT_INSTRUCTIONS.HTML

Steps to follow if hacked

Infected systems should be removed from the network within **20 seconds** to prevent ransomware from attacking the network or share drives.

The sooner you remove the infected machine from network, the less likely other machines are to become infected.

Steps to follow if hacked

- Do not shut down PC, instead, pull the power or network cable.
- Unplug **all wired devices**
- Disable and Unplug **all wireless devices**
- Don't run any "clean-up" programs
- Don't erase anything
- Determine workstation zero
- Call IT provider
- Do nothing else



How to Protect Yourself

Purchase Cybersecurity
Insurance



How to Protect Yourself

Create a Multi Level Plan



HTI SECURITY STANDARDS

- EDR- Endpoint Protection
- Advanced-Threat Firewall
- Cloud Connect- Image Backup

HR TRAINING

- Cyber Smart Training
- Centralized Email

PROACTIVE CYBER SECURITY

- Vulnerability Management

How to Protect Yourself

Create a Multi Level Plan



CYBER SMART TRAINING

- ✓ Weekly Micro Training Video
- ✓ Phishing Testing
- ✓ Personal Dark Web Email Scan
- ✓ Security Risk Assessment
- ✓ Continuous Dark Web Monitoring
- ✓ Policies & Procedures
- ✓ Annual Training Course

Cyber insurance provides often
Require employee cyber security
Awareness training to reduce risk &
qualify for coverage.

How to Protect Yourself

Create a Multi Level Plan



VULNERABILITY MANAGEMENT

Steps:

1. **Identification:** Regularly scan for vulnerabilities using specialized tools.
2. **Prioritization:** Assess the severity, exploitability, and criticality of each vulnerability.
3. **Remediation:** Patch software, configure security settings, or implement additional controls.
4. **Reporting:** Track and document vulnerabilities and their remediation efforts

How to protect yourself in the future

**How to
Recognize
a Phishing
Scam?**



How to protect yourself in the future



- Recognize Phishing Scams
 - The “SLAM” Method
- Practice Makes Perfect
- Password Sophistication
- Common Sense Social Media

Recognize Phishing Scams by using “SLAM” Method



Sender

Check the sender closely. Look for misspelled domains, or a completely different email address than the name of the sender. Ultimately, if you don't recognize the sender, proceed cautiously and don't open attachments. Also, look for multiple recipients on email.



Links

Hover over (but don't click) on any links and avoid clicking on any links that you don't recognize.



Attachments

Don't open attachments from anyone that you don't know and be suspicious of attachments from people that you know but weren't expecting.



Message

Check the subject line and body for suspicious language, misspelled words, and bad grammar.

Attackers Rely on Emotional Issues

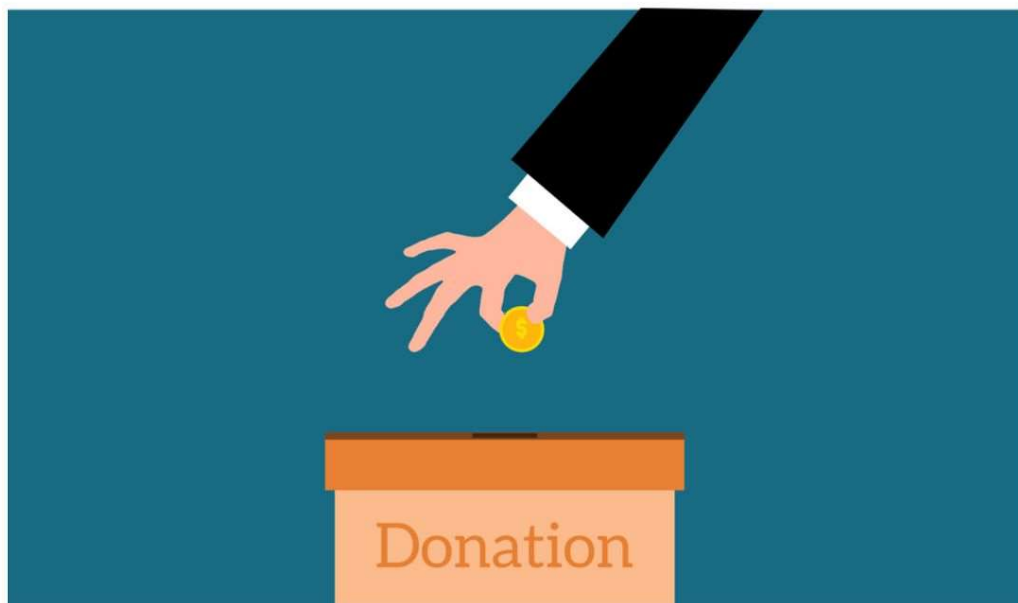
- War in Israel
- Ukrainian Crisis Aid
- Covid Vaccine Appointments

Spam trends of the week: Spammers piggyback on the Israel-Gaza war to plunder donations



Alina Bîzgă
October 16, 2023

Promo Protect all your devices, without slowing them down.
[Free 30-day trial](#)



TOP POSTS



SCAM • SPAM

Spam trends of the week:
Crypto giveaways, false prophets, Fintech phishing...

April 19, 2024 • ⌚ 5 min read • 📌



SCAM • HOW TO • TIPS AND TRICKS

Start Cyber Resilience and Don't Be an April Fool This Spring and Beyond

April 01, 2024 • ⌚ 2 min read • 📌



SPAM • INDUSTRY NEWS • THREATS

Spam trends of the week:
Cybercrooks phish for QuickBooks, American Expre...

November 28, 2023 • ⌚ 4 min read • 📌



PROTECTING YOUR IMPORTANT • HOW TO • TIPS AND TRICKS

Protecting your important:
Stick to these 8 cybersecurity

Ukrainian Crisis

Ukraine Humanitarian Donation



From [Ukraine / Україна Govt](#) on 2022-02-28 15:19

[Details](#) [Plain text](#)

A donation campaign has been launched to support Ukraine and also help refugees fleeing the conflict in Ukraine. The campaign, organized by the humanitarian organization Act for Peace, is hoping to raise \$9,000,000 to support refugees in the region.

Stand with the people of Ukraine. Now accepting cryptocurrency donations. Bitcoin, Ethereum, USDT and NFT

BTC- `bc1qqglytupu8pup07eksh3gd77edkd3ge7ku6809y`

ETH- `0x5535480a9D0F39b545F9c14b0a70a8755237b01f`

Best Regards

Ukraine

#BeautifulUkraine



[Help Ukraine](#) [Home](#) [Donate](#) [Latest donations](#)

What happened to Ukraine?

Ukraine was viciously invaded by Russian troops on 24/2/2022 for the president's personal philosophy and gains. They have mercilessly targeted our people and our infrastructure without any regards to human life. We as a country request you for your support and prayers so that we can survive this war.



Want to donate?

Each donation helps tremendously for our war efforts to keep our people safe and ready to defend ourselves from the Russian aggressors.



Help with Bitcoin

If you want to help Ukraine, please send any amount on the address below. Thank you!

`bc1q7zzvpawk27r8m7ayv5dw2fyxuc2hdcffwaj`

Last donation 1 hours ago



Help with Ethereum

If you want to help Ukraine, please send any amount on the address below. Thank you!

`0x75Ac412E99C864c830C48E222aC88E88A648cE`

Last donation 7 minutes ago



Help with USDT (ERC-20)

If you want to help Ukraine, please send any amount on the address below. Thank you!

`0xaB353ac000C946E9F2caDccE8C756b878003984`

Last donation 8 minutes ago



Help with Litecoin

If you want to help Ukraine, please send any amount on the address below. Thank you!

`Lt6trj2jmeE3rH9p6n2htF8J6wtpyGX`

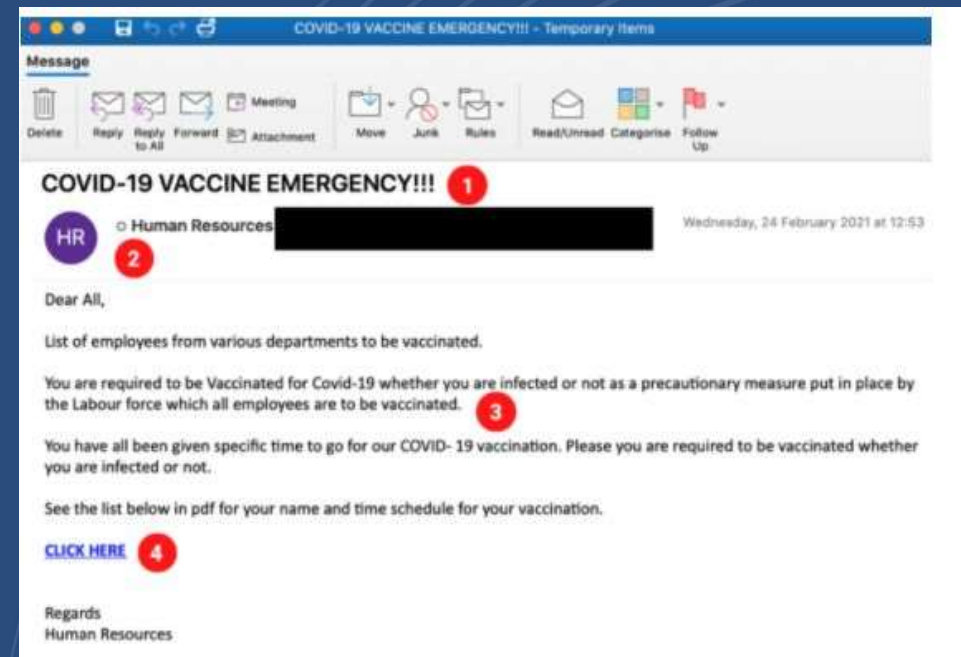
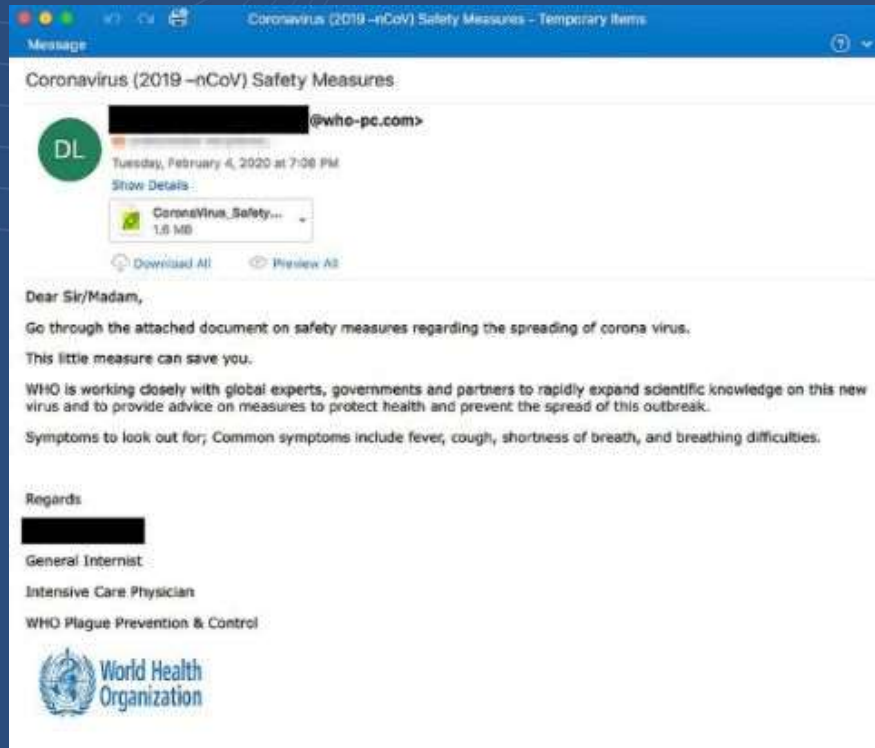
Last donation 9 minutes ago

Latest donations

All latest donations will be shown on random order for the privacy and safety of the donors. Thank you for helping us through these dark times!

Donation with amount of 101\$ to the address `bc1q7zzvpawk27r8m7ayv5dw2fyxuc2hdcffwaj`. This transaction hash is `0a3225cb67932...`
1 minute ago

Pandemic



Tennessee dental practice hacked

Oak Ridge, Tenn.-based Core Dental Health's system was recently [hacked](#), potentially exposing patient information.

An unauthorized individual gained access to the practice's system March 14, 2024 and began making configuration changes, according to a July 1 news release. The practice said it became aware of the incident April 24 after its IT provider noticed abnormal activity. An investigation into the incident determined that the individual gained access to a data folder containing sensitive information and patient information.

Data that was accessed during the hack may include names, dates of birth and possibly dental treatment history. It may also include the social security numbers of some patients under Medicaid.

The practice said the FBI is currently investigating the incident and that it is working with a cybersecurity consultant. It also implemented enhanced security measures to help prevent other future incidents.

Core Dental Health [submitted](#) the incident to the U.S. Department of Health and Human Services Office for Civil Rights Breach Portal July , 2024. The breach portal states that the cyberattack affected 2,349 individuals.

Smishing Attacks

Smishing can be a big problem especially if the person's phone is connected to the internal private office network. Especially bad if they use an Android phone.



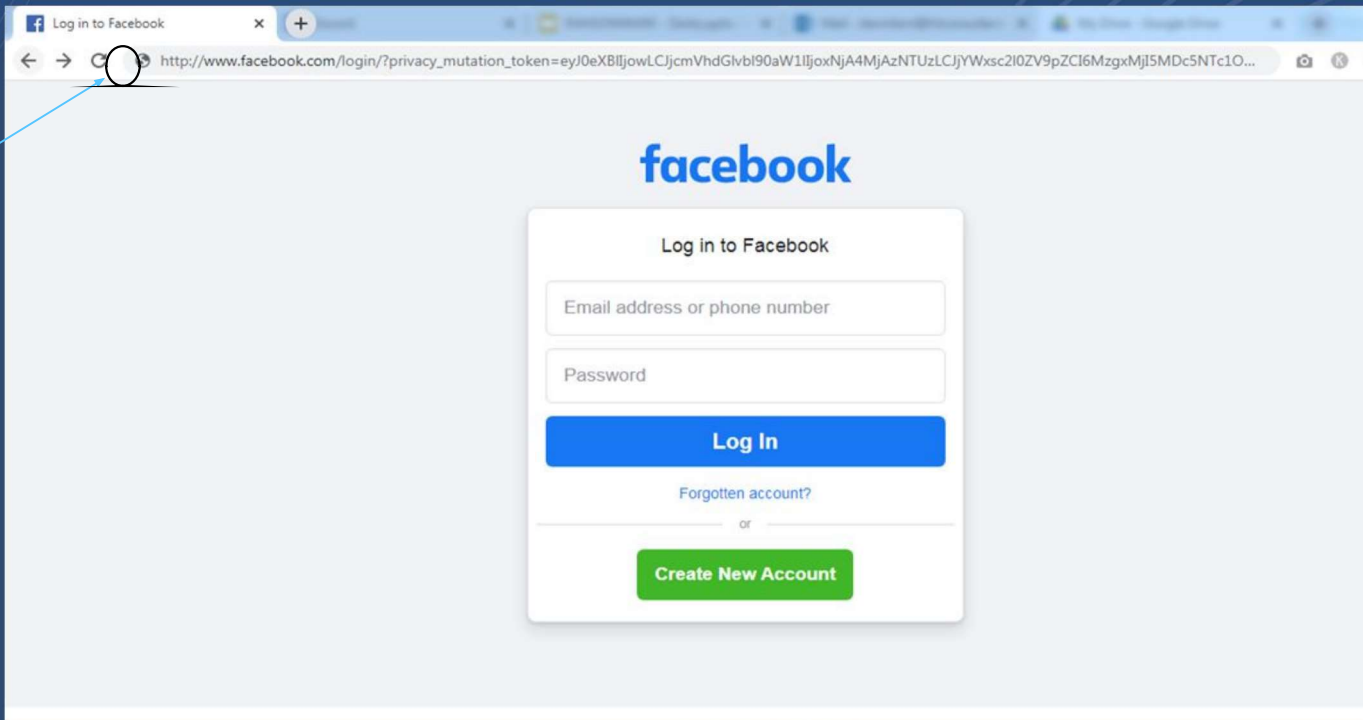
QR Code Attacks



Recognize Phishing Scams

- Bad URL, no “https”
- Bad “From” Address
- Misspellings or Bad Grammar
- Threat of Consequences

Bad URL- no “https”

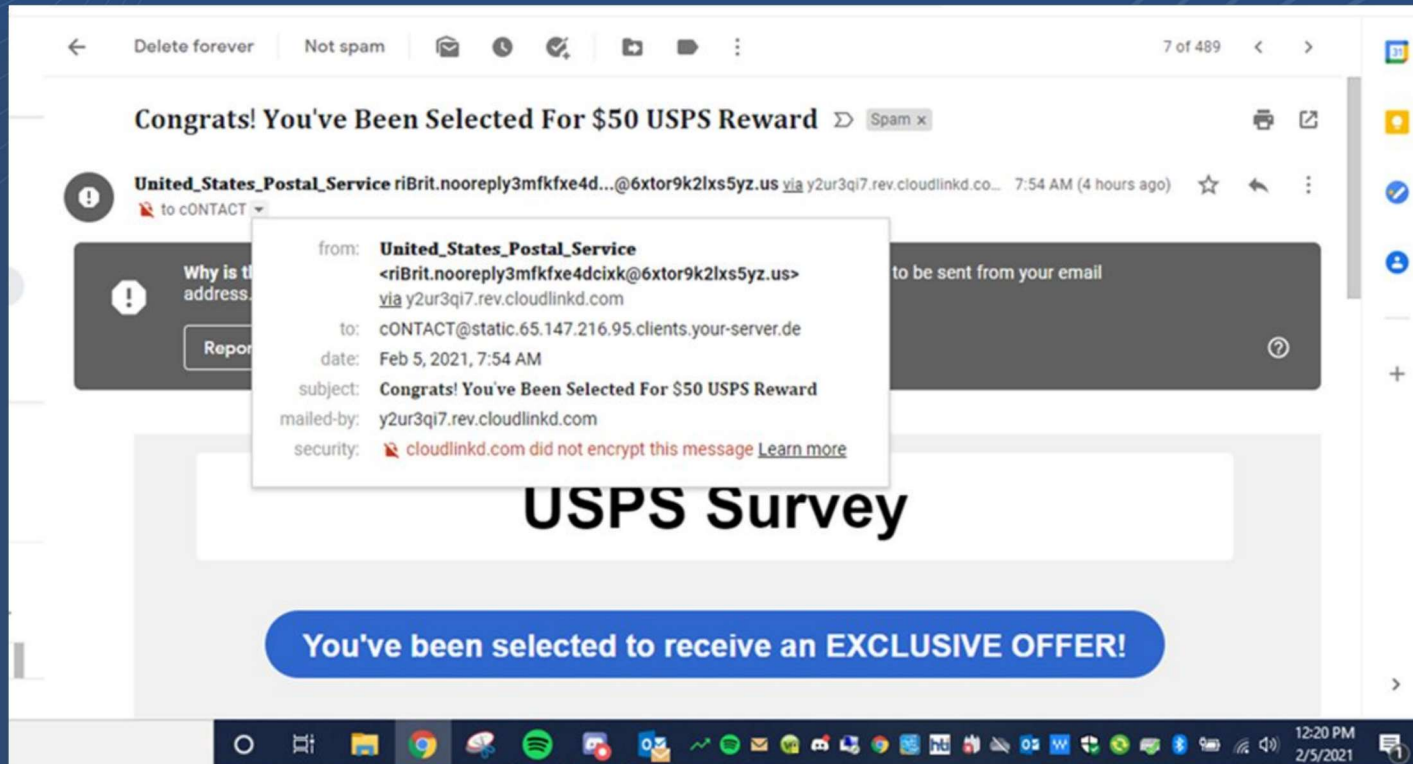


http://

Bad URL- no “S” - “https”




Bad “FROM” email address



Misspellings and Poor Grammar

From: MSteam-Outlook Message Center <no-reply@office365protectionservices.co.uk>
Sent: 19 September 2018 11:44
To: Bob Smith <Bob.Smith@Company.com>
Subject: Account Verification

This mail is from a trusted sender.

 Outlook

Threat
We're having trouble verifying your Office365 account: Bob.Smith@Company.com on our server, most features will be turned off.
To help prevent account malfunctions, please log into your account portal to verify your account.

Spelling mistakes
[SIGN IN TO MICROSOFT ACCOUNT PORTAL](#)

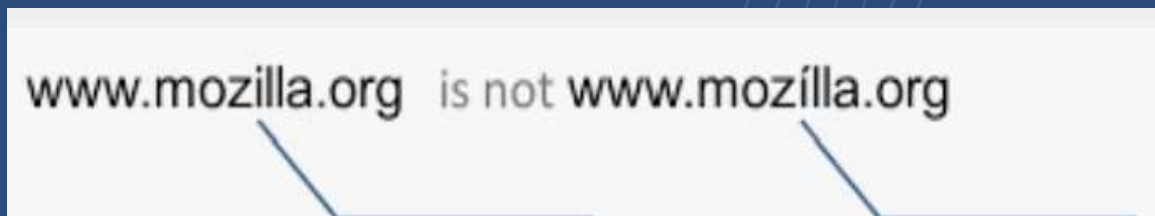
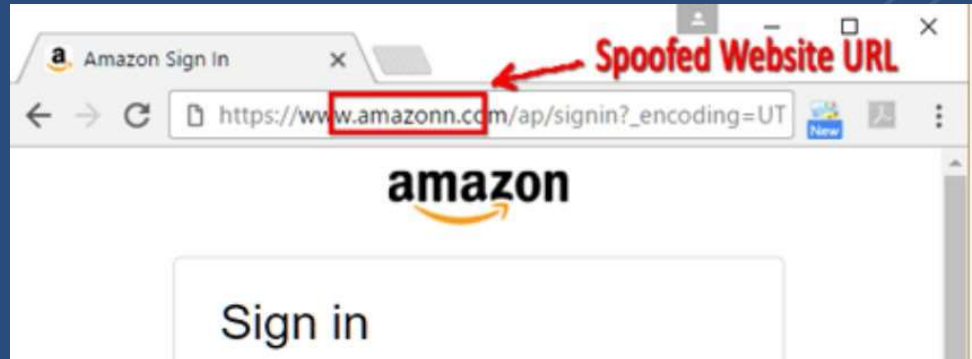
Note : Outlook will automatically fix your account after this process on the microsoft server and all account features will be turned back on

Thanks for using office365 , we hope to continue serving you.

Microsoft Corporation
One-Microsoft Way Redmond
WA, 98052
All Right Reserved | Acceptable Use Policy | Privacy Notice

Grammatical errors
Fake email signature

Visual Website Spoofing



Correct
Spelling

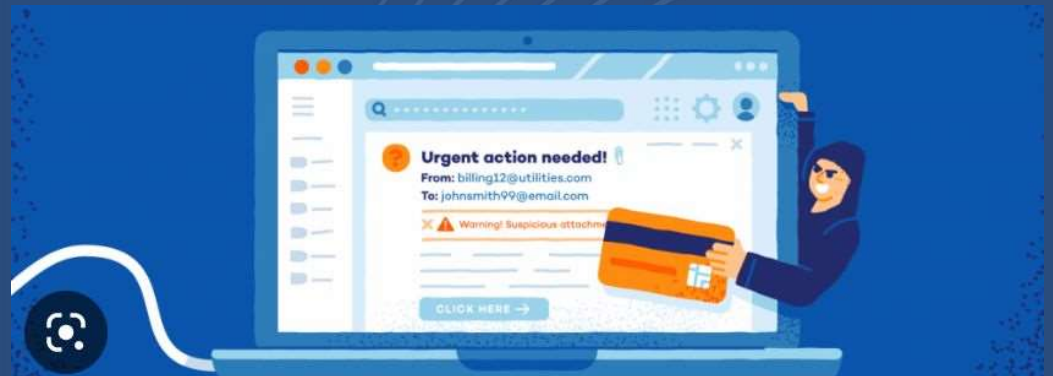
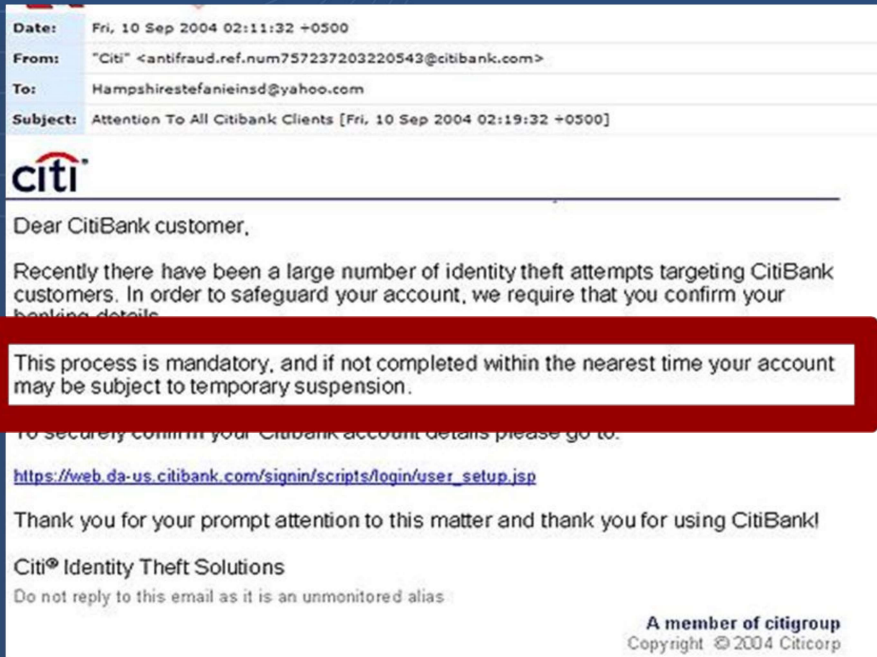
See the difference?

Visual Website Spoofing

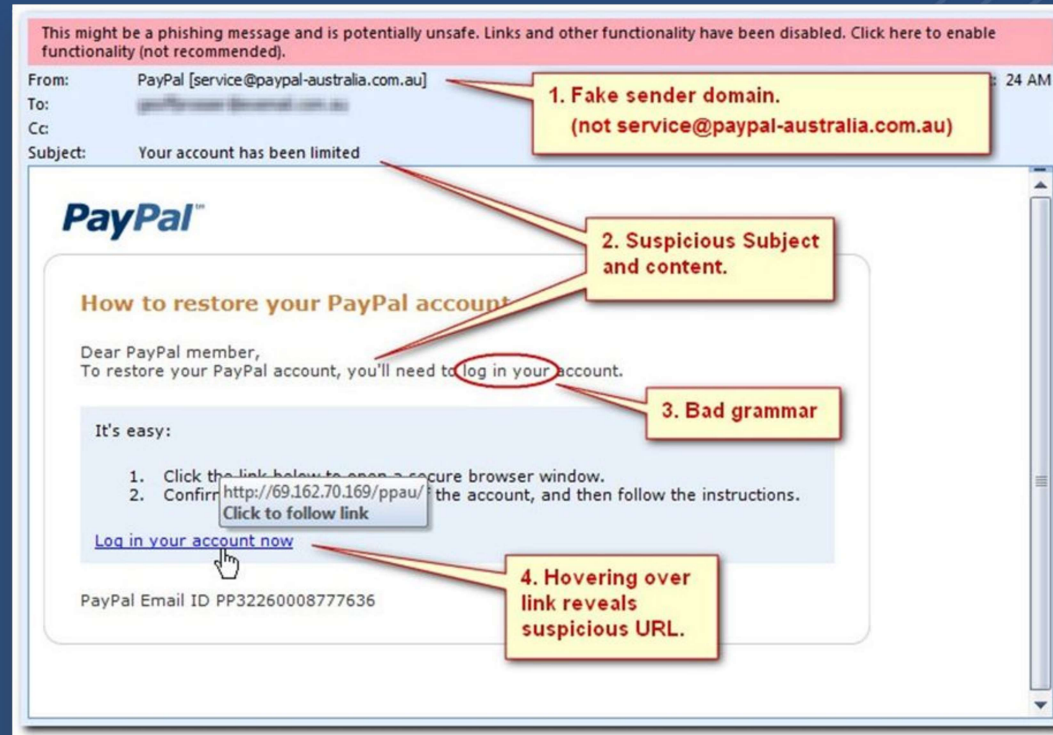
|WWW.G00GLE.COM

|WWW.YOUETUBE.COM

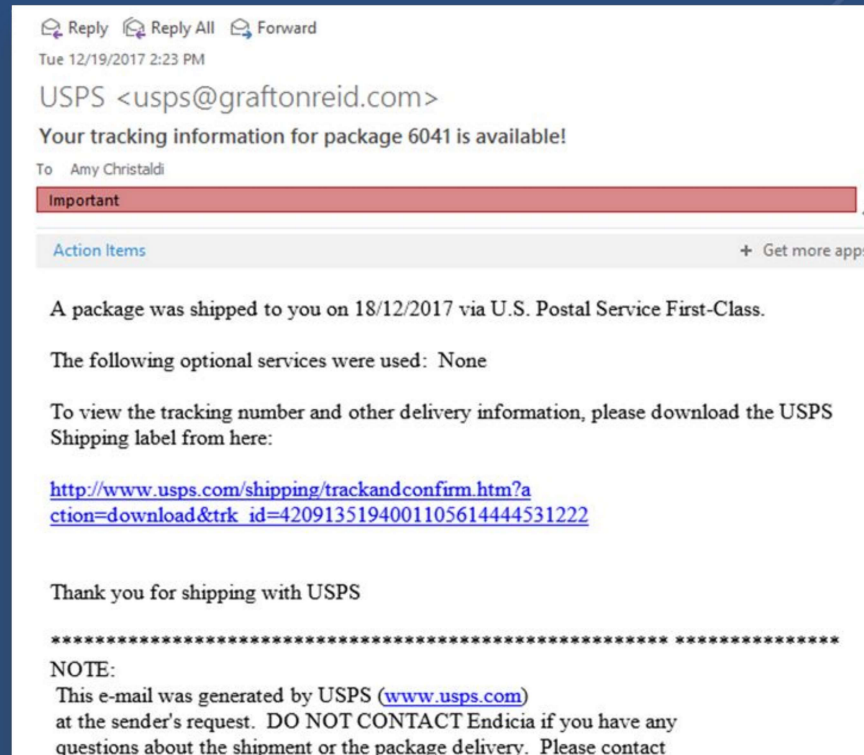
Call to Action or Threat of Consequences



Additional Examples



Additional Examples



Additional Examples



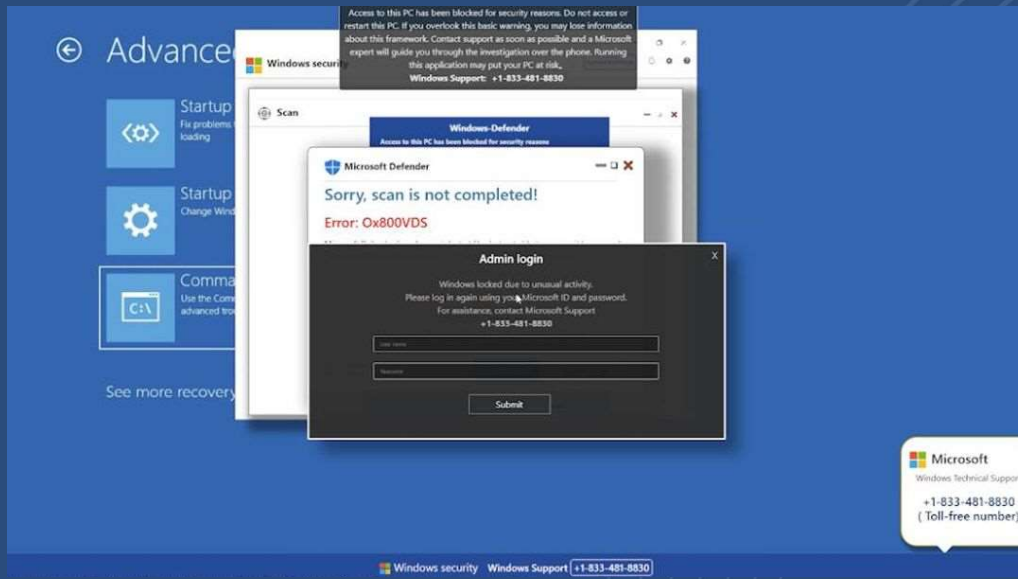
Make Sure to Hover Over Link!

We need to verify y

www.yourbank.com

www.ThisIsNotYourRealBank.com
Click or tap to follow link.

Do Not Fill In Private Info Requested in an Email/Text



Reach out to requesting company directly

Beware of Surveys!

HSBC 

We welcome your feedback on our HSBC website.

Thank you for taking the time to complete the survey. It will take about few minutes.
Your feedback will help us improve our websites.

1. Based on your experience with HSBC website today, how would you rate your overall satisfaction with our website?

☐ 5 – Highly Satisfied
☐ 4 – Quite Satisfied
☐ 3 – Neutral
☐ 2 – Not Quite Satisfied
☐ 1 – Not Satisfied at all

2. What is the purpose of your visit today (please select all that apply)?

☐ Look for information about HSBC
☐ Look for promotions
☐ Login to HSBC iBanking
☐ Apply for products
☐ Get in touch with the bank
☐ Find some research articles
☐ Others, pls specify

FAKE

More Tips To Remember

- Avoid FireFox (AKA Mozilla)
- Avoid using personal machines - LTW
- Employ 2 Factor Authentication (2FA)
- Multi Factor Authentication (MFA)
- Find a good blog or newsletter
- Appoint a Cyber Security Czar
- If it looks suspicious don't open it!!
- Call the institution
- Everyone connects to the guest network!
- Avoid freeware!!

Proper Passwords

- 8 Characters is the minimum suggested length.
- 16 Characters is the recommended length.
- A mix of numbers, letters and characters.
- The more complex the better!
- Use a Passphrase!
- Do not use Google to store passwords
- Last Pass is a good Password Manager

Time it takes a Hacker to Brute Force your password

@coders.bro

Numbers of Character	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 Secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100tn years	7qd years

Are you in green zone?

Think Before You Post



Other Threats to Think About

THREATS TO DENTAL PRACTICES

Middleware: Dental practice use middleware, for example, to connect their appointment software with their billing system.

- Do you utilize any third-party vendors for services billing, accounting or appointment scheduling?
- Have you conducted security assessments or reviewed the security practices of these vendors?
- Do you have contractual agreements in place with these vendors outlining their data security responsibilities?

Who has access to your
Server and network?

Vet Your Current IT Provider

Ask them

- Who backs you up?
- Who is watching my environment?
- Are you independently audited?
- What do you use for your Cybersecurity?

Vet Your Current IT Provider

When it comes to Network Security

- Are my Windows Updates being done?
- Is my AV and AM being updated?
- Are my EP's protected? (Not just the server)
- Is my firewall up to date?

Vet Your Current IT Provider

When it comes to Ransomware

- Am I Protected from Ransomware?
- With what?
- What does it do in the event of an attack?

Vet Your Current IT Provider

When it comes to back-ups

- Am I backed up?
- Where do they go?
- Are they monitored?
- Image level or file level?
- How quickly can you restore me?



More Partners
More Value
More Savings



Since 2010, Synergy has helped thousands of dentists like you save millions by negotiating deeply discounted prices on dental supplies and services.

- Up to 75% OFF supplies & services with Synergy's large Partner Network.
- 25% SAVINGS or more on top quality labs.
- SAVE EVEN MORE when you order using your FREE Method Online e-Procurement Membership (\$69 value).
- FREE shipping on all orders through Darby.
- FREE & discounted educational offers.
- Additional monthly & quarterly promotions from our partners.
- Maximize your savings using the Synergy Member Portal.





Call Now & Find Out How Much
You Can Save with **Synergy!**

**TED OSTERER - VICE
PRESIDENT OF SALES**

516-316-3671
tosterer@thesynergyp.com

THE SYNERGY DENTAL PARTNERS.COM
INFO@THESYNERGY DP.COM | 888-810-2995



THANK YOU FOR YOUR TIME!



Monica Martinez

VP of Sales, HTI



monicam@hticonsultants.com



609-306-0741



www.hticonsultants.com



**Contact HTI for a Free
Cyber Consult today!**

(877) 222-1508 #5 | connect@hticonsultants.com