the NetWork

LeadingIT

Chicagoland CybersecurITy Support

February 2021

Understanding The Nature

Of Cyber Attacks Targeting Your Business

Phishing Ranked The Most Prevalent Type

Of Cybercrime In The US As Cybersecurity Concerns Rise

LeadingIT Launches New IT Support Strategies To Conform With Cybersecurity Predictions For 2021 And Beyond

Understanding The Nature Of Cyber Attacks Targeting Your Business

Whenever you visit various IT media platforms, you may come across news about a big firm targeted by cybercriminals. Major news feeds have stories about big corporations or governments attacked by cybercriminals. They barely report about small and medium enterprises.

Does the media blackout mean the cybersecurity protocols of small and medium enterprises are immune to breaches?

Short answer, no. Cyberattackers often target small and medium businesses because they are easy targets.

What Makes Small And Medium Businesses Easy Targets For Breaches?

According to Fundera, 60% of cyberattacks target small enterprises. Small and medium businesses are easy targets for cybercriminals for various reasons.

• **Scarce Resources:** SMEs have scarce economic resources, meaning they must prioritize areas to allocate funds. Their inability to pay for excellent IT security programs and protocols leaves them exposed to many vulnerabilities, making them easy targets for cyberattackers.

• **Poorly Trained Staff:** Most SMEs' limited resources means they cannot hire adequate staff. The low remuneration and expertise demotivate the workers, and they strive to do the bare minimum. Various cybersecurity threats bypass them.

• **Poor Response Time:** Inadequate reporting and system analysis mean SMEs take time to identify threats. For example, cybercriminals can bypass their cybersecurity measures and spend days or weeks in the network before someone notices their presence.

Common Cybersecurity Threats To Small And Medium Organizations:

1. Phishing Attacks

Phishing attacks happen when cybercriminals send fraudulent communications that seem to be from a credible source. They can email team members pretending to be management. The email can have infected attachments or direct recipients to malware-laden sites. Unsuspecting employees open these attachments or links, infecting the network with malware that performs various functions.

2. Malware Attacks

Cyberattackers can target SMEs with malicious software, such as ransomware, spyware, viruses, and worms. Malware attacks take advantage of a network's vulnerability when you install compromised software or click dangerous links. The malware gives attackers control and disrupts some components.

3. Ransomware Attacks

Ransomware attacks entail cybercriminals taking over networks or stealing sensitive data. Once they achieve one or both targets, they demand payment from an organization to return things to normal. SMEs often struggle to pay the ransom, meaning they risk days or weeks of downtime. An SME's reputation can also suffer if attackers publish or sell clients' data online.

4. Weak Passwords

Many SMEs' workers have little to no training on cybersecurity. This unawareness means they can make mistakes, such as having one password for all their platforms. Some use obvious details to generate their passwords, such as their birth date or pet's name. Cybercriminals can crack their password with little of their personal information.

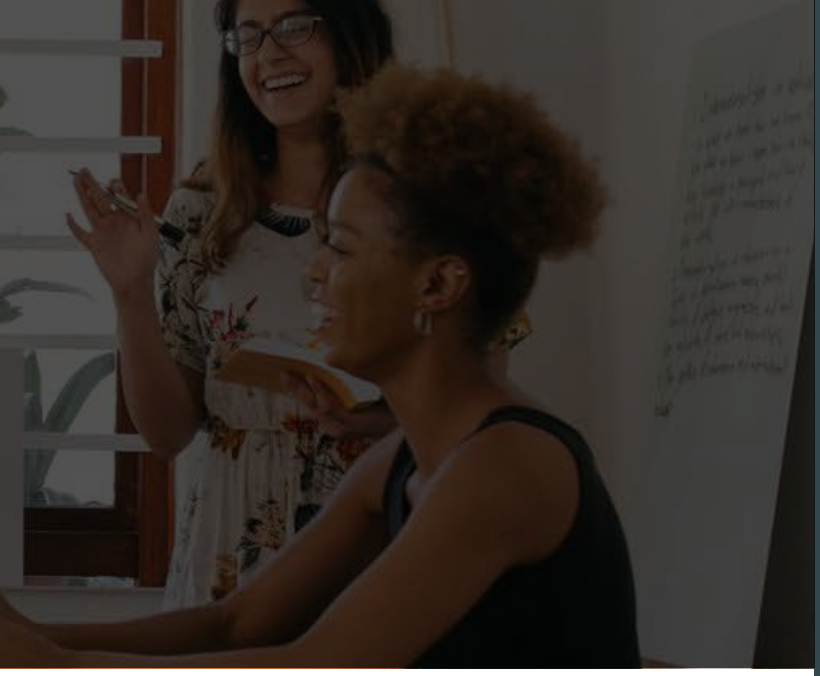
Here is what you can do to ensure you stay safe:

1. Train Your Staff: Many attackers target human weaknesses. Training your employees on cybersecurity threats and protocols can reduce your exposure to attacks.

2. Create Backups: Having backups of essential data can ensure your business remains operational after an attack. For example, ransomware may not cause downtime.

3. Prioritize Cybersecurity: Limit your vulnerabilities, and use antivirus, antimalware, and antispyware programs.

4. Encourage Your Employees to Report Suspicious Behavior: A reporting culture enables you to check out potential threats and develop measures to mitigate against them.



5. Instruct Employees to Change Passwords Frequently: This approach ensures cyberattackers have a tough time cracking their passwords.

6. Review and Improve Your Cybersecurity Measures: Reviewing your progress allows you to keep up with the ever-changing threats and seal loopholes.

7. Limit Access to Your Network: Employees should only access the parts they need. This approach ensures your entire network is not compromised if cyberattackers compromise one employee.

What Are The Benefits Of Having Excellent Cybersecurity Measures In Place?

• No Downtimes: Your business can continue normal operations if cybercriminals breach your network. Your backups enable you to operate, ensuring you don't lose revenue through unfulfilled orders or lack of communication with clients.

• Protect Your Clients' Privacy: You will safeguard sensitive information, such as your clients' addresses, contact information, and social security numbers.

• Avoid Financial Losses: You will not spend resources rebuilding or patching your network after an attack.

• Protect Your Reputation: Your standing with stakeholders can take a hit if they know cybercriminals breached your network. Reliable cybersecurity helps you stop these attacks, preserving your reputation.

• Avoid Legal Trouble: You may face legal issues with government agencies and clients if you fall victim to cyberattacks. These cases can lead to hefty fines, revocation of licenses, or jail time.

Phishing Ranked The Most Prevalent Type Of Cybercrime In The US As Cybersecurity Concerns Rise

What Is Phishing? Phishing.org defines phishing as a cybercrime type where attackers reach out to their targets via telephone, emails, social media platforms, or text messages. The attackers contact their targets by pretending to be legitimate institutions.

The Most Common Phishing Methods Include:

• **Spear Phishing** - Spear phishing is specific and often targets system administrators of companies.

• **Whaling** - Attackers use the whaling method when their targets are the big fish, such as CEOs, Directors, CFOs, or any senior managers.

• **Smishing** - This type of attack uses text messaging to get the attention of the target. These messages often contain a link or a phone number that the attacker expects you to call or click.

• **Vishing** - Vishing has the same objective as the rest of the models. However, it uses phone calls as the primary channels to deliver the attacks.

• **Search Engine Phishing** - Sometimes, attackers use SEO Trojans or SEO poisoning to deliver attacks to surfers.

3 Tips On How To Prevent Phishing

• **Phishing Assessment and Information** - Interestingly, up to **70%** of enterprises don't carry out cybercrime assessments. This makes them pretty vulnerable as an assessment aims to identify and address possible loopholes.

• **Don't Click On Suspicious Emails** - Any unsolicited emails that are too good to be true, sound pretty urgent, and have suspicious links or attachments are red flags. Consider using spam filtering mechanisms to get rid of unsolicited emails.

• **Update Your Browser** - Keeping your browser up to date helps to shield you from security threats that attackers may exploit.

LeadingIT Launches New IT Support Strategies To Conform With Cybersecurity Predictions For 2021 And Beyond

CHICAGO, Ill., Jan. 11, 2021 (SEND2PRESS NEWSWIRE) — LeadingIT, a Chicagoland cybersecurity and IT support company, today refreshed their previously launched cybersecurity measures to help its clients curb the increasing menace of cyberattacks. The launch comes when internet usage and online networking rose to unprecedented levels following the stay-at-home orders and other COVID-19 containment measures.

Across the nation, many corporate employees lost jobs or went out of office confinements to work from home, the internet has been pretty busy. While the world may not experience a surge in new deaths or infections with the rollout of vaccines, the chaos witnessed online will not stop soon. Predictions are rife with new cybersecurity predictions for 2021 and afterward. Being a leading IT company in the area (pun intended), LeadingIT has plans to help its old, new, and prospective clients develop mitigative measures for all the potential threats in 2021 and beyond. These plans were announced as the company celebrates a decade of providing fast + friendly IT support.

10th Anniversary of Provided Excellent Always Available Support

LeadingIT has been around for ten years now, which is no mean feat. The company works with institutions, religious organizations, corporates, businesses, nonprofits, and government entities to provide them with managed services in the information technology and cybersecurity sectors.

"It is quite an achievement to be around for ten years now. Sincerely, the journey hasn't been a walk in the park. We pass our sincere gratitude to our partners, staff, and friends for supporting us through the journey," said Stephen Taylor, the CEO of LeadingIT, in acknowledgment of the company's decade-long service in IT support.

Stephen Taylor continued, "However, we won't let the 10-year celebrations deter us from focusing on the continued cybersecurity threats. Cybercriminals thrive where there is chaos. Thus, the chaos of 2020, together with upcoming events such as the Tokyo Olympics, will provide an opportunity for attackers to prey on your servers, data, and teams."

Specific Cybersecurity Predictions for 2021

According to a report by The University of Maryland, there is an average of 2,224 hacking attempts every day. That translates to an average of one attempted hack every 39 seconds. And with these predictions bound to continue, it signifies a worrying trend for 2021 and beyond.

Notable predictions include:

• Cyberattackers will try to gain access to systems via the over 300 billion passwords and usernames used globally.
• Systems, organizations, and individuals without Multi-Factor-Authorization will suffer security breaches.
• Attackers will continue to swarm RDPs and VPNs as the rise in the remote workforce continues.
• Home networks, computers, and servers will face a higher risk of attacks.
• 55% of enterprises will increase their IT support budgets, according to a Global Digital Trust Insights report.
• Identity management, network security, and messaging security will be the top areas that businesses will spend on.

Measures to Curb the Top Cyberattack Threats in 2021

LeadingIT is at the forefront of helping its clients conform to the latest IT and cybersecurity trends. Stephen Taylor said, "These threats our very real for all businesses but we've built a 7-layer cybersecurity "jacket" to prevent data breaches, ransomware, and forced downtime."

The company believes that ensuring best practices, advanced endpoint detection, two-factor authentication, cybersecurity education, and more will be key to keeping clients safe in 2021 and beyond.

WE ARE CELEBRATING!

Anniversaries

Josh Laemont – Feb 1, 2017

Andy Latos - February 3, 2014

Birthdays

Jason Jimenez - February 9th

Read Our Blog For More
https://www.goleadingit.com/blog