the NetWork

LeadingIT

Chicagoland CybersecurITy Support

February 2025

- Why Are Password Changes Required? Keeping Your Data Safe Made Simple
- How Your Business Can Outsmart New Phishing Tactics
- EOS: A Powerful Framework for Business Growth
- Stop Paying for IT Emergencies and Invest in Smarter Solutions Instead
- LeadingIT Values Victor

GoLeadingIT.com 815-788-6041 @goleadingit

WHY ARE PASSWORD CHANGES REQUIRED?

Keeping Your Data Safe Made Simple

Everything from your bank account to your pet's vet records lives online, so keeping your data safe is beyond important. And yet, few things are as universally hated as the dreaded "Please update your password" notification. But why is this necessary? Let's take a closer look at why password changes matter and how they help keep your data secure.

The Role of Passwords in Security

We all know by now that passwords are the first line of defense against unauthorized access to your accounts. Without a strong password, anyone can stroll in. Unfortunately, though, even the strongest passwords weaken over time. Why? Because hackers are relentless, and time is on their side.

According to GoodFirms' 2023 survey, 30% of IT professionals reported experiencing a data breach due to weak passwords. That's a stark reminder of why vigilance matters.

Why Passwords Need to Be Updated

Over time, passwords can become less secure, and sticking with one password forever is like leaving your door unlocked because it hasn't been kicked in yet. Here's why this strategy is risky:

1. Data Breaches

In 2024 alone, data breaches resulted in over one billion records being exposed. When companies get hacked, stolen passwords often end up on the dark web. If you don't update yours, you could be an easy target.

2. Brute-Force Attacks

These attacks use software to guess your password by trying every possible combination. The longer your password stays unchanged, the higher the odds it gets cracked.

3. Phishing

Did you get tricked into entering your password on a fake website? It happens. If you don't change your password after falling for a scam, the hacker could keep using it to access your data.

How Password Rotation Helps

Regular password changes disrupt the plans of even the most persistent hackers. Even if someone gets ahold of your old password, it's useless once you've updated it.

Some industries don't just recommend this—they enforce it. Financial institutions and healthcare providers often mandate password rotations to meet strict cybersecurity compliance standards. This is not to be annoying; it's to keep your private information safe.

Continue reading on page 7

Pictured on the cover: Carlos, Daniel, and Jeremiah

EOS:

A Powerful Framework for Business Growth

Do you feel like you're constantly reacting instead of proactively building? Like you're just lurching from one urgent issue to the next, with no real sense of control? That's the reality for many businesses. Running a business is a balancing act. That's why frameworks like EOS exist. EOS, the Entrepreneurial Operating System, provides a practical framework for managing six key components of any business: Vision, People, Data, Issues, Process, and Traction.

By focusing on these core areas, EOS helps businesses get everyone on the same page and working towards a shared vision. In other words, EOS gives you a structured way to get a handle on the key areas that drive your business's success, ensuring everyone is aligned and working towards the same goals.

The Six Components of EOS

One EOS implementation specialist shared that the businesses she worked with saw an average revenue increase of 30% in 2020. So, how does EOS actually help businesses become more proactive?

It focuses on these six key areas:

1. **Vision:** Define your direction, core values, long-term goals, marketing strategy, and a 3-year vision for success. EOS provides clarity, aligning the team toward a unified goal.
2. **People:** Make sure you have the right people in the right roles, aligned with your values, and a good fit for their responsibilities. Fine-tuning team structure can enhance chemistry and productivity.
3. **Data:** Focus on the key metrics that measure progress and guide decision-making. By tracking these regularly, you can identify trends early and tackle issues before they become problems.
4. **Issues:** Create a system for quickly identifying and addressing issues. Rather than letting challenges fester, EOS helps you face them head-on, making problem-solving more efficient and consistent through structured processes.
5. **Process:** Establish and document core processes to ensure consistency and efficiency in operations. Clear, standardized processes reduce errors and increase accuracy.

Continue reading on page 7

How Your Business Can Outsmart New Phishing Tactics

"Dear Sir or Madam, I have an urgent business proposal for you." Sound familiar? Once laughably easy to spot, phishing scams have transformed into sophisticated attacks that can fool even the most technologically savvy. Today, cybercriminals use advanced tools and cunning strategies to target businesses, putting your organization at risk of financial loss and data breaches.

To protect your business, it's essential to understand how phishing tactics have evolved and implement proactive strategies to stay one step ahead.

Understanding the New Phishing Landscape

MORE PERSONALIZED ATTACKS

Today's phishing scams aren't one size fits all. Cybercriminals now tailor their attacks using publicly available information, such as names, job titles, and even company-specific details. For example, an attacker might impersonate a known vendor or reference a recent business transaction to gain trust.

AI-DRIVEN PHISHING

Artificial intelligence is enabling attackers to craft highly convincing emails that mimic human communication patterns. AI tools can replicate the tone and style of trusted sources, making phishing emails indistinguishable from legitimate ones.

MULTICHANNEL PHISHING EFFORTS

Phishing isn't confined to email anymore. Scammers are now reaching targets through text messages, social media platforms, and phone calls. This multichannel approach increases their chances of catching someone off guard.

BUSINESS EMAIL COMPROMISE

BEC attacks are some of the costliest phishing attacks. In fact, the FBI's Internet Crime Complaint Center (IC3) reported that BEC attacks accounted for nearly $2.9 billion in losses in 2023. By compromising or spoofing executive email accounts, attackers send fraudulent messages to employees, often requesting urgent financial transactions or sensitive data. These attacks bypass many traditional security measures.

Proactive Strategies to Outsmart Phishing Scams

EDUCATE YOUR EMPLOYEES

Training your employees is one of the most effective ways to combat phishing. Regular workshops and simulated phishing exercises, as recommended by America's Cyber Defense Agency, can help staff recognize red flags like unfamiliar links, unexpected requests, or suspicious attachments. Employees who can confidently identify phishing attempts are your first line of defense.

Continue reading on page 6

STOP PAYING FOR IT EMERGENCIES

& Invest in Smarter Solutions Instead

When it comes to managing IT, many businesses take a "fix it when it breaks" approach, thinking it's the most cost-effective option. On the surface – it makes sense. Why pay for support if nothing's wrong? In reality, there are some serious risks behind a reactive mindset. We're talking about emergency repairs, unexpected downtime, and other expenses that quickly pile up.

The good news? By understanding these hidden costs, you can take steps to better manage your IT and position your business for more efficient operations.

1. *The Premium Price of Reactive IT Support*

When businesses opt for "break-fix" IT support, they only address issues as they arise often with the notion that it's more efficient.The reality is the opposite. Emergency maintenance comes at a premium price that quickly exceeds routine maintenance because it requires immediate attention and expedited parts. Further, emergencies that occur outside of normal business hours incur higher labor costs.

On the contrary, routine maintenance comes at a predictable monthly cost ensuring systems are regularly maintained and issues are addressed before they escalate.

2. *Productivity Losses During Downtime*

When systems go down, work grinds to a halt. Employees are left twiddling their thumbs, clients start getting impatient, and the business takes a hit. One study found that the average cost of downtime is $5,600 per minute.

With proactive IT support, your systems are continuously monitored with issues often resolved before downtime occurs.

Continue reading on page 6

How Your Business Can Outsmart New Phishing Tactics continued from pg 4...

ADOPT TWO-FACTOR AUTHENTICATION (2FA)
By requiring a second form of verification, such as a mobile code or biometric scan, businesses can block unauthorized access even if passwords are compromised.

INVEST IN ADVANCED EMAIL SECURITY
Modern email security tools use machine learning to detect and block phishing attempts before they reach employees' inboxes. As highlighted by Forbes, implementing AI-powered filters can analyze patterns, sender behavior, and suspicious links to enhance protection against sophisticated phishing attacks.

VERIFY UNUSUAL REQUESTS
Simple internal protocols can significantly reduce risk. If employees receive requests for financial transactions or sensitive data, require a secondary confirmation method–like a phone call to the requestor–before taking action. These procedures are particularly effective against BEC attacks.

PARTNER WITH IT EXPERTS
A managed IT service provider, like LeadingIT, brings expertise and advanced tools to proactively monitor and secure your business against phishing and other cyber threats. Partnering with a professional IT team ensures you stay ahead of emerging risks. Phishing scams will continue to evolve, but you don't have to be their next victim.

Stop Paying for IT Emergencies continued from pg 5...

3. Unplanned Hardware and Software Costs

A common issue with reactive IT support is the lack of planning for hardware upgrades and software renewals. Businesses often find themselves scrambling to replace failing equipment or renew licenses at the last minute, which can mean paying expedited fees or premium prices. A business that does not plan for hardware upgrades, for example, may face unexpected failures, leading to emergency purchases and increased costs.

Managed IT services include strategic planning to avoid such situations. Providers track hardware lifecycles and software needs, ensuring renewals are planned and budgeted in advance.

4. Cybersecurity Risks and Their Costs

Perhaps the most significant hidden cost of reactive IT is the risk of a cybersecurity breach. Without proactive measures in place, businesses are more vulnerable to attacks like ransomware, which can result in devastating financial losses. According to IBM's 2024 Cost of a Data Breach Report, ransomware branches average $5.37 million (or $4.38 million if law enforcement is involved), making them the most expensive type of attack.

The Case for Proactive IT Management

The hidden costs of reactive IT support – premium repairs, downtime, unplanned expenses, and cybersecurity risks–can quietly erode your bottom line. By switching to a proactive IT model, businesses can save money, improve productivity, and protect against potential threats.

LeadingIT offers all-inclusive IT services that eliminate the unpredictability of reactive IT support. With unlimited support, proactive monitoring, and strategic planning, we're here to help businesses avoid costly surprises and focus on what they do best.

EOS: A Powerful Framework for Business Growth continued from pg 3...

6. Traction: Set clear priorities, hold teams accountable, and regularly assess progress toward goals. EOS provides the framework to stay focused and on track, ensuring consistent movement toward your objectives.

Our Experience with EOS

At LeadingIT, we've experienced the positive impact of EOS firsthand since implementing it in 2024.

Key highlights from our experience include:

- Increased Clarity and Accountability: EOS helped us define roles and responsibilities with clarity, reducing ambiguity and creating a sense of ownership across the team. This eliminated the common issue of tasks slipping through the cracks due to unclear ownership.
- More Effective Problem-Solving: The structured L10 meetings have been pivotal in allowing us to solve problems proactively. By addressing issues early, we've prevented them from escalating and disrupting operations, which has improved efficiency and reduced stress among team members.
- Strategic Planning and Goal Setting: Our annual EOS-facilitated planning meeting was highly effective. It provided an opportunity to objectively review our past year's performance, set ambitious yet achievable goals for the upcoming year, and create a roadmap for success.

Conclusion: Transform Your Business with EOS

Implementing EOS requires commitment, consistent effort, and a willingness to be honest with your team. While the process can be demanding at times, the rewards are substantial. EOS helps build a stronger, more cohesive team, improves operational efficiency, and provides a greater sense of control over your business. If you're looking for a proven system to drive sustainable growth and improve your overall business performance, EOS is definitely worth exploring.

Why Are Password Changes Required? continued from pg 2...

Best Practices for Strong Passwords

Here are a few tips to make sure your password is strong:

- **Make them strong and unique:** Use a mix of uppercase and lowercase letters, numbers, and symbols. Avoid predictable patterns like "1234" or names.
- **Get a Password Manager:** A reputable password manager can help you store and organize your passwords safely, so you don't have to memorize each one.
- **Turn on Multi-Factor Authentication (MFA):** MFA adds an extra layer of security. Even if someone steals your password, they'll need extra verification to access your account.

The Bottom Line: Update Your Passwords

Yes, changing your passwords can feel like a chore. But it's a small price to pay for peace of mind. Regularly updating your passwords reduces the chances of your information being compromised and helps prevent unauthorized access. Staying one step ahead is your best defense. Make password security a priority, and keep your information safe.

LeadingIT Core Values Victor of the Month

Hats off to Jose, our new Service Delivery Manager, for earning this month's Values Victor award for being Accountable!

Jose is the backbone of keeping us accountable, not just to the numbers that drive our company, but to each and every one of our clients. His commitment to transparency and owning up to mistakes sets the gold standard for us all.

Big thanks to Jose for showing us how it's done and ensuring we stay on track and make things right.

LEADINGIT VALUES:

- We Are Driven
- We Chase Excellence
- We Are Humbly Confident
- We Are Accountable
- We Stay Positive

WE ARE CELEBRATING!

Birthdays

Jayson Roesel - February 8th
Vanessa Canete - February 28th

Anniversaries

Jayson Roesel - 2/1/2022
Matthew Perry - 2/1/2022
Maxwell Kulwiec - 2/1/2022
Christopher Hansen - 2/1/2022
Jaclyn Murray - 2/1/2022
Vanessa Canete - 2/28/2022
Giancarlo Jabon - 2/16/2023
Simon Ramirez - 2/12/2024
Mark Peasley - 2/6/2024

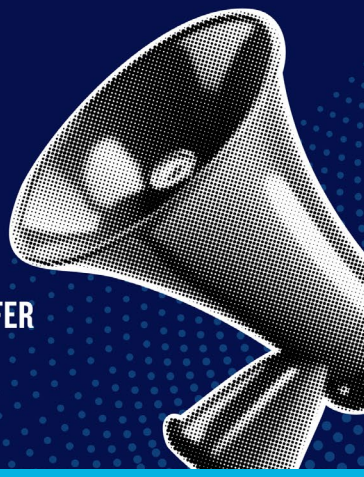
LeadingIT

$1000 REFERRAL PROGRAM

Do you know an organization that needs unlimited IT and cybersecurity support with an unbeatable guarantee?

You'll earn **$50** for every referral.
If they sign up, you'll receive **$1000!**

LEARN MORE



GOLEADINGIT.COM/REFER
815-788-6041

Continue reading on our blog at goleadingit.com/blog

LeadingIT

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