Hello and welcome to Don't get hooked.

In this presentation, I will walk you through the types of Phishing tactics commonly used today and provide some examples of how they are applied.

I want to share with you a few tips you can use to be safe, and finally, I would like to leave you with five steps you can use as leadership to help protect your hospital in the future.

If you have questions, please feel free to speak up during the presentation. You can also type in the chat; however, I will not monitor this during my presentation, but I will leave time at the end for questions. I hope you enjoy it!

A little bit about my company.

Bytes Managed IT specializes in a wide range of services, including tailored IT services for healthcare in the Midwest.

Our innovative approach starts with a thorough investigation of what your hospital or clinic needs to succeed to ensure we execute the ideal strategy for you.

While we offer many services at Bytes, here are some popular services for our healthcare partners.

Fully managed image-based backup services monitored and maintained by Bytes staff and service desk management to help offload your current IT so they can focus on driving your support and IT initiatives.

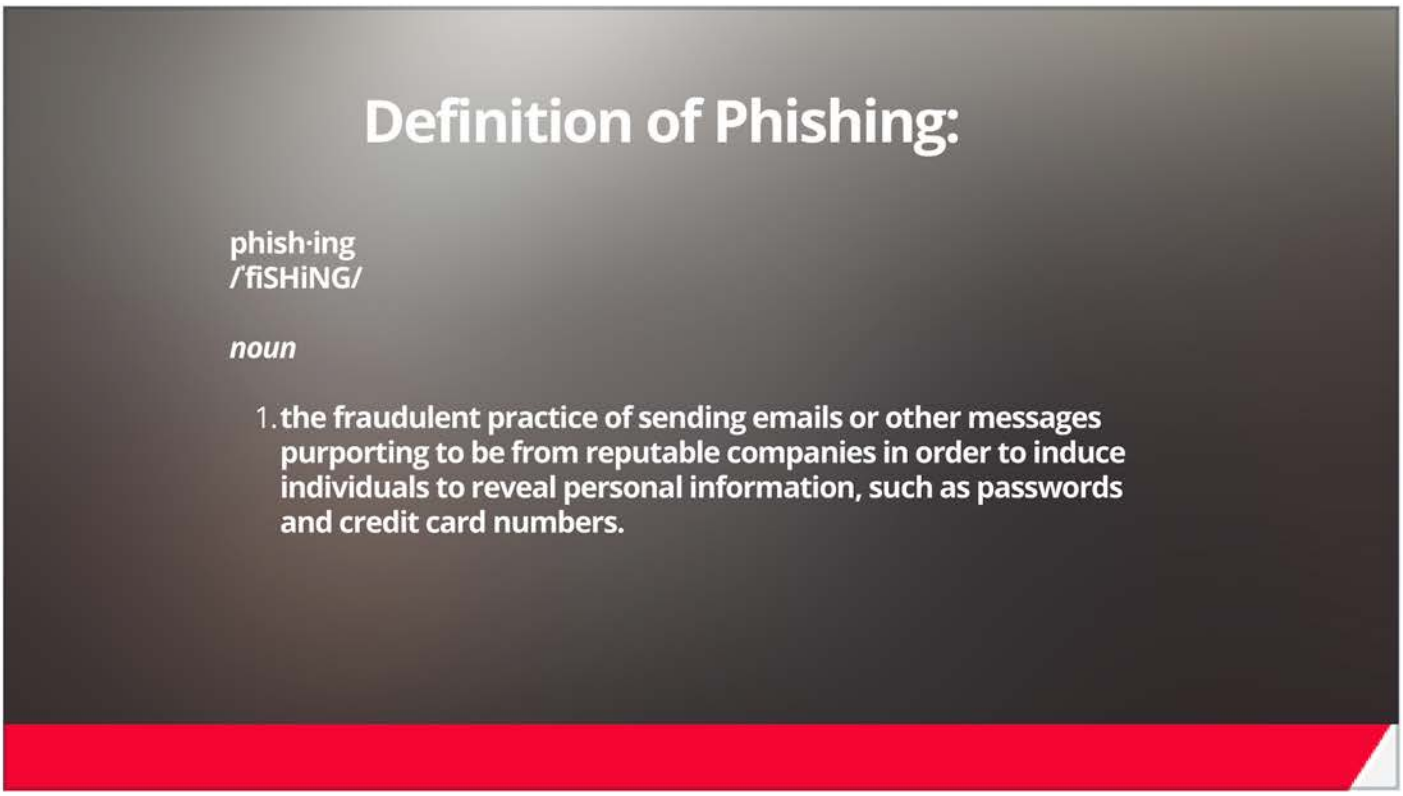
Hi, my name is Todd Lewis and I am the Owner and Co-Founder of Bytes Managed IT since its inception in 2005.

Bytes is a Managed Service Provider in Scottsbluff, Nebraska. We currently serve more than 100 Small to Medium businesses throughout the Midwest.

Today, we proudly provide our services in Nebraska, Wyoming, Colorado, and West Virginia.

Our partners span several vertical markets, including financial, local government, and healthcare, including two critical access hospitals.

As an entrepreneur in the technology industry for over 20 years, I pride myself on providing cutting-edge solutions and reliable IT services.



Let's get into the presentation. we are going to start with defining Phishing.

Phishing is the practice of tricking individuals into giving away sensitive information, such as login credentials or financial data, by disguising oneself as a trustworthy entity. Attackers execute Phishing through various means, such as email, phone calls, text messages, or even social media. Attackers might use pretexting and pretend to be vendors, suppliers, financial institutions, or even an executive team member to trick the individual into providing sensitive financial information and account credentials or transferring funds to a bank account controlled by the attacker.

Phishing attacks can have severe consequences, leading to financial losses, loss of sensitive patient and financial information, and damage to your organization's reputation. Phishing can lead to identity theft among other risks.

Another thing to consider is that once a phish is successful, the bad actor can then use that access to spread malware or ransomware laterally, which can cause significant damage to computer systems and networks.

Why do you need to worry about the threat landscape?

Although Cybersecurity firm Critical Insight reports that the total number of successful breaches in healthcare overall has decreased from the peak in 2020 due to COVID-19. It does not mean we can relax.

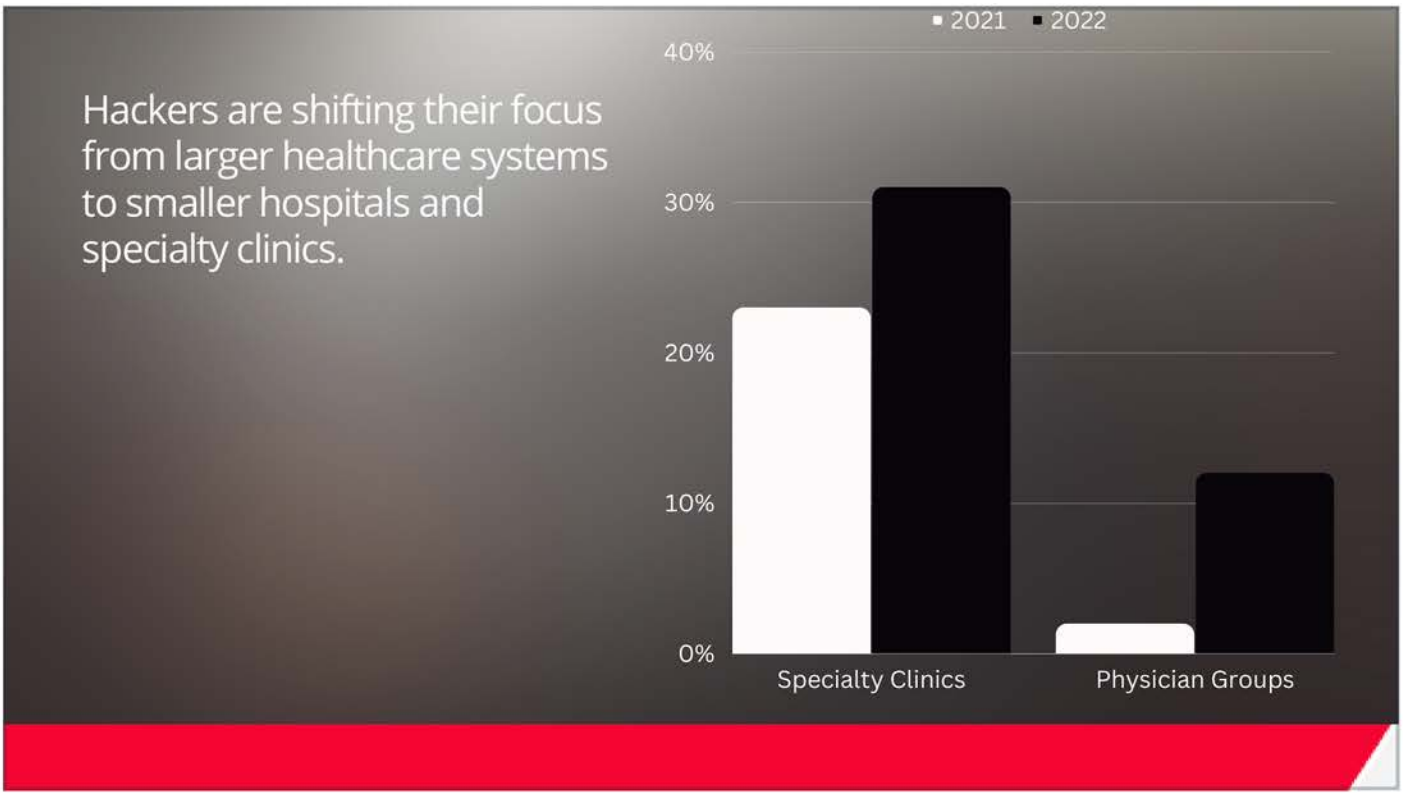
Hackers are shifting their focus from larger healthcare systems to smaller hospitals and specialty clinics, which often lack the same level of security preparedness, staff size, or budget.

According to securityaffairs.com, Consulate Health Care, a large provider of specialty healthcare services for seniors, was hit by the Hive ransomware group.

Hive recently leaked 550 GB of data, including PHI and PII, that it claims to have stolen in the attack. The attack occurred on December 3, 2022, and was disclosed on January 6, 2023. The gang claims to have stolen a wide array of data, including contracts, NDA documents, and proprietary company data, such as internally facing budgets and investor relations. They also stole employee and patient PII and PHI, such as medical records, credit cards, emails, and social security numbers.

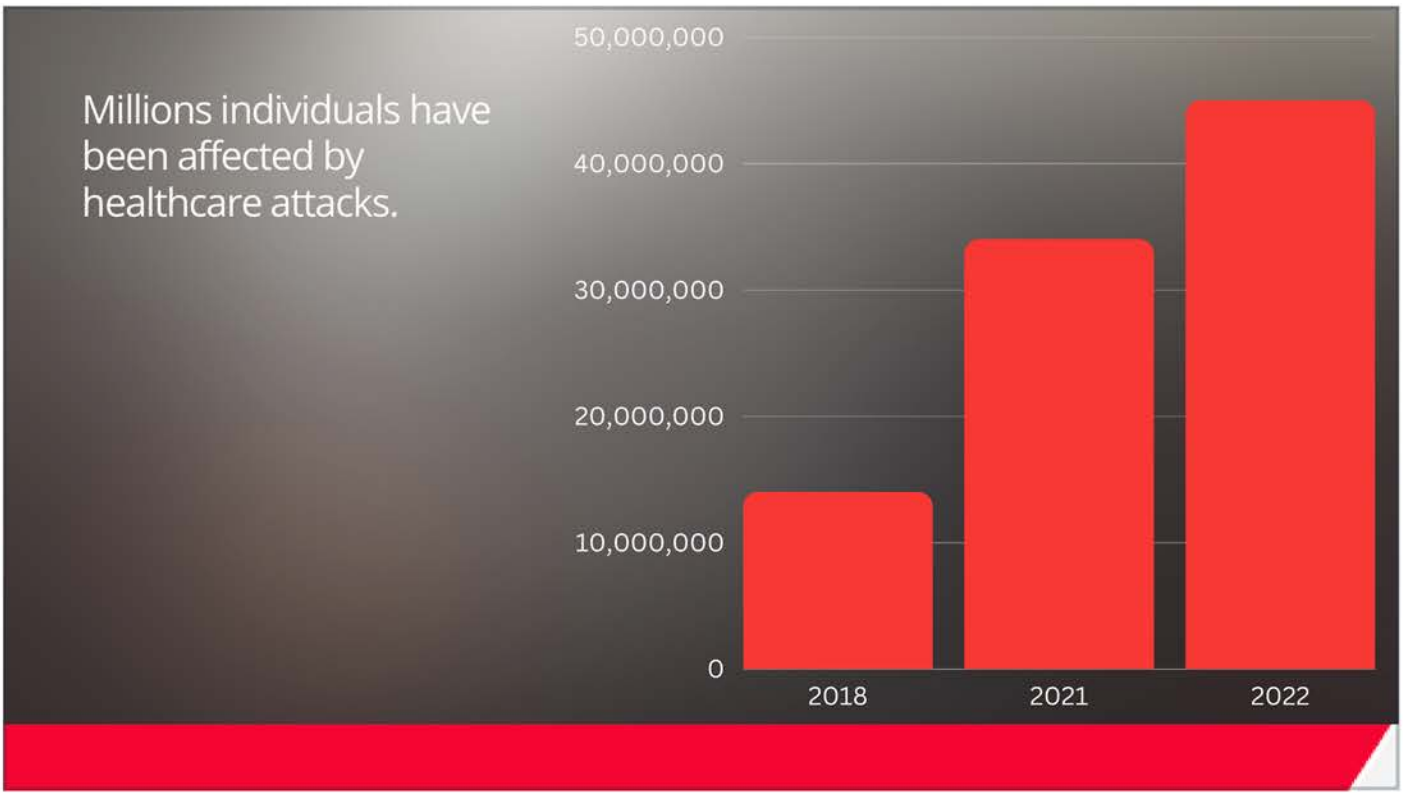
This deluge of data was revealed on Hive's dark web leak site.

According to DataBreaches, This happened after negotiations failed because they couldn't afford the ransom.



Critical Insight goes on to state that the number of cyber-attacks on specialty clinics rose from 23% in 2021 to 31% in the first half of 2022. The number of attacks on physician groups, also increased.

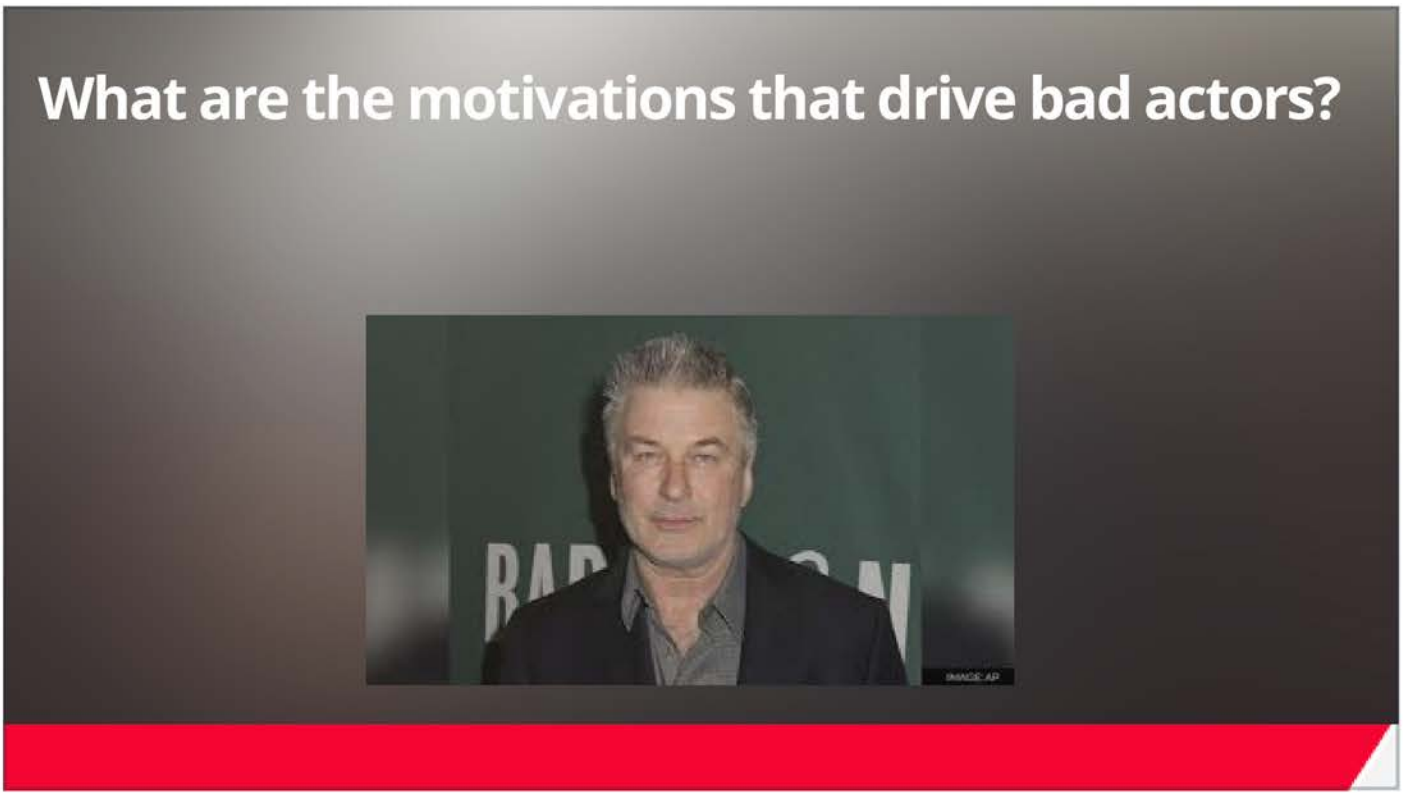
It has grown from 2% of total breaches in the first half of 2021 to 12% in the first half of 2022.



In another article from fiercehealcare.com, In 2021, 45 million individuals were affected by healthcare attacks, up from 34 million in 2020. That number has tripled in just three years, growing from 14 million in 2018.

This is according to the report which analyzes breach data reported to the U.S. Department of Health and Human Services by healthcare organizations.

So, you can see that the bad guys are still and will continue to keep knocking on your door to see what they can get.



What are the motivations that drive bad actors? Oops! not that kind of bad actor. j/k I like Alec

That's the bad guy I was looking for.

There are a variety of motivations that drive bad actors to use Phishing. Listed on this slide are some of the most common.

One of the primary motivations for bad actors is the potential for financial gain. They can use the sensitive information obtained through Phishing to steal money or commit financial fraud. They can make money by selling stolen information in the underground market (DarkWeb) or through Ransomware as a Service.

Some bad actors may use Phishing to obtain sensitive information for espionage. This could include information about a company's operations, financial data, or trade secrets.

(pause)

An example of disruption is where they may use Phishing to gain access to a company's network and launch a ransomware attack that encrypts all of the data, making it inaccessible to the compa ny.

Some bad actors might have ideological reasons, like political or social motivations, to launch a phishing attack against a specific target.

The motivations behind phishing attacks can vary widely depending on the attacker and the target. Still, financial gain and information theft are the most common reasons bad actors use Phis hing.

Why is Phishing so commonly used in a cyber-attacks?

Well....We are social beings.

Facebook and LinkedIn are the most common social media platforms used today in our demographic. If you think about the amount of information available on these platforms, you could learn a lot about a person.

Facebook has information about your personal life, family and pet names, date of birth, friends' names, and all of your personal interests.

LinkedIn provides all the information about your work history, company, and co-workers. You could also learn about particular vendors you work with based on who you follow and interact with.

We are inherently trusting and task oriented.

Humans are naturally inclined to trust others, which has been a crucial aspect of our survival throughout history.

Trust has helped us form social bonds, build communities, and work together to achieve common goals. Trusting others allows us to rely on their help in times of need, and it enables us to form mutually beneficial relationships.

Additionally, trusting others is often easier and less cognitively demanding than constantly doubting and second-guessing every interaction. We are all in a hurry.

The human brain is wired to make assumptions and take shortcuts, so it is more efficient to trust others until there is a reason not to.

These are some of the reasons why social engineering is so effective, it preys on the natural tendency of people to trust, and it exploits their willingness to help others.

But...there is hope. It's also important to note that humans are not indiscriminately trusting; we have a built-in mechanism of trust evaluation based on the context, past experiences, and the perceived trustworthiness of the person or organization.

We can foster that trait.

Here are a few ways to become more aware of and less susceptible to social engineering tactics.

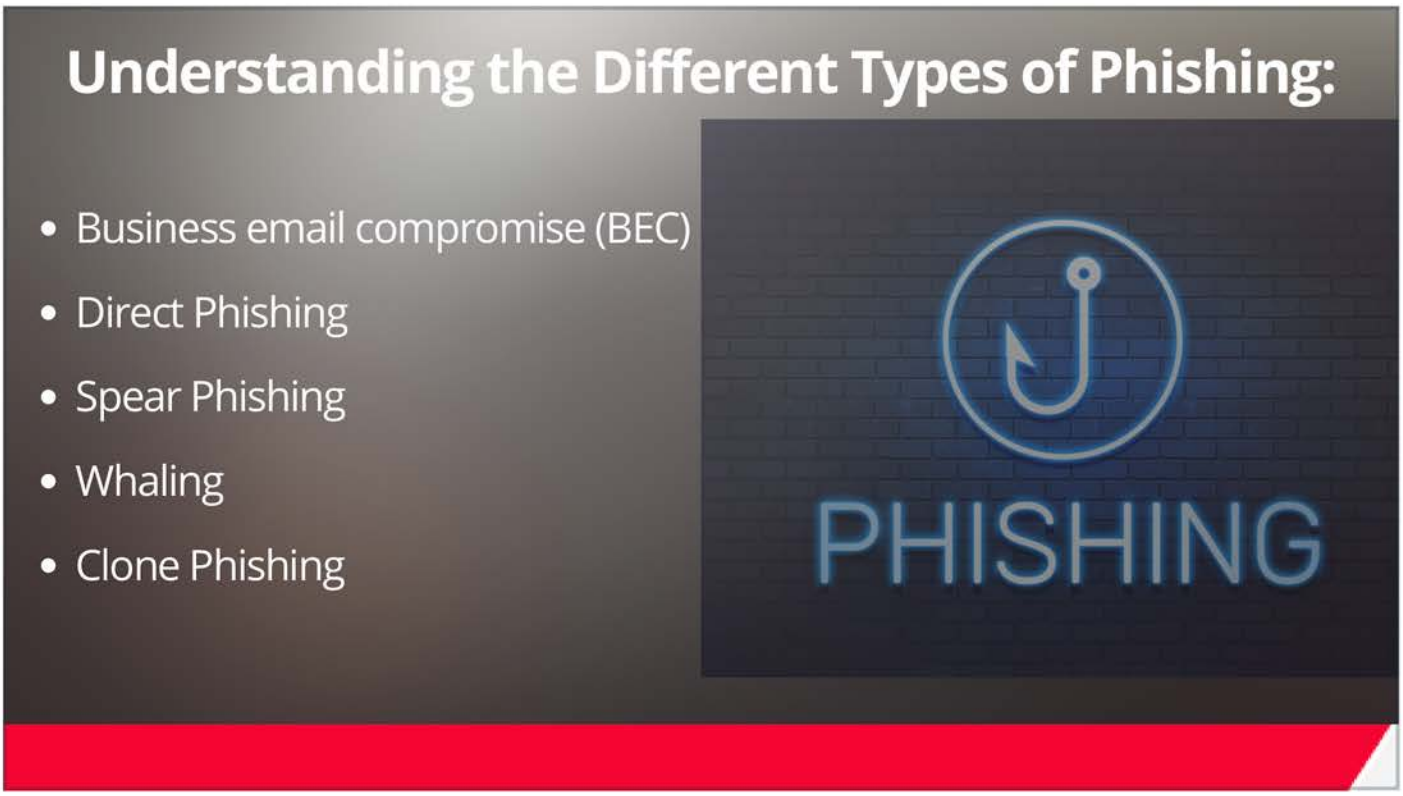
1. Stay informed about the latest social engineering techniques and scams, such as Phishing and pretexting, so you know what to look out for. A simple google search will reveal this information.

2. Don't trust unsolicited phone calls, emails, or messages, even if they appear to be from a legitimate source. Always verify the identity of the person or organization before sharing sensitive information.

3. Be careful about what personal information you share online and use strong passwords and two-factor authentication to protect your accounts.

4. Don't click on links or open attachments in emails or messages unless you are confident of their authenticity. Remember, if it asks you to perform an action or the message seems urgent, this is the time to stop and think before you click.

By being more aware of these tactics and taking steps to protect yourself, you can reduce the chances of falling victim to social engineering.



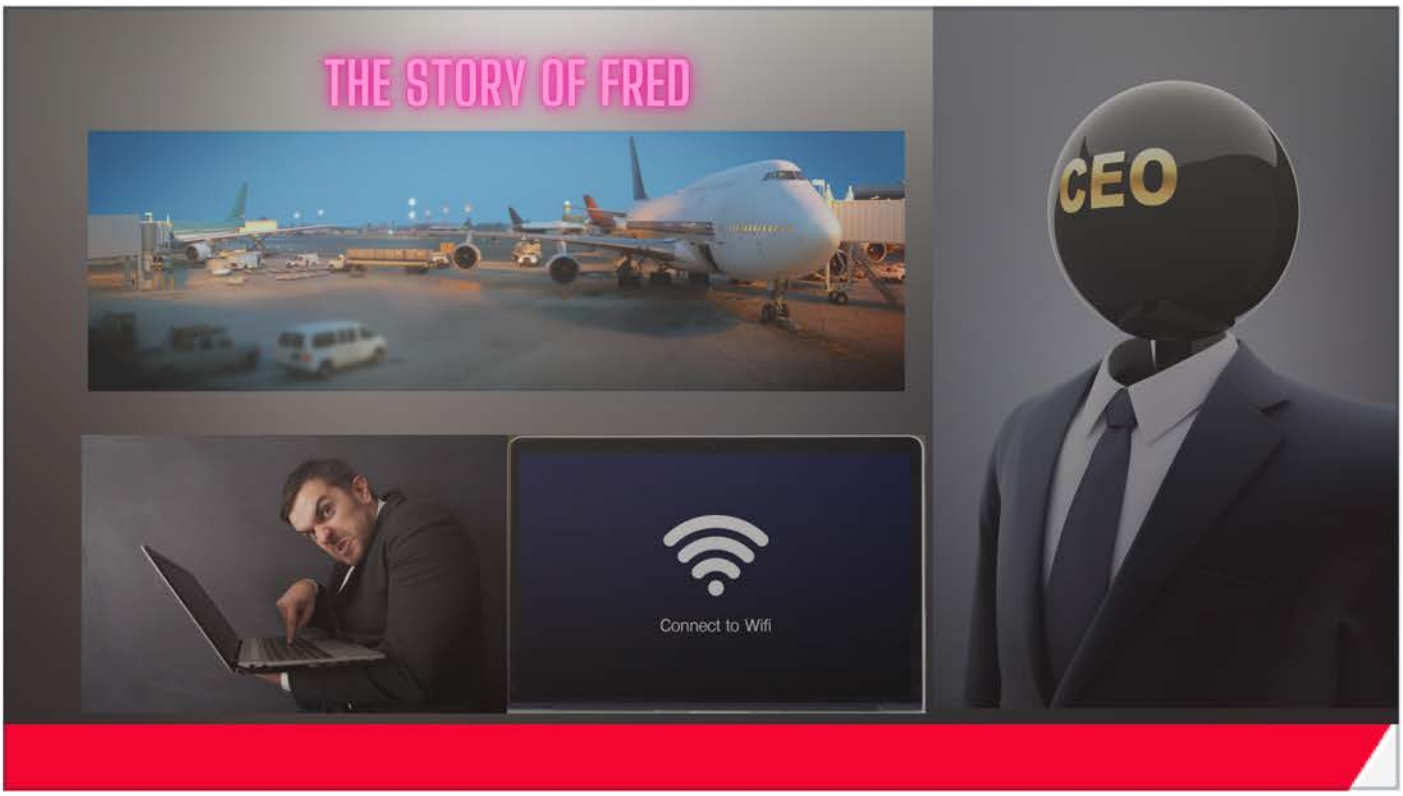
There are many forms of Phishing; I will address the five most common.

Let's start with Business email compromise (BEC)

BEC is a scam where attackers gain unauthorized access to a company's email account and use it to send fraudulent emails to the other company employees or the company's suppliers or customers.

The attackers often pose as an employee of the company and may request a transfer of funds or sensitive information.

BEC attacks are often a form of spear-phishing, targeting specific employees or departments within a company. The tactics, such as social engineering, Phishing, and malware infections can vary. But the goal is often to bypass security controls and trick employees into acting before thinking.



Let me tell you a story about Fred.

Fred is the CEO of a hospital and has been working hard to procure a new piece of medical equipment for the radiology department.

This equipment will set their facility apart from all the regional competition.

Fred was on his way back from a business trip. While at the airport waiting for his flight, he was talking with the vendor on the phone.

He must have been a great talker because he was able to procure a discount on the equipment, but it was necessary to close the deal that day.

So Fred drafted an email to his CFO informing them about the great news.

He asked them to send the money to get the deal done that day and provided the account information to wire the money. Everyone was very excited!

Unfortunately, While Fred was talking to the vendor, a nearby hacker overheard the conversation about the fund transfer and activated his wireless access point.

When Fred needed to connect to the internet to send the email to the CFO he unknowingly connected to the hacker's free hotspot and in his haste he forgot to activate his VPN.

The hacker set up packet sniffing and captured any information transmitted or received on that link. When Fred logged into his email, he provided his user credentials.

Once Fred was on the plane, the hacker used this information to log into Fred's email. After reviewing the previous email, the hacker formatted a new email to the CFO using the same format and language as the previous email, with a few modifications.

The hacker changed the account numbers to his untraceable account and let the CFO know he had made a mistake in the account information. The hacker added that he needed this done ASAP and that he was boarding the plane and would be unavailable for the next 2 hours.

I'm sure you can all guess what happened next!

Direct Phishing is a phishing attack in which the attacker sends an email or message directly to many potential victims, pretending to be a legitimate source, such as a bank or a government agency.

The message may ask the victim to click on a link or enter personal information on a fake website.

Did you know that Cybercriminals create over 1.4 million phishing sites every month.

An example of direct Phishing would be an attacker sending an email to a large group of people, pretending to be from a well-known financial institution such as a bank, claiming a problem with their account.

The email may ask recipients to click on a link to log in to their account and provide personal information, such as their passwords or Social Security number to verify who they are to resolve the issue.

The link in the email, however, would lead to one of those fake websites which would look identical to the bank's website, where the attacker would then collect the information.

Spear phishing is a more targeted version of direct Phishing. In this attack, the attacker spends more time researching and learns more about the victim to tailor the message specifically to them to increase the chances of success.

The message may use personal information, such as the victim's name or company name, to make it seem more legitimate.

An example of spear phishing would be an attacker sending an email to a specific individual, pretending to be their boss, asking them to transfer a large sum of money to a particular bank account. The email may use the boss's name and title and may even include their signature to seem more legitimate.

The email may also include details about an ongoing project or meeting to increase credibility further.

The victim, who believes the email is from their boss, may transfer the money without realizing it is a phishing attempt.

Whaling is a type of phishing attack that targets high-level executives or other high-profile individuals, who are known as "whales."

This is because, if successful, the attack generally has a high payout.

The messages sent to these individuals look like they are from other high-level executives or government officials.

The attacker will spend many hours researching the CFO to gather information on their job responsibilities, personal interests, or professional connections as well as researching any open projects they are working on.

Using this information, the attacker then crafts a personalized email to the CFO, posing as a trustworthy entity such as a vendor or a business partner.

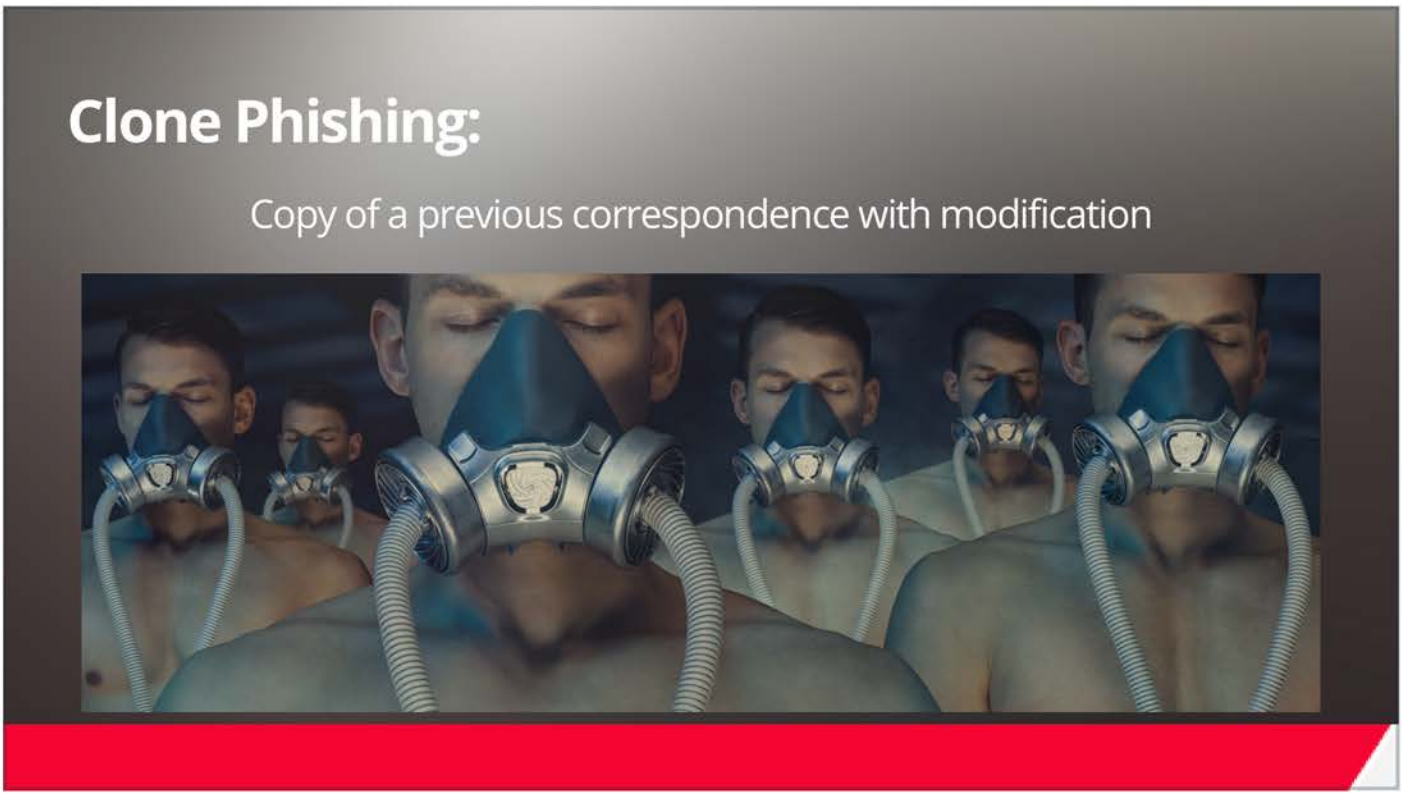
For example, the attacker might craft an email that seems to be coming from a legitimate supplier, and in that email, they might request the CFO to read the attached PDF, a policy on how to do business with them. The attacker will make the email seem more legitimate by adding details like the supplier's logo and letterhead. Because the email appears legitimate, the CFO opens the attachment without verifying the authenticity of the request.

Unfortunately, this PDF has specially crafted malware embedded that takes advantage of a known exploit in Adobe Reader and installs a trojan on their machine.

This trojan leads to the attacker compromising their payroll information and sending the next payroll run to fraudulent accounts stealing hundreds of thousands of dollars.

A similar scenario happened here in NE last year, resulting in over 250 thousand dollars lost.

It is essential to be aware that these types of attacks can happen and to take steps to verify the authenticity of requests, even if they appear legitimate. Executives and their staff need to be vigilant in verifying the authenticity of financial transfer requests, as they are often the target of whaling attacks.



Clone phishing is when the attacker creates a copy of an existing email, often one the victim has previously received, and replaces the email's attachments or links with malicious ones.

An example of clone phishing would be an attacker taking an existing email that a victim has previously received and trusted, such as an invoice or a shipping confirmation, and make a copy of it.

The attacker would then replace any attachment or links in the email with a malicious one. The attacker may also change minor details in the email to make it seem more legitimate as to why it is being resent or replied to.

The victim may be unable to tell the difference between the legitimate email and the copy and may click on the malicious links or attachments, exposing themselves to the attacker's scheme.

For instance, the attacker may have intercepted an email sent to the victim regarding a purchase order. The attacker would then use this information to clone the email and change the invoice attached with a malicious information. When the victim opens the email, sees the invoice from a business he trusts, and follows the instruction, he may transfer money to the wrong account.

Okay, we are through the bad stuff.

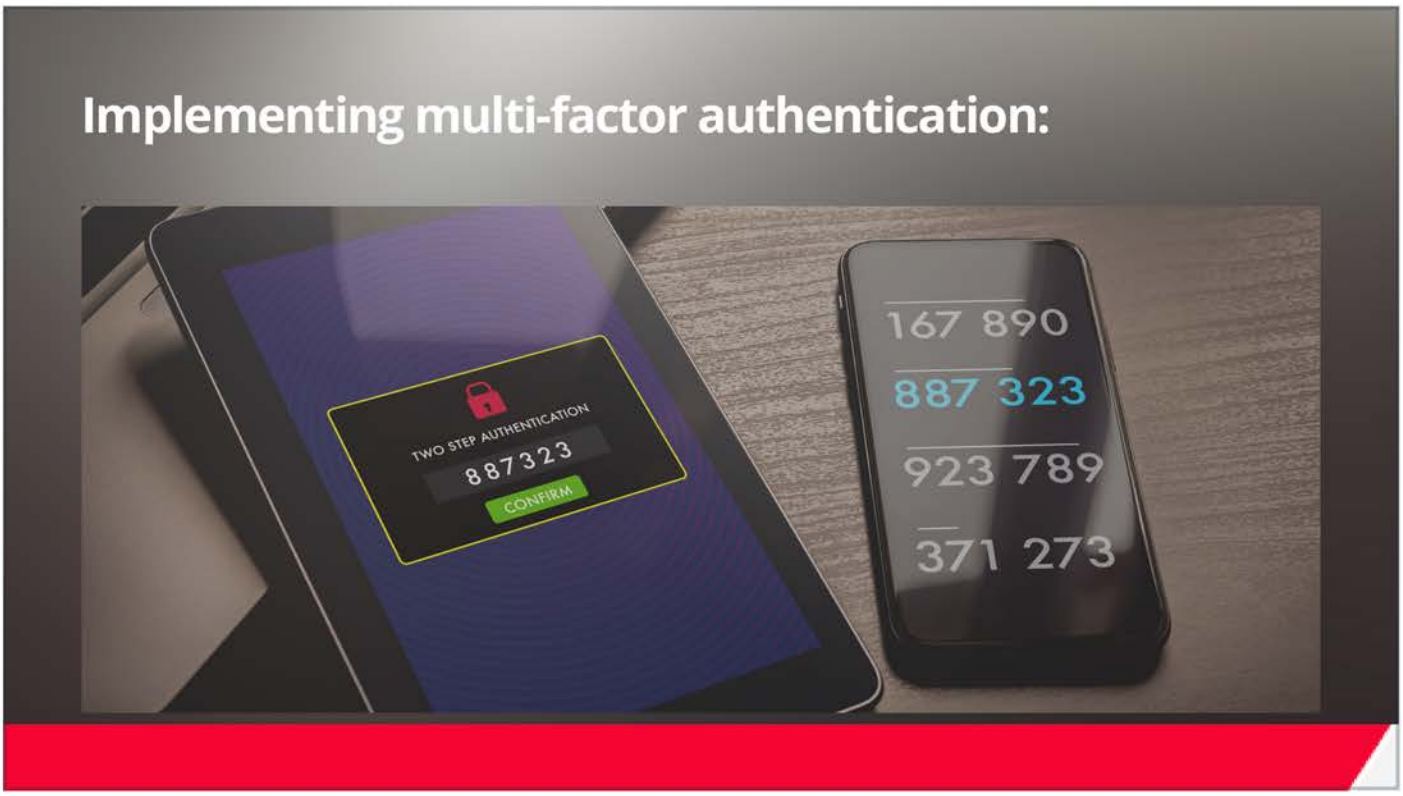
Let's discuss how we can avoid becoming a statistic and better protect ourselves and our organization.

One of the most effective ways to protect against Phishing is to educate employees on the risks and how to recognize and avoid phishing attempts.

Your organization Needs to be training employees on the different types of Phishing, such as spear phishing, whaling, and clone phishing, as well as how to spot suspicious emails and what to do if they receive one.

Providing regular training and reminders will help to keep employees vigilant.

This constant reinforcement helps to establish a culture of Cyber awareness.



Another way is utilizing Multi-factor authentication I am sure that most of you are aware of this. But are you using it everywhere you can?

(MFA) is an effective way to protect against phishing attacks because it requires an additional verification step, such as a fingerprint or a one-time code sent to a mobile device in addition to a password to access sensitive information.

Using MFA makes it much more difficult for attackers to access sensitive data even if they have a user's password!

While adding MFA to every authentication today is challenging, I would highly recommend it for all remote access and cloud services, for both business and personal.

Another protection is email filtering software. This can help to block phishing emails and other malicious emails before they reach employees. URL filtering software can help to block access to malicious websites by testing the URL in a sandbox prior to letting the user access it.

While they won't stop every attack, these tools can help to reduce the risk of employees falling prey to phishing scams.

It is essential to verify the authenticity of requests through official channels, even if they appear legitimate.

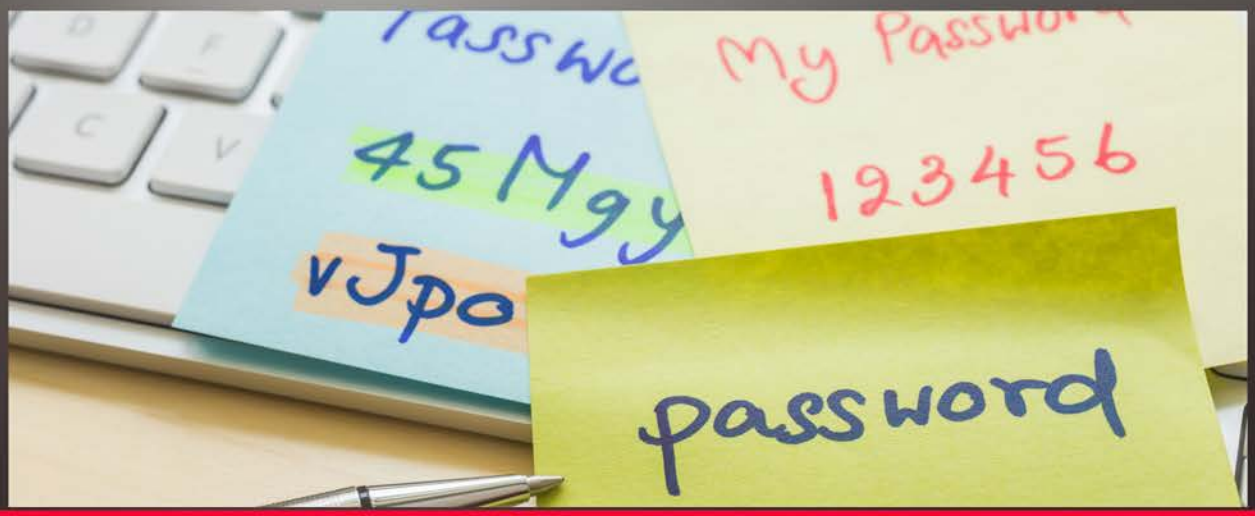
This includes confirming the sender's identity and checking the details of the request, such as bank account numbers or the link to a website, before acting.

Please pick up the phone and call the vendor to verify their information. Open your browser and type the published website of the company you are trying to reach. Don't ever rely on the contact information provided in a suspicious communication.

These simple steps can prevent a lot of damage.

Always remember that if it seems urgent and asks you to do something, you should be more cautious and take the time to verify.

Use a password manager:



Another useful tool and not widely adapted today is a password manager.

This is a tool that allows you to securely store and manage all your login credentials in one place.

Using a password manager, you can create strong, unique passwords for each of your accounts and quickly access them whenever you need to log in.

This tool helps protect your accounts from hacking attempts and other cybercrime and can save you time by eliminating the need to remember multiple passwords. So you can make your passwords unique and more complex.

Many password managers also include additional security features such as MFA and encrypted password sharing.
They also sync between your devices so your passwords are always available to you.

I would recommend that you research available password managers and pick one that is designed for the enterprise allowing you to manage and support the accounts for your organization .

A password manager will eliminate the need for all those bad habits we have developed over the years of dealing with the password nightmare, such as sticky notes, excel sheets, or other locally stored documents containing our passwords.

Using unique passwords prevents credential stuffing, which is an automated attack where a hacker uses a list of known email addresses and passwords (often obtained from a previous data breach and sold on the dark web) to try and log into multiple websites like Facebook, Twitter, or amazon. If you use the same password for numerous sites, you are at a much higher risk of becoming a victim.

As a Leader , you play a critical role in protecting your organization against Phishing and other cyber-attacks. Here are five things you can do.

1.
Ensure your organization has the resources to implement adequate cybersecurity measures, such as employee education and awareness training,
security software,
multi-factor authentication,
and incident response planning.

2.
Ensure that cybersecurity is a priority in budgeting and allocate funds for the necessary resources and staff to keep your organization safe and secure.

3.
Stay informed about the latest cyber threats and trends and ensure that your organization's cybersecurity measures are up-to-date and effective.

4.
Understand the financial impact of a cyber-attack, including costs related to recovery and loss of your business, and have a plan to address those costs if an attack occurs.

If you don't have Cyber insurance, you need to get it. If you have it, make sure it is enough to

cover your costs. More often than not it isn't. Also reach out to your insurance provider and run through a scenario to see what is and what is not covered.

5.
Encourage compliance with cybersecurity policies and procedures among employees, vendors, and business partners, and ensure that all stakeholders are held accountable for their actions.

A great website to get started building a culture of Cyber Readiness is cisa.gov.

Download the Cyber Essentials Starter Kit. This is a great resource.

It has a track for both Leaders like you and your IT Staff.

Let's take a look at this great resource.

CISA's Cyber Essentials is a guide for leaders of organizations to develop an actionable understanding of where to start implementing organizational cybersecurity practices.

I recommend starting with the Cyber Essentials Starter kit, a set of modules designed to break down the overall Cyber Essentials into bite-sized pieces for your IT department and leadership to work toward full implementation.

It is consistent with the NIST Cybersecurity Framework and other standards that are being adopted and accepted as the gold standard today for Cyber Security.

Managing cyber risks requires building a culture of cyber readiness. It needs to be constantly reinforced and led from the top down.

CISA breaks it down into 6 essential elements:

1. Yourself: Drive Cybersecurity strategy, investment, and culture.

Your awareness of the basics drives cybersecurity to be a significant part of your operational resilience strategy, and that strategy requires an investment of time and money. Your investment drives actions and activities that build and sustain a culture of cybersecurity.

2. Your Staff: Develop security awareness and vigilance.

Your staff will often be your first and last line of defense, one that must have and continuously grow the skills to practice and maintain readiness against cybersecurity risks.

3. Your Systems: Protect critical assets and applications.

Information is the lifeblood of any business; it is often the most valuable, intangible asset.

Know where your data is stored and what applications and networks you use to access that information. Then build security into and around these.

4. Your Surroundings: Ensure only those who belong to your digital workplace have access.

The authority and access you grant employees, managers, and customers in your digital environment need limits, just as those set in the physical work environment do.

Setting approved access privileges requires knowing who operates on your systems and with what level of authorization and accountability.

5. Your Data: Make backups and avoid the loss of information critical to operations.

Even the best security measures can be circumvented with a patient, sophisticated adversary.

Learn to protect your information where it is stored, processed, and transmitted. Have a contingency plan, which generally starts with recovering systems, networks, and data from known, accurate backups.

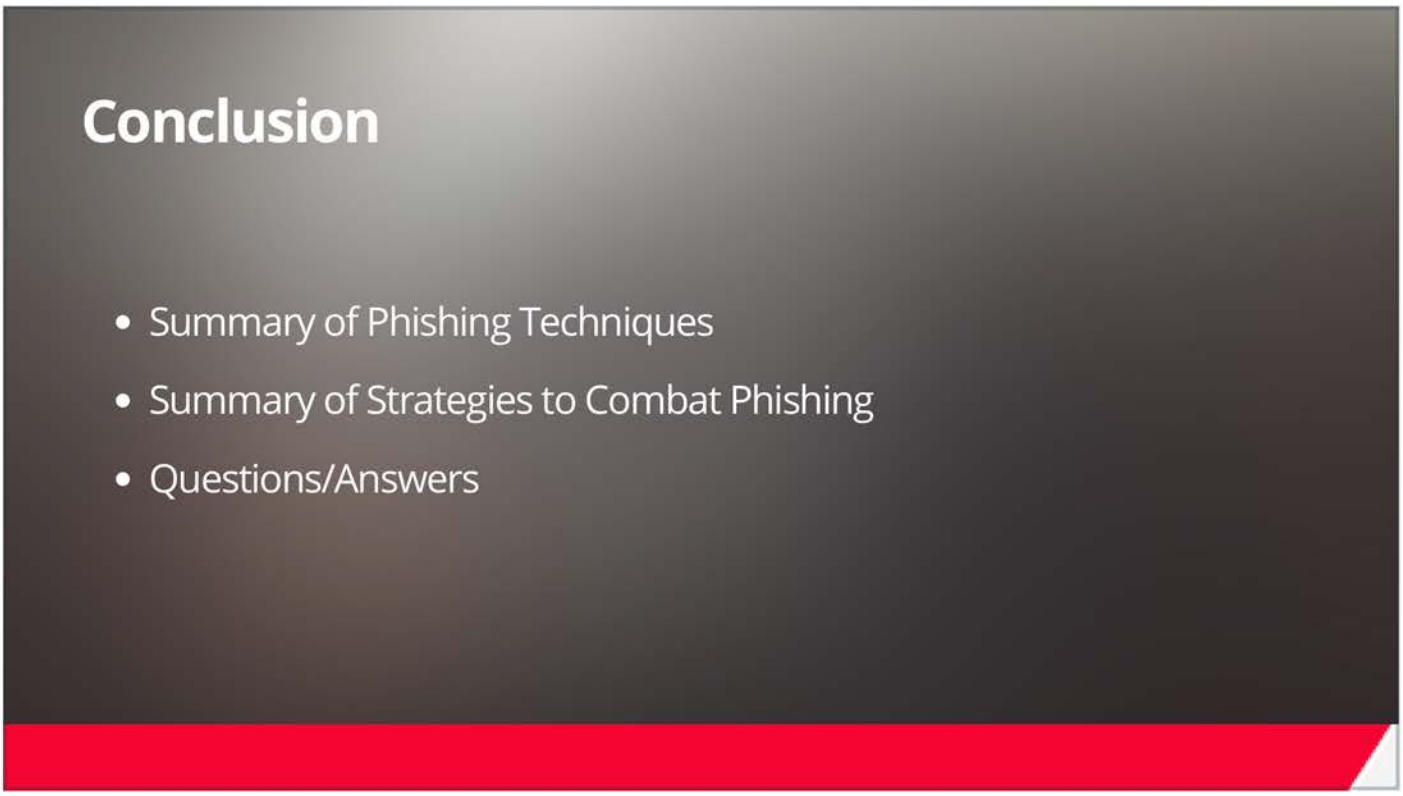
6. Your Crisis Response: Limit damage and quicken restoration of normal operations.

The strategy for responding to and recovering from a compromise is a plan.

Prepare for and conduct drills for cyberattacks as you would a fire.
Make your reaction to cyberattacks and system failures an extension of your other business contingency plans.

To be successful, you will need established procedures, trained staff, and knowing how - and to whom - to communicate during a crisis.

In summary, by having a plan in place, regularly training and educating employees, implementing strong security measures, regular testing and updating, strict access controls, monitoring network activity, clear communication lines, and incident response protocols. You can have a Culture of Cyber Readiness and an organizational mindset that practices and prioritizes the protection of its digital assets and systems from cyber threats.



Today we defined what Phishing is and covered the different types of Phishing techniques.

Which include Business email compromise, direct Phishing, spear phishing, whaling, and clone phishing.

Remember anyone is susceptible to Phishing, even a seasoned IT professional like me! It's essential to educate yourself and your employees, implement multi-factor authentication where you can and then continually reassess this.

Use email and URL filtering software, and above all, verify the authenticity of requests or email, even if they appear legitimate.

Now, go and build your culture of Cyber Readiness and above all Don't get hooked!

I would be happy to answer any questions.