The Top 10 Cyber Risks To Your Practice and How to Avoid Them

As your technology evolves, so do your practice's risks. Hackers have become more sophisticated and utilize the Dark Web to purchase ransomware schemes, access to server credentials, credit card accounts, and many other nefarious activities. In short, Cybercrime is big business!

This report will provide information and counter-moves to help protect you and your practice.

ACT SMART I.T.
Helping You Benefit From Today's Technologies

~~ Our Story ~~

David and Pam Snell were team members at Creating Ultimate Smiles with Dr. Barry Brodil in Hanover for 20 years.

During that time, they provided the IT support that included maintaining computer systems and creating their website. They had the exceptional opportunity to attend dental seminars and conferences including those given by the American Academy for Cosmetic Dentistry, The New England Academy for Cosmetic Dentistry, the MISCH Institute, The Schuster Group for Practice Management, The Homoly Group for Implant Marketing, the Linda Miles Group, Rocky Mountain Rendezvous and, of course, Yankee Dental, where they were speakers in 2000 and 2001.

Computers and technology became a real passion for David, and they built American Computer Technologies during that time with Dr. Brodil as their business mentor. David helped the practice transition from proprietary practice management software to DOS and then Windows-based software. He also helped the practice become early adopters to intra-oral cameras, digital imaging software, and digital Xrays.

They have seen dental practice needs change over the past 30 years. Today, technology in the operatories isn't just the norm, it is a necessity! It needs to work seamlessly and dependably.

No other company on the South Shore has more experience relating to the many different practice options out there.

Our Mission is to delight our clients with exceptional, friendly, and accurate service every single day.

Dr. Brodil was a strong believer in education for himself and his team, and that belief became instilled in David and Pam. They are all continuously taking courses to improve their knowledge and skills. Each team member completes at least 8 hours of continuing education every month.
We discuss procedures to improve service, among other important topics at our monthly team meeting.

David and Pam are extremely proud of their dental heritage and look forward to helping many more dental practices in the future.

A few statistics; the reasons we all should be worried...

Summary of findings

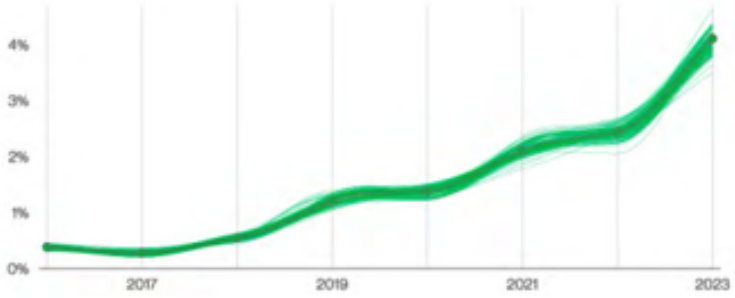


Figure 5. Pretexting incidents over time

Social Engineering attacks are often very effective and extremely lucrative for cybercriminals. Perhaps this is why Business Email Compromise (BEC) attacks (which are in essence pretexting attacks) have almost doubled across our entire incident dataset, as can be seen in Figure 5, and now represent more than 50% of incidents within the Social Engineering pattern.

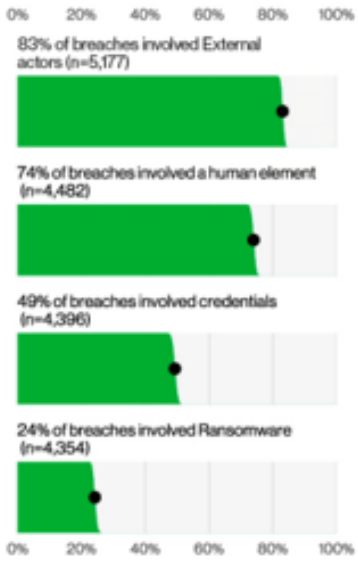


Figure 6. Select key enumerations

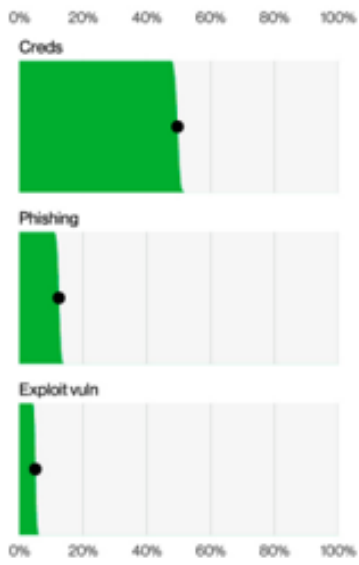


Figure 7. Select enumerations in non-Error, non-Misuse breaches (n=4,291)

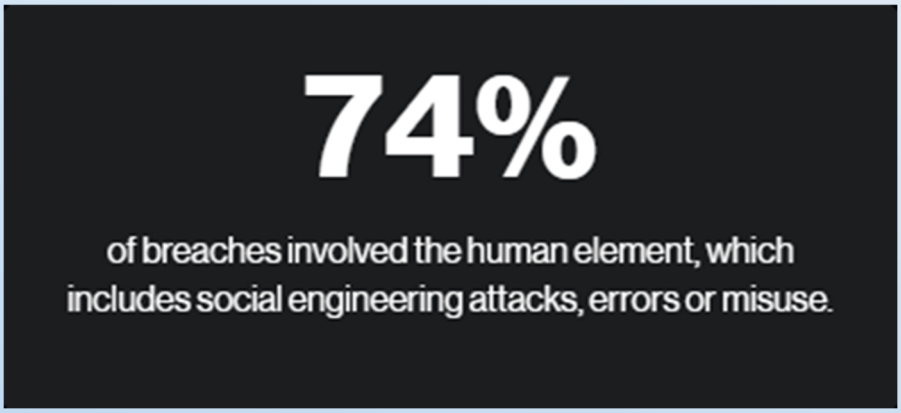
74% of all breaches include the human element, with people being involved either via Error, Privilege Misuse, Use of stolen credentials or Social Engineering.

83% of breaches involved External actors, and the primary motivation for attacks continues to be overwhelmingly financially driven, at 95% of breaches.

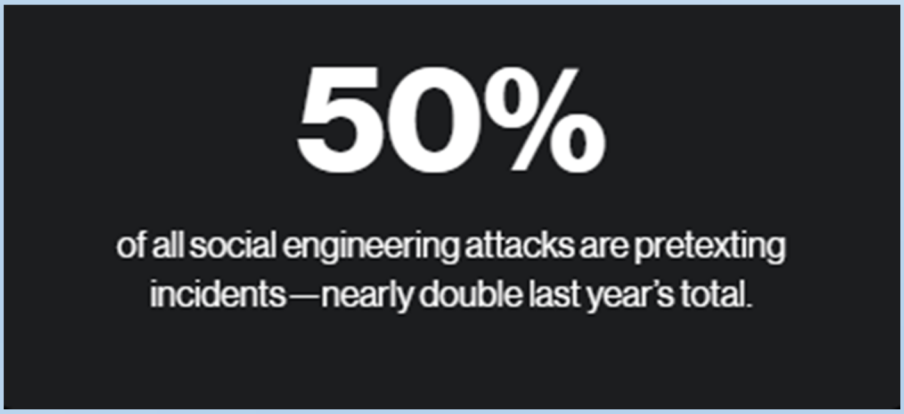
The three primary ways in which attackers access an organization are stolen credentials, phishing and exploitation of vulnerabilities.

Source:
"Verizon 2023 Data Breach Investigations Report"
https://www.verizon.com/dbir

Primarily from organized crime groups
19% involved internal actors, who caused both intentional and unintentional harm through misuse and simple human errors.



Use of stolen credentials or Social Engineering.
Help people-proof your systems.



Pretexting—an invented scenario that tricks someone into giving up information or committing an act that may result in a breach

Source: https://www.Verizon.com/dbir

10. You don’t have a 3-2-1 backup system in place

A good backup can save you from many threats of loss:
Tornados, Hurricanes, flood or other water damage, theft, employee error or even a disgruntled employee’s malicious act of revenge.

Create 3 copies of your data (1 primary copy and 2 back-ups)

Store your copies in at least 2 types of storage media (local drive, network share/ NAS, etc)

Store one of those copies offsite

What good is a data backup if you never check it?
Only 34% of companies test their backups – 77% of those who do have found failures!
You need to be able to rely on a good backup in case disaster strikes!

Just because your data is “In the Cloud” doesn’t mean that your data is backed up-
Make sure and do a test restore regularly

Backing up your data is essential, but also keep in mind that you need a plan for data re-covery.
In some cases, downloading your backup to restore to a corrupted machine can take

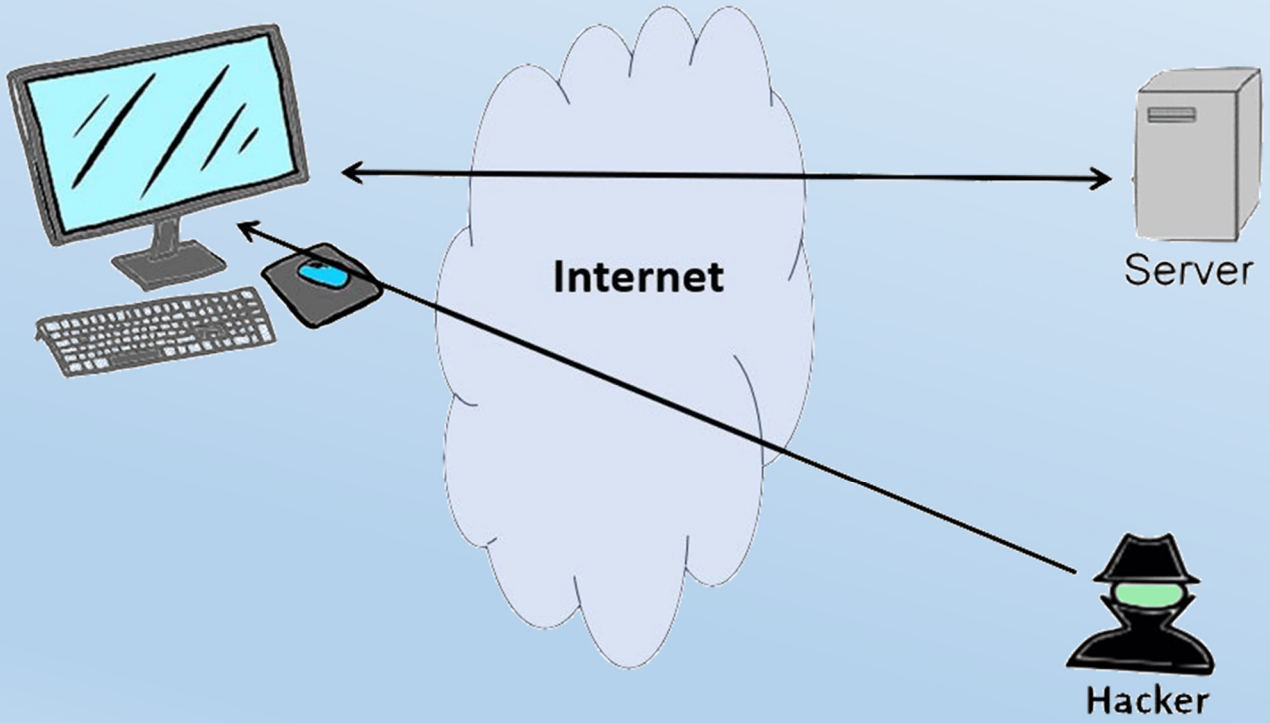
A FREE backup isn’t guaranteed at all so it’s practically worthless

9. You don’t have a business-class firewall protecting your network

Why a Business-class Firewall? Here are 3 simple reasons:

Consumer-grade Routers -

1. Simple consumer-grade routers use simpler software code to route traffic, which is widely known by hackers and easier to exploit.



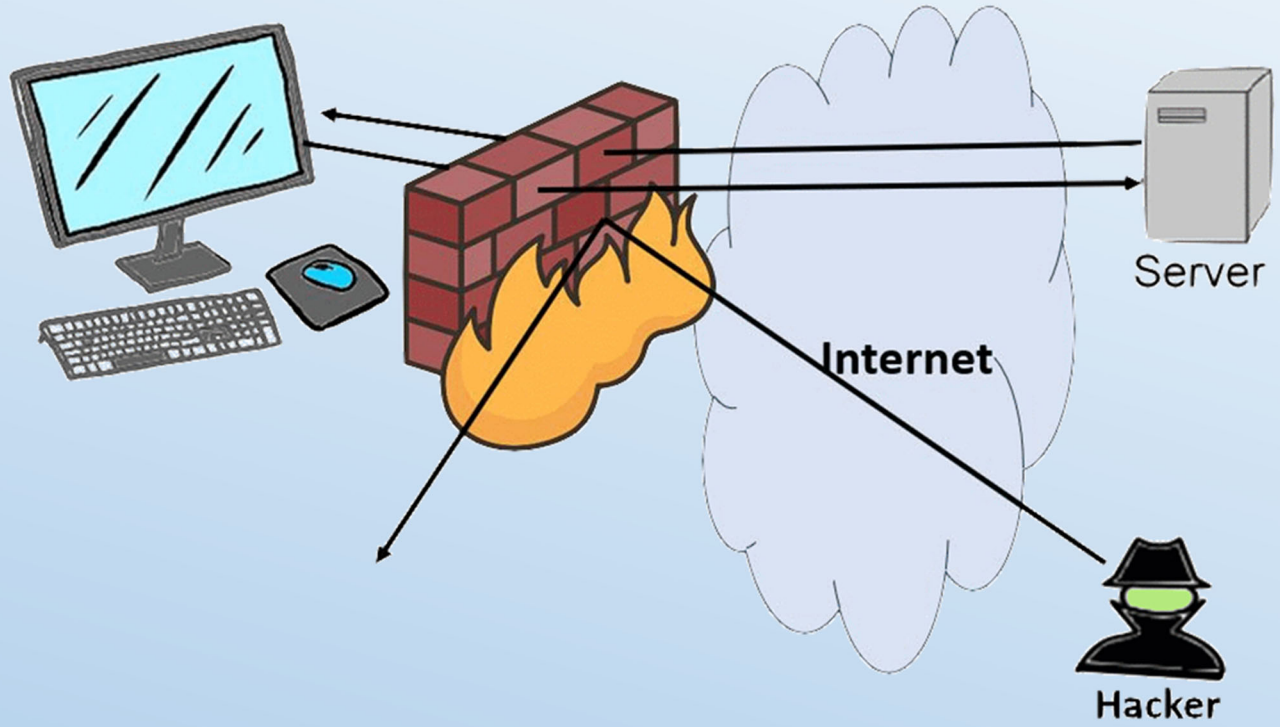
2. Normally do not provide any analytics and do not receive regular software updates from the manufacturer.

3. Do not include sophisticated features like Active Directory Integration, Content filtering and more -- the stuff you really need to protect your practice.

Business-Class Firewalls

The following 3 items are an absolute MUST HAVE when considering protecting your private network data:

1. **Traffic Scanning and Monitoring:** Has the ability to scan network traffic in real-time for malware and spyware, and block those attempts before they ever make it to the computers or server.



2. Intrusion Detection System: The firewall should be able to track and monitor your bandwidth. In non- geek speak: It watches for patterns and is able to pick out anomalies and block them. The ability to keep a record of and view intrusion attempts (hackers trying to get in) or remote access attempts (usually employees or vendor support) is a must,
especially for healthcare practices.

3. Application control: The firewall should be able to prevent unauthorized applications from running on the network and slowing it down as well as filtering options for blocking content (pornography), social sites, personal email and games.

8. You don’t use strong, unique passwords wherever possible

Your UNIQUE email password

Your email password must be strong and DIFFERENT from every other password that you use.

If a hacker gets into any of your secured sites, the first thing they will try to do is change the password so you can’t get back in.

How do they do that?
They request a password reset – sent to your email address.

If they can get into your email, they have the keys to your kingdom and can access every account that you have.

Take a few minutes and change your email password ASAP!

Password Best Practices:

- Don't use your email password for any other account
- If you use the service often (like your bank account), memorize a passphrase enhanced with numbers and symbols

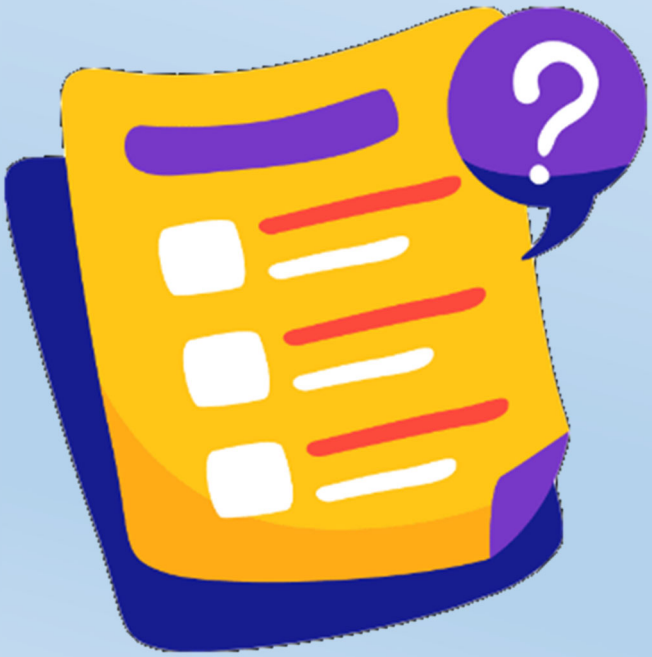
- **Get a password manager** for less used sites and have it create random combination passwords unique to each site.

- **Never save your passwords** in your computer browser – if your computer gets hacked, they can get into all your accounts!

- **Challenge Questions:** in many cases, you can find the answers to your challenge questions on FaceBook or other social media sites

  * Mom's middle name? ***Chanel #5*** *(Her favorite perfume)*
  * Street you grew up on*?* ***Monopoly Street***
  * Your best friend in High School? ***Pizza***

There's no one checking that your answers are true, so have fun with responses that you can remember.



- Use a ***PassPhrase*** rather than a Password

DentalRiskyBusiness
Dent@lR!$kyBu$1ness

https://www.security.org/how-secure-is-my-password/

Note: Even the unchanged phrase "DentalRiskyBusiness" would take 3 hundred trillion years! It's 19 characters!

Of course, AI is adapting and we expect that these calculations will change and go down in the future

Make Your Passwords More Secure:

- Use **Multi-Factor Authentication** whenever it is offered
  Note: We used to call it two-factor authentication (2FA), but more factors are better. You'll find all the terms used interchangeably with "multi-step," "two-step," and "verification," depending on the marketing.
  As PCMag's Lead Security Analyst Neil J. Rubenking put it, "There are three generally recognized factors for authentication: something you know (such as a password), something you have (such as a hardware token or cell phone), and something you are (such as your fingerprint). Two-factor means the system is using two of these options." Multi-factor means you might even use more than two.

- **Change your passwords** (PassPhrases) every 3 months
  This is a controversial subject. Some institutes say that changing your password often makes users create easy to guess passwords.

- **Use a Password Manager** so you can use 12+ character, perfectly random passwords whenever possible
  Note: The best business password manager allows everyone in an organization to spend less time trying to remember strong, unique passwords for all their accounts. The password manager stores login credentials for each person and includes a random password generator that helps them create a random strong password for each of their accounts. The best password managers for businesses also let administrators keep an eye on employees' password hygiene. That is to say, you can see which employees have weak or reused passwords, and who's not using multi-factor authentication to secure their accounts, which allows you to prompt them to improve their password security.

PC Magazine offers a list of the Best Password Managers
https://www.pcmag.com/picks/the-best-password-managers

7. Your Team shares email addresses, making it impossible to know who is doing what and where.

We see this in so many practices.

FrontDesk@ XYZDental.com which is used by all the support staff.

Or, even worse, FrontDeskXYZDental@gmail.com!

- EVERY member of the team needs their own email address at your domain (Mary@XYZDental.com)
- You control where your data is and can take control back at a moment's notice
- Each team member is accountable for their logins
- Each team member has accountability for training

6. You lack an Acceptable Use Policy so office equipment is used for personal benefit

Years ago, many people used their work computer for personal use because they didn't have one at home. Today, almost everyone has a computer so there is no need to subject the practice's network to the possibility of being hacked. Almost everyone carries their own personal computer in their pocket or handbag; the smart phone!

Protect your practice with an Acceptable Use Policy that designates how office equipment can be used.

What is an Acceptable Use Policy (AUP)?

An AUP is a document that spells out what an employee can and cannot do when using computers and computing resources in an organization

You are required to have one to satisfy HIPAA and HITECH requirements.

With Facebook and other "social" sites responsible for over 40% of viruses, malware, and ransomware, employees should know where they are permitted to go online with practice devices, particularly when there is patient health information (PHI) on those devices.

7 Benefits of an AUP

1. Informs employees of the rules upfront
2. Limits an organization's legal liability and protects against legal action
3. Limits personal use of an organizations resources
4. Can help with cost control by limiting use of resources, such as storage and bandwidth
5. Helps secure an organization's data from cyber attacks and data breaches
6. Helps prevent compliance violations
7. Protects an organization's reputation from intentional or inadvertent employee actions

The process of developing an Acceptable Use Policy can be challenging, but it's essential if you want to protect your practice's data, devices, and networks.

You can find a template to use as a "starter" here:
https://www.techtarget.com/whatis/definition/acceptable-use-policy-AUP

Disclaimer:

We are not lawyers, so do not use this policy resource in your practice without having your attorney adjust and tweak it for your exact circumstances.

5. You lack other policies, including:

- **Password Policy**—your practice's expectations on the proper use and security of passwords used in your office
- **Disaster Recovery Policy**—who is responsible for which actions in the case of a disaster
- **Bring Your Own Device Policy (BYOD)** - this one is tricky because if you allow employees to use their own devices, you are relinquishing control and ownership of the data that they carry. Consult an attorney if you decide to allow BYOD in your practice
- **Social Media Policy**—what your employees may or may not say on social media.

4. You don’t provide ongoing security awareness training as required by HIPAA and PCI Compliance

What is security awareness training?

Security awareness training is the process of educating people to understand, identify, and avoid cyber threats. The ultimate goal is to prevent or mitigate harm—to both the practice and its patients—and reduce human cyber risk.

According to the Annual Cybersecurity Attitudes and Behaviors Report for 2022(2023 won’t be out until the first week of October):

- 92% of respondents took action after a security training
- 58% say they are better at recognizing phishing
- 45% started using strong and unique passwords
- 40% started using MFA
- 40% started regularly installing software updates

3. You think that just having cybersecurity insurance will save you if you have a breach

From a Sophos Cyber Insurance Report:

Goal	Requirement
Secure cyber insurance coverage	**Advanced cyber threat protection** is increasingly a requirement in order to get coverage. Managed detection and response (MDR) services, extended detection and response (XDR) technologies, and next-gen endpoint protection are the most common requirements.
	Multi-factor authentication (MFA) is fast becoming a prerequisite for coverage, with insurers insisting that clients close one of the most common security gaps before they absorb the risk. "I was told that if we don't get MFA within a year, our cyber insurance will be dropped." Healthcare provider, USA "Our cyber insurance renewal is predicated on us enabling MFA for remote access." IT support and services provider, USA

Reduce the likelihood of making a claim – and higher premiums in the future	As with other types of insurance, if you make a claim you can expect a significant increase in your premiums in subsequent years. By minimizing your risk of being impacted by a cyberattack, you reduce the likelihood that you'll need to call on your policy and help keep your premiums down.
Reduce the risk of non-payment in the event of an incident	Poor IT security hygiene can prevent you from receiving financial support in the event of an incident. If the insurer believes that you 'left the door open' through weak practices they may have grounds to not pay out. "We do not pay for any claims, losses, breaches, privacy investigations, or threats due to the use of outdated or unsupported software or systems." Hiscox Cyberclear™ policy wording, UK, June 2021
Minimize the impact if an incident does occur	Responding quickly and appropriately to a cyberattack can significantly reduce the impact and cost of the incident.

FYI –

New SEC Rules Require Publicly Traded U.S. Companies to Reveal Cyber Attacks Within 4 Days

"In recent months, more than 500 companies have become victims of a cyber attack spree orchestrated by a ransomware gang called Cl0p, propelled by the exploitation of critical flaws in software widely used in enterprise environments, with the threat actors leveraging new exfiltration methods to steal data, according to Kroll."

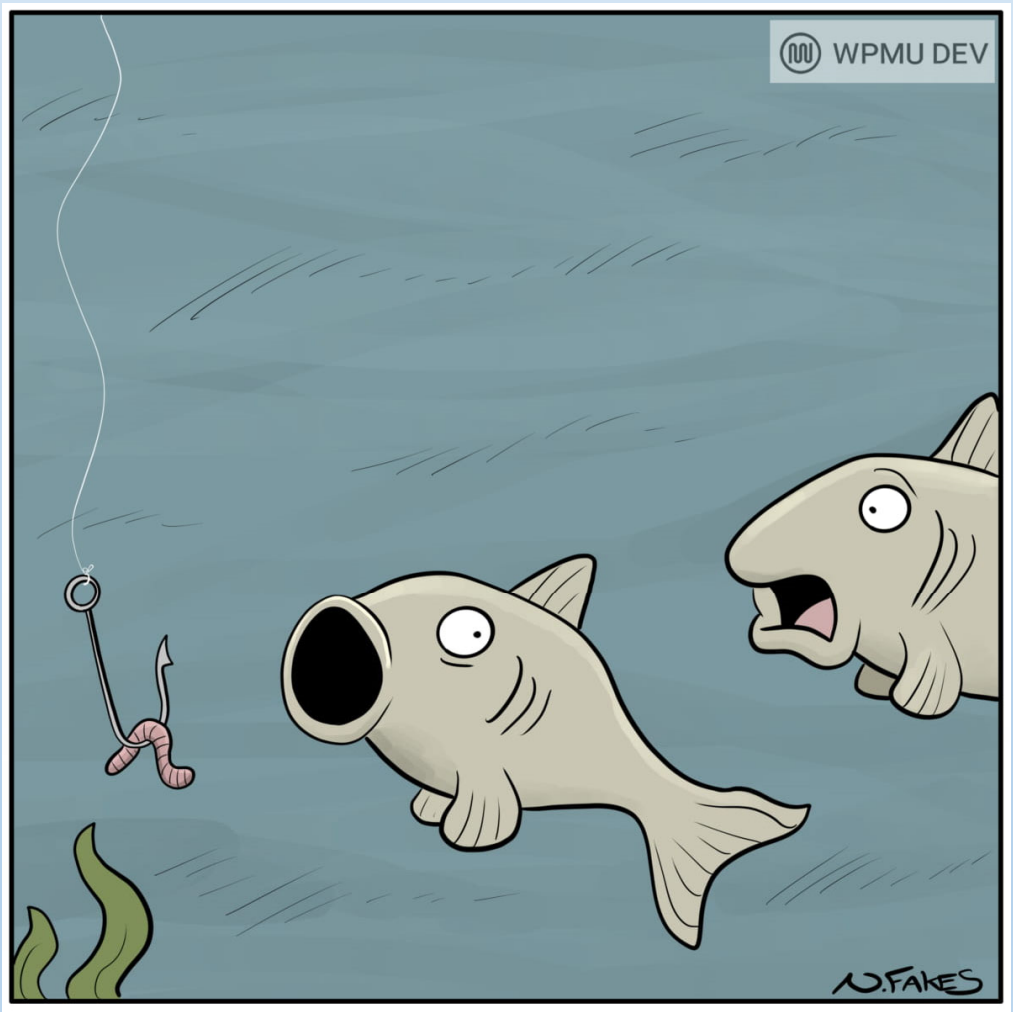
"... organizations should have repeatable and well-documented incident response plans with communication plans, procedures, and requirements on who is brought into the incident and when," McQuiggan added."

https://thehackernews.com/2023/07/new-sec-rules-require-us-companies-to.html

2. Phishing is one of the most effective threats to your practice and AI is making it worse!

With about 91% of data breaches coming from phishing, it is the most exploited form of social engineering and presents the single greatest threat to information security.

AI or artificial intelligence, is making phishing emails harder to spot.

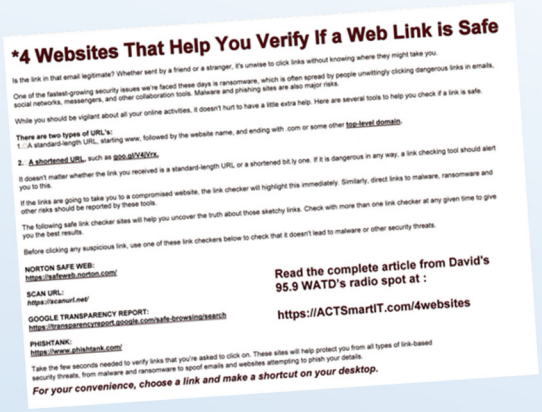


Why is it called “Phishing”

Like a person fishing lures a fish with bait, a hacker lures their victims with the bait of information they would like or are curious about.

With about 91% of data breaches coming from phishing, it is the most exploited form of social engineering and presents the single greatest threat to information security.

If you’d like FREE copies of this postcard for every computer user in your practice, **https://actsmartit.com/phishing/**



*4 Websites That Help You Verify If a Web Link is Safe

Is the link in that email legitimate? Whether sent by a friend or a stranger, it's unwise to click links without knowing where they might take you.

One of the fastest-growing security issues we're faced these days is ransomware, which is often spread by people unwittingly clicking dangerous links in emails, social networks, messengers, and other collaboration tools. Malware and phishing sites are also major risks.

While you should be vigilant about all your online activities, it doesn't hurt to have a little extra help. Here are several tools to help you check if a link is safe.

There are two types of URL's:
1. A standard-length URL, starting www, followed by the website name, and ending with .com or some other top-level domain.

2. A shortened URL, such as goo.gl/V4Vrx.

It doesn't matter whether the link you received is a standard-length URL or a shortened bit.ly one. If it is dangerous in any way, a link checking tool should alert you to this.

If the links are going to take you to a compromised website, the link checker will highlight this immediately. Similarly, direct links to malware, ransomware and other risks should be reported by these tools.

The following safe link checker sites will help you uncover the truth about those sketchy links. Check with more than one link checker at any given time to give you the best results.

Before clicking any suspicious link, use one of these link checkers below to check that it doesn't lead to malware or other security threats.

NORTON SAFE WEB:
https://safeweb.norton.com/

SCAN URL:
https://scanurl.net/

GOOGLE TRANSPARENCY REPORT:
https://transparencyreport.google.com/safe-browsing/search

PHISHTANK:
https://www.phishtank.com/

Take the few seconds needed to verify links that you're asked to click on. These sites will help protect you from all types of link-based security threats, from malware and ransomware to spoof emails and websites attempting to phish your details.

For your convenience, choose a link and make a shortcut on your desktop.

Read the complete article from David's 95.9 WATD's radio spot at :

https://ACTSmartIT.com/4websites

On the back, there are 4 websites that can help you verify if a web link is SAFE!

NORTON SAFE WEB:
https://safeweb.norton.com/

SCAN URL:
https://scanurl.net/

GOOGLE TRANSPARENCY REPORT:
https://transparencyreport.google.com/safe-browsing/search

PHISHTANK:
https://www.phishtank.com/

Always be suspicious – of any unsolicited communication from businesses or individuals, regardless of the message medium.

Don't click on links or attachments in suspect emails, textx or social media messages.

Directly contact the alleged sender via their official website, phone number, or email address if you are not sure of the legitimacy of a message you have received.

File a complaint with the FBI Crime Complaint Center (IC3) to help shut down cybercriminals.

SOCIAL MEDIA PHISHING

Cybercriminals use social media as a channel to carry out phishing attacks aimed at stealing personal information or spreading malware; some attacks are even used to highjack you accounts to launch follow up attacks on your connections or followers.,

WHAT TO LOOK FOR

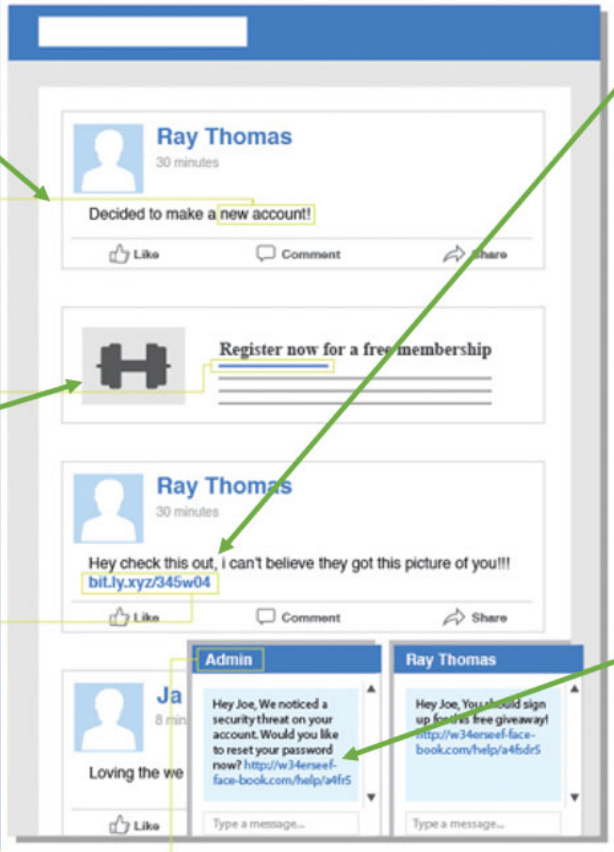
Playing Pretend

Scammers ***create replica*** accounts and inform victim's friends/followers that their previous account was abandoned.

Messages are sent *to victim's friends that demand the recipient to click on a link with an aim to collect personal data, e.g. credit/debit card numbers.*

Bogus Posts

Social Network feeds can contain ***bogus posts*** that trick users into clicking on a link and providing personal information.



Social Media Malware

Scammers can ***pose as a friend/follower*** and send messages with links to sites that are infected with malware.

Even messages from known friends may include links to sites that have been hacked.

Stay Suspicious

Phishers can ***pose as admins*** from social networking sites in an attempt to gain access to passwords and other account information.

1. You think you don't have to worry about any of this because you are too small to be hacked!

59% of small business owners with no cybersecurity measures in place believe their business is too small to be attacked

In this documentary, we meet Dr Shayla Fowler Kasel, a Sim Valley, CA physician struck by ransomware.

Her story is in episode 2; Hunters and Hunted and discusses how ransomware caused her to close her practice.

If you'd like to see the entire series including **Episode 1: Origins of Cybercrime** and **Episode 3: Weapons and Warriors:**

https://www.sophos.com/en-us/content/ransomware-documentary?cmp=160329

You'll know when you've been hit by ransomware because the bad guys will have the ransom screen displayed on your monitor. The notice may look like these or be something entirely different, but every notice will say that you need to pay the ransom to get your data back and be able to work.

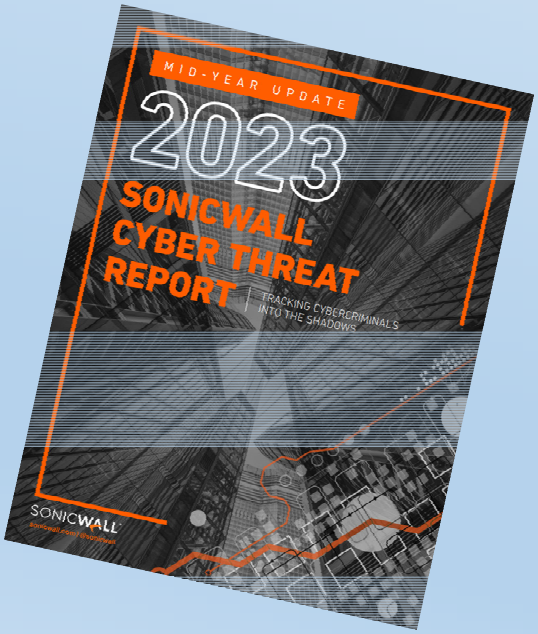
The Good News:

In 2023, ransomware attacks are DOWN! According to the just published ***mid-year update of the 2023 Sonicwall Cyber Threat Report***

A few factors include:

- **The Hive Takedown:** In January 2023, the U.S. FBI announced it had infiltrated and taken down the Hive ransomware operation — previously the third-most active ransomware gang.

- **Increased Law Enforcement Scrutiny:** the FBI and federal agencies from around the world have been arresting cybercriminals and seizing funds! Organizations willing to pay a ransom dropped, causing the hackers to begin conducting layoffs!



The Bad news:

Instead of ransoming your data, they are going straight to extortion and demanding money to keep the data from being leaked. Since no ransom, no ransomware reported!

The Top 5 steps you should take following a ransomware attack
The 3 things you should *not* do after the attack.

Note:
We strongly recommend that you consult your attorney and your insurance carrier before you take any steps and before you have an issue. Some insurance policies have specific details on how to handle ransomware or a data breach and if you don't follow their exact steps, you could void your coverage and any claims.

Step #1

Take a photo of the ransomware message (you may need it later to restore your data and for law enforcement).

Immediately disconnect the device from the network and all wireless connectivity (Wi-Fi, Bluetooth) including unplugging the internet/ethernet cable if the device is hard wired.

Step #2

If you have Cyber Insurance Contact Your Insurance Carrier And Your Attorney

Don't use email to communicate with either of these entities

If your insurance covers ransomware, your carrier most likely has steps that you'll need to take, such as finding a forensic specialist and writing an events statement.

We suggest calling your legal counsel as you may need their assistance with your insurance carrier, your clients and possibly other law enforcement agencies. If you're in a regulated industry (medical – finance – law) this step is urgent! If you don't have an attorney, you'll want to find one that specializes in technology.

Step #3

If you ***don't*** have Cyber Insurance

When it comes to ransomware, or any type of malware/virus/breach – time is of the essence! Reporting the attack right away will allow your service provider or inhouse staff to take immediate action and prevent more attacks.

The IT staff will likely advise you to disconnect affected devices from the network if you haven't already to prevent the ransomware from spreading. They will probably take all other systems offline and turn off the Wi-Fi for the entire network.

If it's early enough, the ransomware may be prevented from spreading across the entire network, which will help you get back to work quicker.

Step #4

Report The Attack To Authorities

Ransomware is a crime.

You should report attacks to CISA (Cybersecurity & Infrastructure Security Agency) and your local FBI office.

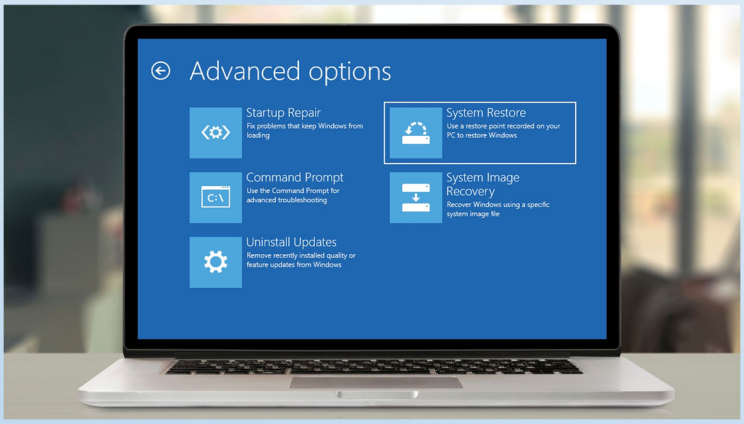
https://us-cert.cisa.gov/forms/report

https://ransomware.ic3.gov/

Step #5

Restore or Start Fresh

You have two options to get back to work. You can either restore via a system restore point or a backup to the devices or you can start fresh - either with a good backup or without. While they sound similar, they are not.



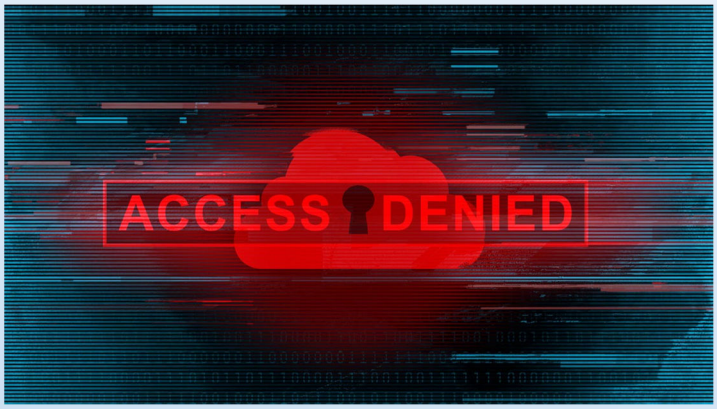
Your first option is to simply use a System Restore Point to get your system back up and running. Sounds easy enough?
Why not just run a system restore?
It is not the best solution for removing the virus or malware that caused the problem in the first place.

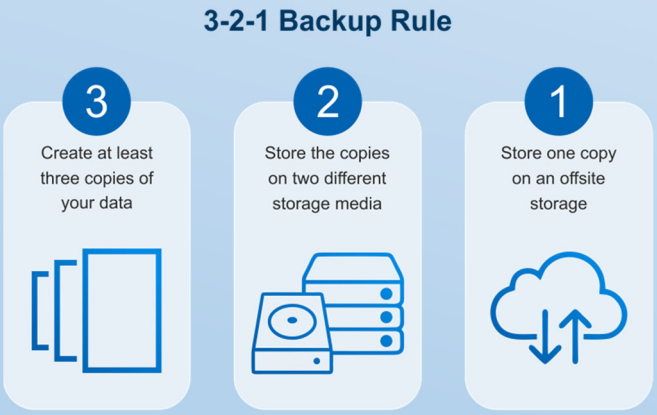
Malicious software is typically buried within all kinds of places on a system, meaning a System Restore can't root out every instance. Also, System Restore does not save old copies of your personal files as part of its snapshot.

Your second option, in my own personal opinion and those of the FBI and CISA is the better idea, is to start fresh (preferably with a good backup) and here's why. The surest way to confirm malware, ransomware, or any backdoors put in by the hackers have been removed is by doing a complete wipe of the hard drive.

It's not uncommon to be hit again with ransomware shortly after you've "cleaned" up from the first incident if you only restore from a system restore point or a restore a backup before doing a clean wipe first. If you're going to give your old phone to a family member you factory reset it first so that none of your personal data is left behind.

Something to keep in mind, ransomware can (and usually does) encrypt your local backups. Hackers know if you have a backup then you won't need to pay their ransom. If your ONLY backup is connected to a computer that is infected with ransomware, odds are that your backup will have its data encrypted along with everything else.





If you've been following a good backup policy with both local and off-site backups, you should be able to use backup copies that you know weren't connected to your network after the time of attack, and therefore protected from infection.

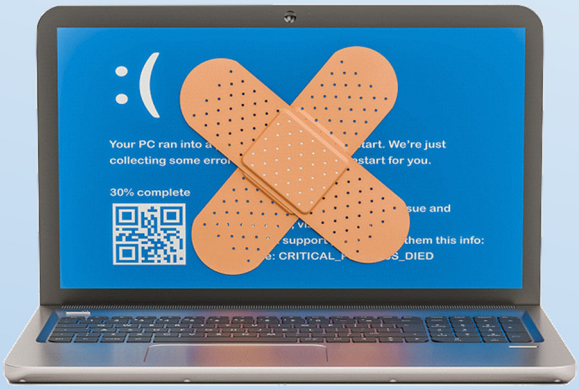
Ransomware can activate in the cloud too. If you are using a cloud backup product depending on it's configuration and the ransomware infection those files may or may not be useable.

The 3 (mistakes or traps) things you should *not* do after the attack.

1.NEVER Pay The Ransom

Paying the ransom may seem attractive to some, especially when paying is less expensive than the potential downtime, contacting insurance and doing the back-and-forth process of forensics and claims. Hackers count on this which is why they tend to target the small to mid-sized companies because it often makes more financial sense for them to just pay out. The problem with paying is there is no guarantee you'll regain full access to your data or your data won't be corrupted and a payment will not prevent your information from being leaked or sold on the dark web by the criminals.

2. Don't Use the Infected Computer Again Until it's Taken Care of by a Professional.



This is not the time to have your DIY staff member or your neighbors high school "techie" kid help you or try to "fix" the issue. If you don't have a real/dedicated in-house IT staff member, seek an IT service provider.

3. Don't Let Embarrassment Or Fear Keep You From Alerting People Who Can Help

Keeping an attack a secret can have big consequences. The longer it takes to get help the faster it lets the hackers and ransomware dig deeper into your network.

Yes, ransomware is not a pleasant experience, but if you have some basic protections in place you can recover from a ransomware attack.

Resources Used For This Report:

- https://www.TechTarget.com
- https://www.Sophos.com - sophos-supports-cyber-insurance-ds.pdf
- https://www.StaySafeOnline.com
- https://www.Ready.gov
- https://thehackernews.com/2023/07/new-sec-rules-require-us-companies-to.html
- https://www.sophos.com/en-us/content/ransomware-documentary
- https://staysafeonline.org/news-press/press-release/press-release-oh-behave-2022/
- https://www.strongdm.com/blog/small-business-cyber-security-statistics
- https://www.sonicwall.com/2023-cyber-threat-report/

We've made every effort to ensure the accuracy of the information in this report.
~ ACTSmart IT

ACT SMART I.T.

Helping You Benefit From Today's Technologies

332 Main Street
Wareham, MA 02571

855-WOW-SERVICE
781-826-9665

ACTSmartIT.com

David@ACTSmartIT.com