the NetWork

LeadingIT

Chicagoland CybersecurITy Support

July 2022

66% of Organizations Were Hit by Ransomware in the Last Year. Are You Next?

How Phishing Simulations Can Improve the Security of Your Organization

Lessons Learned: How to Prevent the Next Big Cyberattack

LeadingIT Intern Spotlight

GoLeadingIT.com (815) 893-2525 @leadingit-solutions

66% of Organizations Were Hit by Ransomware in the Last Year. Are You Next?

No matter what type of business you operate, you live with the constant threat of cyber attacks. Without adequate IT services, your organization may be even more exposed than you realize. Phishing attacks and ransomware can cost companies countless time and money. Despite the danger, many companies have yet to take the threat seriously. When organizations remain unprotected and lack a recovery plan, the right attack could spell disaster. Below are some of the cyber security issues that companies face that leave them exposed.

Failure to Recognize the Threat

For many organizations, cyber threats seem like a worry for companies of different sizes or in different industries. Unfortunately, this leads some to ignore the need for professional IT services that can help protect digital assets. However, businesses of all sizes and in all industries are susceptible. Hackers are looking for easy targets, and they often find them in companies that least suspect an attack.

Failure to Educate Employees

Your employees are the first line of defense against cyber attacks. This is because they are often the initial target for phishing and ransomware attacks. While the right IT services can ensure that your hardware and software are secure, employee education is essential to keep your systems and data safe. Let your people know what to look for and what to do when they suspect a threat. Also, don't forget that this needs to be an ongoing effort, and cybercriminals are constantly developing new approaches. The right IT service provider can connect you to resources to help keep your employees up to date and on the lookout.

Treating Cybersecurity as an IT Issue Only

Too many businesses fall victim to cyber-attacks because they see them only as an IT issue. However, whether your IT services are handled in-house or by a managed IT services provider, it is not enough to think of cyber risks as just a technical issue. Cyber attacks are, in fact, a financial issue. The cost of recovering from a ransomware attack or other cyber intrusion can be enough to send even a healthy company into bankruptcy or entirely out of business. Therefore, everyone from top leadership to line employees needs to be aware of the threat and part of mitigating the risk.

Ignoring the Threat of Remote Work

Whether it was related to the pandemic or just a part of a company's business model, remote work is here to stay.

Amy

Unfortunately, by its nature, it opens up organizations to a greater risk of attack. When all employees are on-site, it is simpler to develop IT solutions to keep data in and intruders out. However, employees connecting remotely create many more potential points of failure. This requires more robust IT services and a clearer focus on security to maintain control of your data and systems.

Failure to Create a Backup Plan

With the right IT service provider, you may be able to avoid a ransomware attack or other data breach. But don't count it. Smart companies do everything possible to avoid an attack but have a clear plan in place to recover in the event of the worst happening. Companies need robust ongoing backups that make it easy to restore in the event of an attack or any other disaster that requires restoration of data.

Don't Be Next

Cybercrime isn't going away any time soon. It is a reality all businesses must deal with. Fortunately, with the right IT services, staff education, and planning, you can avoid an attack and be ready if someone does manage to defeat your defenses. Be sure you are ready.

Pictured on the cover: Nathan and Scott

How Phishing Simulations Can Improve the Security of Your Organization

According to an IBM study, data breaches costed businesses an average of $4.24 million per breach in 2021 alone. This is why it's integral for businesses to take steps to secure their data from bad actors. In fact, data breaches and cyber-attacks represent one of the costliest threats to businesses today.

And one of the leading causes of data breaches is phishing.

What is Phishing?

One of the most effective types of cyberattacks over the past few years has been phishing. Phishing attacks happen when a person sends a fraudulent message that appears to come from a trusted source. It is normally carried out via email. According to a Proofpoint survey, 83% of organizations fell victim to an email-based phishing attack in 2021, with 54% reporting dealing with over three cyberattacks in the same year.

Phishing puts individuals and organizations at risk because it gives cyber-criminals access to proprietary company information, personal data, financial information, and other sensitive information.

In fact, some companies may be blacklisted by internet or financial services companies in extreme situations of phishing attacks. This prevents the organizations and their staff from communicating with the outside world and paying for goods and services. One of the most effective IT solutions that organizations use to tackle phishing is a phishing test or a phishing simulation.

The Role of IT Services

A phishing test is a practice where security and IT service experts create fake phishing emails and send them to employees. These spoof attacks teach employees how to recognize genuine phishing attempts and how to protect their data from cybercriminals who use this technique.

Phishing tests improve the cybersecurity awareness of employees in a practical, safe setting. Employees gain actual phishing experience while avoiding the risks. They are also given the opportunity to improve their cybersecurity practices in a significant manner. Employees that fail the phishing test are typically given instructions on how to improve their ability to recognize phishing emails in the future.

Continue reading on page 4

LESSONS LEARNED:
How to Prevent the Next Big Cyberattack

In less than one year, we witnessed two of the most significant cyberattacks in history. The Colonial Pipeline ransomware attack caused a jet fuel shortage for many air carriers and cost them an estimated $5 million, while the Marriott breach involved more than 5.2 million guests, damaging their reputation and costing them millions in fines.

Cybercrimes have a large impact on companies and individuals. The cost of cybercrimes is expected to reach $10.5 trillion by 2025, so it's essential to understand how to prevent an attack from happening to your business. ***Here are four key insights on how you can protect your business.***

1. Train your front-line defense.

Human error is at blame for 95% of cybersecurity breaches. Any threat mitigation technology or firewall is worthless without providing cyber literacy training to your employees.

2. Understand your risks.

Many may assume that large companies are more at risk for a cyberattack. However, small businesses account for 58% of malware attack victims.

3. Create reliable backups.

Backing up regularly and keeping backups on different servers to prevent infection is an excellent foundation for ransomware protection. You can get your operations back up and running with quality backups while minimizing ransom payment costs and downtime

4. Keep your systems and software up to date.

Cyberattacks often occur because your systems or software are not current, exposing vulnerabilities. Installing updates and patches guarantees that you are running the most secure programs and software versions.

Continue reading: goleadingit.com/blog

LeadingIT Intern Spotlight:

Nathan

Bench and Delivery Technician

• What drew you to LeadingIT originally?

I came to LeadingIT during a field trip for my high school. I met quite a few members of our team while I was here and also set up a job shadow for school. I shadowed both Peter and Steven, and I fell in love with IT more.

• In your time at LeadingIT, what has been your favorite project?

My favorite projects are the ones where I have to ask my teammates for help. I enjoy learning new things and struggling on something. Configuring a VPN can be as simple as going to a friend.

• If you could switch positions with anyone at LeadingIT who would it be and why?

I would enjoy to see what a day in Stephen Taylor's life would be like. Owning a business is a dream of mine and getting a behind-the-scenes of what business is like, would be great experience.

• What would you say to someone considering a career with LeadingIT?

I would tell them to keep your options open when applying/working here. There is definitely more positions for this business than meets the eye.

• If you could snap your fingers and be an expert at something, what would it be?

If I could be an expert at anything, I would have to choose computers. Being able to do anything with your car's computer, your own computer, or anyone else's computer without needing to look it up would save so much time.

Phishing Simulations continued...

The Results IT Services Can Give You

Phishing simulations provide several distinct advantages for businesses. This includes raising awareness of potential threats and providing employees with the information they need to identify social engineering attacks. By conducting phishing tests on a regular basis, companies can increase their employees' cybersecurity awareness and teach them to recognize the major warning signs in phishing emails.

Furthermore, as employees become more aware of potential phishing scenarios, they will act as the first line of defense against such emails. This should be an easy sell to the employees since the lessons learned will also help them outside of work. Anyone can be the target of a phishing or social engineering attack.

Simulated phishing campaigns with proper reporting protocols are a great indication of an organization's strong security culture. As a result, the likelihood of fraudulent behavior decreases.

Awareness Increases Security

Phishing tests can be a great way to identify any holes or vulnerabilities within an organization. Training can be a great way to increase awareness of potential problems, but a test will ensure the material is being put into practice.

Security is the collective duty of all employees in a company. But people must be aware of the threat in the first place. LeadingIT is an expert in cybersecurity and IT support for companies of all sizes. We provide decades of experience and expertise to ensure your business and data stay safe from cybersecurity threats, so you can focus on what matters.

LeadingIT

Serving the Chicagoland area with offices in Woodstock, Downtown Chicago, and now in Manteno, IL.

Check out our blog at goleadingit.com/blog

WE ARE CELEBRATING

Birthdays

Mark Seplowin - July 9th
Michael Seplowin - July 9th
Peter Apostle - July 23rd

Anniversaries

Dave Gregory - 7/22/2013