Protecting patient data from cybercriminals

By Anne Genge, CIPP/C, CHSP, CHSRAS
Dental cybersecurity speaker/educator

It starts with one click. An email arrives in your inbox, a seemingly routine message from a vendor, a patient or a colleague. A single click on a malicious link or attachment is all it takes to unleash a cyberattack, locking you out of your systems, stealing your data and holding it hostage until a sum of money is paid. This type of attack is called ransomware, and it is the most common cyberattack in the dental industry today.

For oral and maxillofacial surgeons – whose practices depend on uninterrupted access to digital tools like patient records, imaging systems and scheduling software – ransomware is not just a tech problem; it poses an operational and revenue crisis.

What is ransomware?

Ransomware is a type of malicious software (malware) that encrypts the victim's data, rendering it inaccessible. In this type of attack, cybercriminals use encryption against their victims. Encryption was originally designed to protect data by scrambling it and making it unreadable except to those with a special key (a long password). The attackers encrypt your data, then demand payment – often in cryptocurrency – in exchange for a decryption key to unlock your files. Imagine your entire office is locked by an unbreakable digital padlock, and the only key is held by criminals demanding a ransom.

Cybercriminals have now taken ransomware to the next level by threatening to release a victim's data on the dark web if the victim doesn't pay. This tactic, known as double extortion, increases pressure on victims by exposing them to potential HIPAA violations, lawsuits and reputational damage, even if they have data backups.

Extorting patients directly

In the United States, cybercriminals have increasingly targeted patients directly following breaches of healthcare systems. Notable instances include:

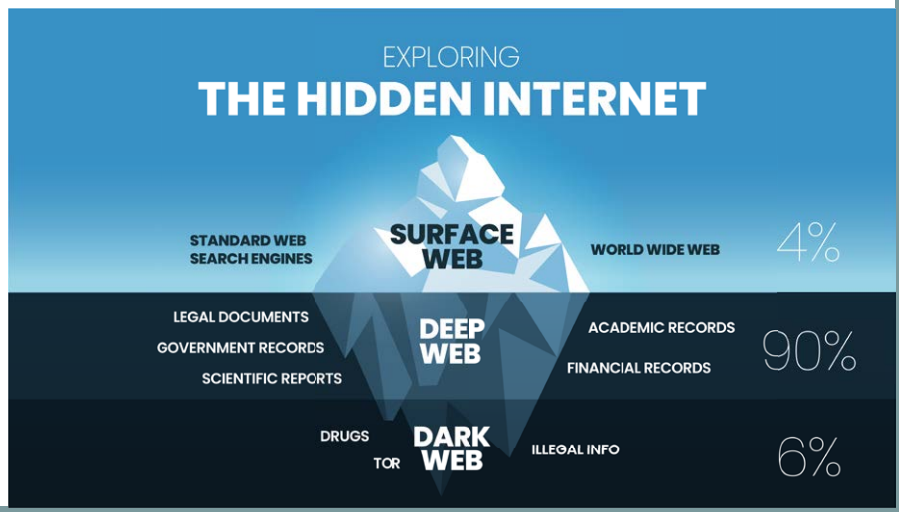
- **Fred Hutchinson Cancer Center (Seattle)** – After a cyberattack, patients received emails from hackers threatening to release their personal information unless a ransom was paid.[1]
- **Integris Health (Oklahoma City)** – In 2023, a cyberattack compromised data of over two million patients. Subsequently, patients received extortion emails demanding payment to prevent the sale of their personal data on the dark web.[2]

These incidents reflect a troubling trend in which cybercriminals, facing improved cybersecurity defenses from healthcare providers, resort to directly extorting patients to maximize their illicit gains.

What is the dark web?

When stolen data is leaked, it often ends up on the dark web, a hidden part of the internet where cybercriminals operate anonymously. Think of the dark web as an underground black market where everything from personal information to illegal goods is bought and sold. Patient data, names, Social Security numbers and medical histories are especially valuable to criminals because they can be used for identity theft, fraud and other nefarious outcomes.

continued on next page



How do ransomware attacks happen?

The most common entry point for ransomware is through email phishing attacks. According to Stanford research, 88 percent of breaches are caused by human error,[3] and according to Varonis, over 94 percent of malware is delivered via email.[4] AI-generated phishing emails and tactics add to the challenge of keeping dental practices safe.

Here's how ransomware often unfolds:

1. A staff member receives an email disguised as a legitimate message from a trusted source.
2. The staffer clicks a link or opens an attachment, unknowingly downloading ransomware.
3. The ransomware spreads through the network, encrypting files and locking systems.
4. The business is asked to provide a ransom fee to gain access to locked data.

Cybercriminals also may steal data and demand a ransom not to publish the information on the dark web. In certain cases, they have even tried to extort patients directly.

It is important to know that phishing attacks can happen via text, websites, phone and social media. Security awareness training is an important part of cyber resilience and prevention.

Real-world impacts of ransomware

A dental practice fell victim to ransomware when an employee clicked on a phishing email. Within minutes, the attackers locked the system and demanded $71,000 in ransom. Despite paying, recovery was slow, some data was lost and the practice incurred additional costs for forensic experts and cybersecurity upgrades. Some practices, like Wood Ranch Medical,[5] have even gone out of business due to insufficient backups.

For oral and maxillofacial surgeons, downtime doesn't just mean canceled appointments, it means canceled surgeries, loss of revenue and potential risks to patient care. Recovery from such an attack can take weeks, during which a practice may hemorrhage money and lose trust with patients and referring dentists.

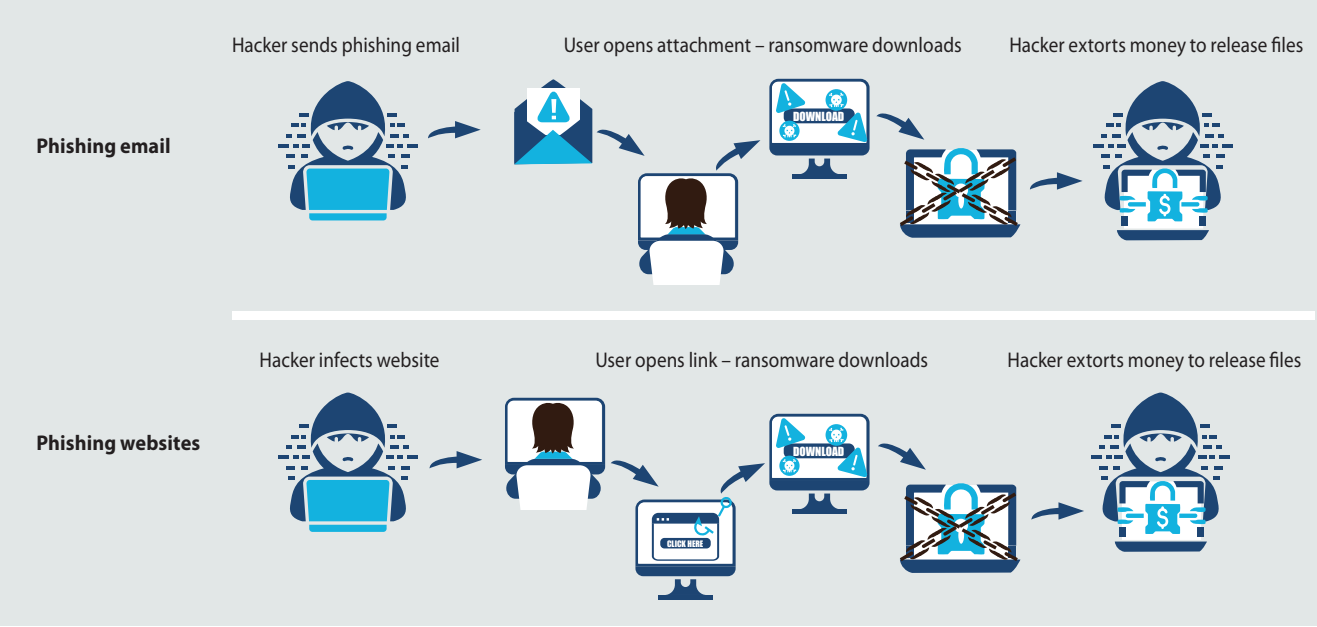
Although not specifically coined as a ransomware attack, another example of how easily things can go bad occurred last year when a New Jersey OMS practice reported a data breach affecting over 74,000 individuals. After the breach

A hypothetical example of a dental office phishing email.

was detected, an investigation showed that unauthorized access went back nearly one month. Compromised information included patient names, Social Security numbers, birth dates, addresses, driver's license numbers, medical and health insurance details and financial account information.

The incident highlighted areas for improvement including:

- **Prompt detection and response** – The breach went undetected for nearly a month, highlighting the need for continuous network monitoring to identify and address suspicious activities swiftly.
- **Comprehensive data protection** – The exposure of sensitive personal and medical information underscores the importance of robust encryption and access controls to safeguard patient data.
- **Regular security assessments** – Conducting routine security audits can help identify vulnerabilities, ensuring that protective measures are up-to-date and effective.
- **Employee training** – Educating staff on cybersecurity best practices can reduce the risk of breaches caused by human error or social engineering attacks.
- **Transparent communication** – Notifying affected individuals and relevant authorities promptly is crucial for maintaining trust and allowing individuals to take protective actions.



Possible ways a hacker can use ransomware.

- **Proactive measures** – Implementing additional safeguards post-incident is essential, but proactive measures are vital to prevent breaches from occurring.

Other considerations to protect a practice

Preventing ransomware and other cyberthreats requires a combination of technology, training and proactive planning. Most practices need professional experts to design and execute a comprehensive cybersecurity strategy. Here's how to get started:

- **Use email security filtering to minimize inbound threats.** Deploy advanced email filtering tools that automatically block spam, phishing attempts and malicious attachments before they reach your inbox. Choose a solution that integrates seamlessly with your existing email platform (e.g., Microsoft 365, Google Workspace) and offers real-time updates against emerging threats. These tools can identify suspicious patterns, scan links and attachments for malware and quarantine harmful messages. With over 94 percent of malware delivered through email, filtering tools drastically reduce the risk of human error by preventing malicious messages from ever reaching your staff.
- **Back up your data so you can recover from disasters.** Backups allow you to recover from disasters such as server crash, fire, theft, flood, sabotage, natural disasters, etc. Determine your maximum acceptable amount of downtime, then get a professional evaluation of your current backup solution and plan to ensure you can recover in the amount of time you need. Finally, ensure daily backups of your systems and store them securely, both on-site and in the cloud. Get a professional to set this up properly to ensure all data is included. Test backups regularly to ensure they work.
- **Utilize business continuity solutions – keep working through disasters.** Investigate solutions with instant virtualization to switch to backup systems and minimize downtime during an attack or server failure. Newer technologies for business continuity include virtual failover servers and failover internet connections to ensure minimal downtime in case of cyberattacks or other disasters. These are your practice's airbags, deploying immediately to keep operations running during a crash.
- **Enable multi-factor authentication (MFA) for extra defense.** MFA adds an extra layer of security by requiring a second form of verification (like a text code) before accessing sensitive systems. Even if your credentials are stolen, this can help prevent cybercriminals from accessing your data and systems. It's like needing both a key and a security code to unlock your digital vault.

continued on next page

- **Keep systems updated to minimize system vulnerabilities.** Outdated software is an open door for hackers because it means that security holes have not been patched. This allows hackers to exploit the software for their gain. Set up automatic updates to patch vulnerabilities as soon as fixes are released or, even better, have an IT security provider monitor and manage this for your practice.
- **Develop a written incident response plan to ensure rapid response.** Have a clear plan for responding to an attack, including who to contact (e.g., IT, cyber insurance legal counsel) and how to notify patients if their data is compromised. Write a chart and/or checklist to ensure you can respond quickly, properly and with less stress.
- **Partner with cybersecurity experts to ensure your plan works.** Work with IT providers who specialize in healthcare cybersecurity and understand HIPAA requirements. Look for those offering 24/7 monitoring and rapid incident response.

At its core, cybersecurity isn't just about protecting your practice or complying with HIPAA, it's about protecting your patients. Their trust in you includes the expectation that their sensitive information will remain secure. By implementing these measures, you're not only safeguarding your business but also ensuring the continuity of care.

Remember: A single click can lead to a crisis, but with the right preparation, your practice can avoid downtime and emerge stronger in the face of digital threats. ■

Anne Genge is a multi-certified privacy and cybersecurity expert who has won global awards for her work in cyber risk management, ransomware prevention and cybersecurity education for healthcare providers. For more than 20 years, she has been a technological innovator and educator working closely with practice owners, dental teams and IT providers to protect patient and practice data and to enable compliance with privacy regulations.

Looking for more resources on this topic? Black Talon Security is the OMSNIC Preferred Partner for cybersecurity. Visit BlackTalonSecurity.com/OMSNIC for more information.

References

1. Bruce, G. Why hackers are extorting patients directly. Beckershospitalreviewcom, 2024. Available at: BeckersHospitalReview.com/cybersecurity/why-hackers-are-extorting-patients-directly.html?oly_enc_id=2214G1474278B3W. January 22, 2024

2. Wilson, C. Integris Health faces federal lawsuits amid data breach; dark web extortion alleged by victims. KOKH, 2024. Available at: OKCFox.com/news/local/integris-health-faces-federal-lawsuits-amid-data-breach-dark-web-extortion-alleged-by-victims-cyber-security-tor-darknet-personal-info-hospital. January 9, 2024

3. Sjouwerman, S. Stanford Research: 88% of Data Breaches Are Caused by Human Error. blogknowbe4com, 2020. Available at: Blog.knowbe4.com/88-percent-of-data-breaches-are-caused-by-human-error.

4. Sobers, R. Varonis. 157 Cybersecurity Statistics and Trends [updated 2024]. Available at: Varonis.com/blog/cybersecurity-statistics. September 13, 2024

5. Alder, S. Wood Ranch Medical Announces Permanent Closure Due to Ransomware Attack. HIPAA Journal, 2019. Available at: Hipaajournal.com/wood-ranch-medical-announces-permanent-closure-due-to-ransomware-attack/. September 30, 2019

6. Aaron, D. 82% of Ransomware Attacks Target Small Businesses, Report Reveals. Techco, 2022. Available at: Tech.co/news/82-of-ransomware-attacks-target-small-businesses-report-reveals. February 7, 2022

This is number 202 in a series of articles on practice management and marketing for oral and maxillofacial surgeons developed under the auspices of the Committee on Practice Management and Professional Staff Development and AAOMS staff. Practice Management Notes from 2002 to present are available online at AAOMS.org.