PALMTECH
I.T. Solutions For Business

THE PALMTECH TIMES

PalmTech Computer Solutions | October 2021

"I DIDN'T KNOW"

Unfortunately, That Excuse Doesn't Replenish Your Bank Account, Resolve A Data Breach Or Erase Any Fines And Lawsuits.

It's coming ...

- That day a hacker steals critical data, rendering your office useless ...
- That day when your bank account or credit card is compromised ...
- Or that day when your customers' private lives are uprooted ...

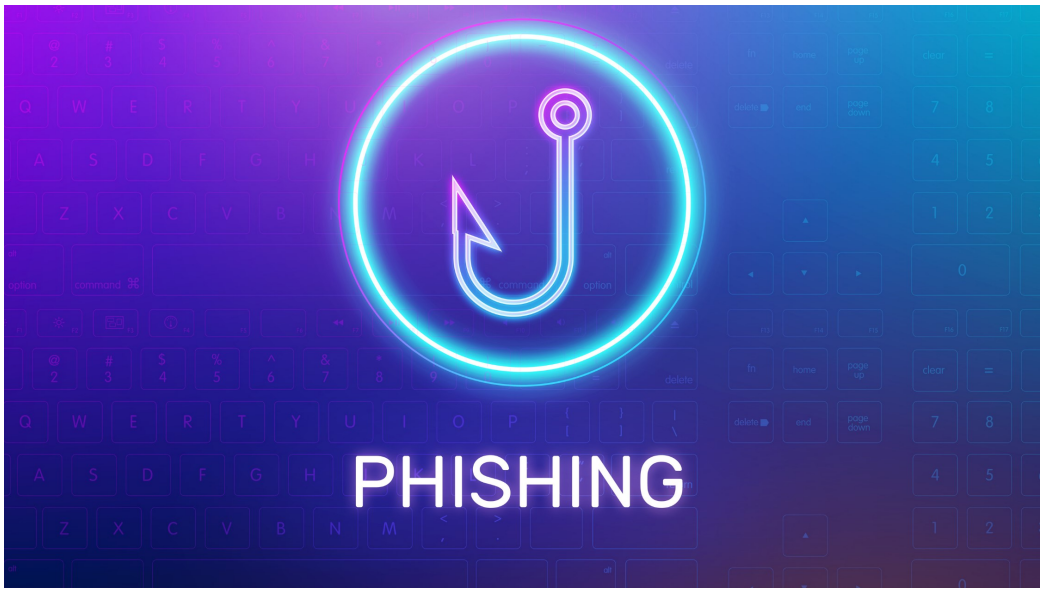
Cybercriminals are constantly inventing NEW ways to infiltrate your company, steal your assets & disrupt your life. The ONLY way to STOP THEM is by CONSTANTLY EDUCATING yourself on how **to PROTECT what's yours!** We can help! Sign Up for our "Cyber Security Tip of the Week". You'll receive byte-sized quick tips via email packed with solutions to stay one step ahead!

www.palmtech.net/resources/cyber-security-tip-of-the-week/

This monthly publication provided courtesy of Chuck Poole, CISSP, CEO of PalmTech Computer Solutions.

Our Mission

To equip small and midsized businesses in the West Palm Beach area with a smooth running and seamless IT platform that enhances productivity, improves efficiency, and creates a competitive advantage.



1 In 4 Companies Is At Risk For A Phishing-Related Data Breach

Workers are more plugged in than ever as the rise of remote and hybrid work has created an extremely email-dependent business world. More than half of all remote workers rely on email as their primary form of communication. At the same time, we've seen a historic increase in both phishing and data breach risk for the past two years, spawning an email security problem that impacts every business. An estimated one in four businesses had an email security breach in 2020, and one-third of these email security breaches can be traced to phishing.

The relationship between phishing and a data breach has been apparent for years. A solid 90% of incidents that end in a data breach start with a phishing email. This is reflected in the Verizon Data Breach Investigations Report 2021 (DBIR). Once again, phishing takes the crown as the top data breach threat that organizations face. This is the third year in a row that phishing has topped the chart, beating out insider acts, malware, and even human error, but it doesn't stop there – phishing that directly caused a data breach increased by 10% in 2020 and that's a substantial jump. The risk of phishing causing a data breach is so severe that the phishing category still tops the DBIR list even without the inclusion of ransomware, which has grown into such a behemoth that it's earned its own category.

continued on page 2

Phishing-Related Data Breach Facts To Remember

- An estimated 75% of organizations in the United States were hit by a successful phishing attack that resulted in a data breach in the last 12 months
- Just under 95% of ransomware arrives at businesses via email
- Precisely targeted ransomware, typically delivered through spear phishing, has grown by 767%
- The number of data breaches that involved ransomware doubled in 2020
- Cloud data breaches, enabled by phishing, are up more than 35% in 2021 over 2020

More Emails Means More Phishing

This rise in phishing risk that can put a company on the path of a data breach tracks with the tremendous increase in email volume that started in March 2020, because more email coming into businesses means more phishing messages that could land in an employee inbox, and any phishing message that an employee receives has the chance of spawning a data breach. An estimated 306.4 billion emails were sent and received each day in 2020, triple the average increase of past years. That figure is expected to continue to grow steadily as companies continue to grapple with the implications of the ongoing pandemic and virus variants that could lead to long-term remote work becoming the norm. If email volume continues to trend the way that experts expect, it is estimated to reach over 376.4 billion daily messages by 2025.

Phishing Carries Ransomware That Can Be Used To Snatch Data

Add a side of ransomware to that phishing and it ratchets up the danger of a data breach. Data is a valuable currency on the dark web and the dark web data markets are hot. Cybercriminals can make a solid chunk of change from a ransomware attack even if the victim doesn't pay just from selling off the data that they stole in the incident. One unlocked database can go for as much as $20,000, or up to $50 per 1,000 entry – and that database can be sold many times to different interested parties. Password lists are extremely desirable. Valuable database records typically include some personally identifying information (PII) in each entry like username, email address, full name, phone number, home address, date of birth and occasionally social security and identification numbers.

Fight Phishing Through Security Awareness Training

Phishing-related data breaches are the most common kind. That means businesses that want to reduce their chance of a data breach need to implement measures that reduce the chance of phishing incidents landing successfully. A solid grasp of email handling best practices and the threats that businesses face can help reduce risk faster than you might think.

Every time an employee resists or reports a phishing message, their company dodges a bullet and a big bill. But getting a business in a position to reap rewards like that involves putting work and investment into **security awareness training.** Many businesses may not see the value in something as nebulous as security awareness training, especially with IT departments facing major budget cuts. However, that investment in security awareness training pays off handsomely and it has a strong ROI. On average, smaller organizations (under 1,000 employees) can enjoy an ROI of 69% from a training program.

If you'd like assistance putting a strong phishing-defense system in place for your employees, contact us at info@palmtech.net or 561-969-1616.

Are Your Employees' Credentials For Sale On The Dark Web?

Visit www.palmtech.net/darkweb/ For A Free Scan!

DON'T BELIEVE THESE DISASTER RECOVERY MYTHS!

Modern technology changes rapidly, but not all businesses can match its pace. When it comes to disaster recovery (DR), for instance, we see business owners clinging to ideas that no longer apply. It's high time you learn the truth about the following DR myths so you can stop believing them.

MYTH 1: TAPE BACKUPS ARE THE BEST SOLUTION

Tape backups are physical objects that deteriorate over time. Try listening to a cassette tape from the '90s. Its sound may be distorted already, or it probably doesn't work at all. Similarly, your tape backups will start to fail over time. At first, only a few files may be affected, but you will gradually lose all your data.

It is also a common practice to store another set of tape backups outside your premises to secure them in case a natural disaster befalls your office. However, if your storage spaces themselves are unsafe from natural disasters, this could pose a problem.

Unlike tape backups, cloud-based backups are safe from deterioration. They are also stored in multiple secured locations that are protected from natural disasters, so your data backups are as safe as they can be.

What's more, cloud-based backups save you time in many ways. Data is automatically backed up online, so you don't need to manually copy information onto your tapes. You also won't need to manage boxes of tapes, freeing you to focus on more valuable tasks.

MYTH 2: THE RTOs YOU WANT ARE TOO EXPENSIVE

Essential to any DR plan is its recovery time objective (RTO), which is the ideal period when everything must be up and running again to avoid serious losses. Before the cloud, a "swift" recovery time would take days and cost up to six figures.

Cloud and virtualization solutions have made this much faster and affordable than ever before. Most DR providers can back up your critical data in an hour or two. And if you ever need to recover data, most services can do so in less than a day.

MYTH 3: DISASTER RECOVERY IS FOR BIG BUSINESSES, NOT SMBs

Due to the astronomical costs previously associated with DR, only big businesses could afford backup and recovery solutions. Thanks to the cloud, however, these have become more affordable for small- and medium-sized businesses (SMBs). From dental offices to small retail operations, SMBs can now take advantage of the best DR solutions in the market. Advances in IT and the cloud have also eliminated the obstacles of complexity, costs, and insufficient IT resources.

We hope that by dispelling these myths, you'd be convinced to implement a disaster recovery plan (DRP) for your business. Thanks to improvements in data storage technologies, it is now more affordable and efficient to implement a DRP, in turn making it easier to ensure BC. If you'd like to learn how our DR solutions can safeguard your business, email us at info@palmtech.net or call us at 561.969.1616.

For more mythbusting, don't miss our recent blog post - Cybersecurity Facts vs Myths: **www.palmtech.net/mythbusting/**

MYTHBUSTERS

Top Tips When Selecting An MSP For Your Business

Technology underpins nearly every aspect of modern business processes. Managing it, however, can be complex and tedious. This is where managed IT services providers (MSPs) can help. Whether your company needs software solutions, network infrastructure management services, or cloud technology, MSPs can provide all this and more.

MSPs Defined

MSPs are companies composed of specialists from various IT fields. They deliver various IT services (e.g., cloud computing, cybersecurity, backup and disaster recovery) and proactively manage their clients' IT systems under a subscription model.

Selecting The Best MSP

While there are numerous MSPs out there, not all of them are equipped to meet your company's unique needs. You can only achieve optimum IT results by selecting the right MSP.

Here are some criteria to keep in mind:

Depth of skills and experience – An MSP should have the skills and experience that go beyond basic software installation, maintenance, and upgrades. They should also have strong expertise in advanced IT functions, such as database management, cloud technology, security, and cross-platform integration, so they can keep pace with your company's growing IT requirements.

Financial stability – With IT being the backbone of your business operations, you need an IT partner who will be there for the long haul. Assess their stability by looking into their annual reports and financial statements. Check how many clients they have and their customer retention numbers. Also, read customer reviews and testimonials online customer reviews and testimonials.

Competitive service level agreement (SLA) – An SLA is a contract that dictates the standards that your MSP must meet. It should be able to answer these questions: Do they offer 24/7 support? Can they conduct remote and on-site support? What are their guaranteed response and resolution times? If they fail to meet their committed service levels, do they offer rebates or money-back guarantees?

Third-party vendor partnerships – Pick an MSP with an ongoing relationship with the technology vendors (e.g., Microsoft, Oracle, Salesforce) whose products you already use in your IT environment. Verify the partnership the MSP has with those vendors. The higher the partnership level, the more vendor certifications the provider has, which means they can provide plenty of expertise to your business.

Choosing the right provider is a crucial decision that will impact your business's performance and success. If you want to learn more about how MSPs can support your business, contact us today at 561-969-1616.