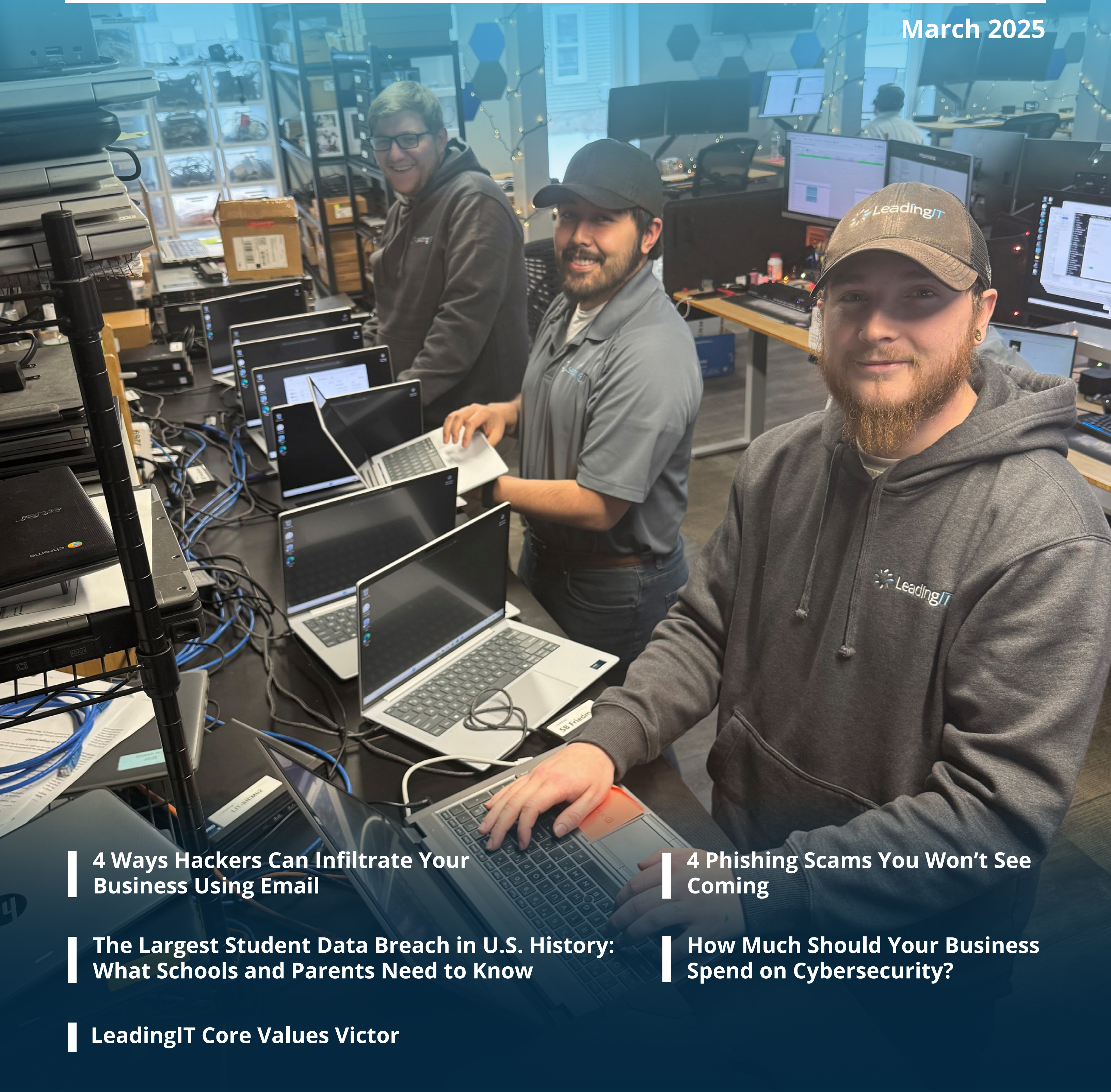
the NetWork

LeadingIT

Chicagoland CybersecurITy Support

March 2025



GoLeadingIT.com ☎ 815-788-6041 in @goleadingit

4 Ways Hackers Can Infiltrate Your Business Using Email

Email, the lifeblood of modern business communication, is also, unfortunately, a prime target for cybercriminals. A successful email breach can cripple a business, exposing sensitive data, disrupting operations, and damaging reputation. Here are four common ways hackers will try to infiltrate your email system.

1. Phishing and Social Engineering: The Art of Deception

Phishing attacks remain one of the most effective methods hackers use to gain access to email accounts. IBM reports that phishing is the most frequent cause of data breaches, with 15% of incidents stemming from these email-based attacks.

Phishing attacks trick individuals into revealing login credentials or downloading malware. Hackers send emails mimicking trusted sources, often creating urgency to prompt quick action. Clicking on malicious links or attachments can install malware and/or redirect to fake login pages that steal credentials.

Beyond phishing, social engineering involves manipulation tactics designed to gain trust.

Common methods include:

- Pretexting: Creating a fake scenario to deceive victims (e.g., posing as IT support to request login details).
- Baiting: Offering something enticing to lure victims (e.g., a USB labeled "Employee Salaries 2024" that installs malware).
- Quid pro quo: Offering a service in exchange for sensitive data (e.g., fake tech support asking for credentials).

Hackers often research their targets extensively, gathering details from social media or other online sources to craft highly convincing attacks.

2. Insufficient Authentication: The Open Door

Strong authentication is the first line of defense against unauthorized email access. Unfortunately, many individuals and organizations still rely on weak passwords and single-factor authentication (SFA). Weak passwords are easily guessed or cracked using readily available tools. SFA, which typically involves just a username and password, is vulnerable to phishing attacks and password breaches.

Multi-factor authentication (MFA) significantly enhances security by requiring multiple forms of verification, such as:

- A password
- A one-time code sent to a phone
- A biometric scan (fingerprint or facial recognition)

Even if a hacker steals a password, they still need additional factors to access the account.

3. Legacy Systems: The Weak Link

Outdated software and systems create significant security risks. Legacy email platforms, which may not receive regular security updates, are prime targets for hackers because they:

- Often lack modern security features
- Are susceptible to known exploits that hackers can easily access
- Have less frequent security patches, leaving doors open for attacks

Organizations that rely on legacy systems should prioritize upgrading to modern, secure email platforms. Regularly patching and updating all

continue reading on page 7...

Pictured on the cover: Matthew, Carlos, Daniel

The Largest Student Data Breach in U.S. History: What Schools and Parents Need to Know

The recent PowerSchool data breach, potentially the largest student data breach in U.S. history, has sent shockwaves through the education community. This incident, stemming from a missed basic security step, highlights the vulnerability of student data and raises critical questions about data protection practices in schools nationwide. Both schools and parents must understand the implications of this breach and take proactive steps to safeguard student information.

PowerSchool, used by over 15,000 school districts across the U.S., manages student records, including grades, attendance, and personal information. While the full extent of the breach is still being assessed, it could impact millions of students, making this a critical issue for schools and parents.

What Data Was Potentially Exposed?

The data breached may include:

- Personally Identifiable Information (PII): Names, addresses, birthdates, student IDs.
- Academic Records: Grades, transcripts, attendance.
- Demographics: Race, ethnicity, socioeconomic status.
- Contact Information: Parent/guardian phone numbers and emails.
- Special Education Records: Details on disabilities and IEPs.

This breach is particularly concerning because this data could be misused for identity theft, targeted marketing, or discrimination, impacting students and their families for years. According to the Identity Theft Resource Center, minors are disproportionately affected by identity theft, with their personal information often targeted due to its "clean slate" status.

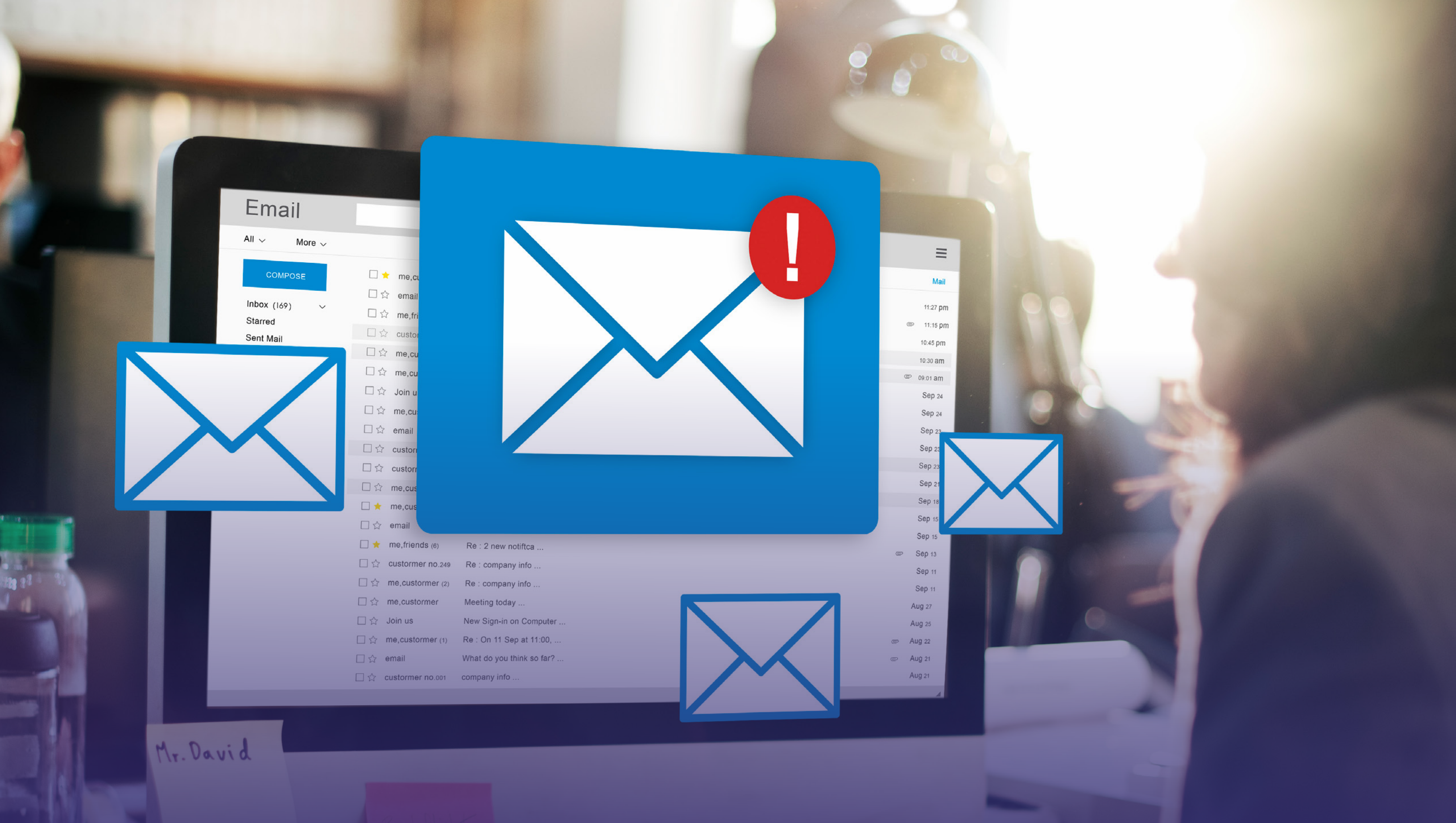
What Schools Need to Do

The PowerSchool breach underscores a critical need for schools to prioritize data security. With school-related cyber attacks surging to a record 121 in 2023—a dramatic increase of 50 attacks compared to 2022—the threat is more serious than ever. Schools must take immediate action.

Here are some essential steps:

- Conduct Thorough Security Audits: Regularly assess existing security measures and identify vulnerabilities.
- Implement Strong Access Controls: Restrict access to sensitive data based on the principle of least privilege. Ensure that only authorized personnel can access specific types of information.
- Enforce Multi-Factor Authentication (MFA): Require MFA for all accounts with access to student data.
- Provide Regular Security Training: Educate staff about cybersecurity best practices, including recognizing phishing scams and practicing strong password hygiene.
- Develop Incident Response Plans: Establish clear procedures for responding to data breaches, including notification protocols and steps for mitigating damage.

continue reading on page 7...



4 Phishing Scams You Won’t See Coming

Phishing attacks have become increasingly sophisticated, posing significant threats to businesses of all sizes. In 2023, a staggering 94% of organizations reported being targeted by phishing scams, up from 92% in 2023.

These advanced tactics are particularly dangerous because they often bypass traditional security measures, making them harder to detect and prevent. As cybercriminals develop more cunning methods, it's crucial for businesses to stay informed about these emerging threats to protect their operations and data.

1

AI-Powered Phishing

Gone are the days of obvious scam emails filled with typos and broken English. Today's AI-powered phishing attacks are sophisticated enough to mimic your CEO's writing style or craft industry-specific messages that look legitimate at first glance. In fact, Harvard Business Review reports that 60% of participants in their study fell victim to AI-generated phishing emails.

Here's what makes them dangerous: AI can analyze your company's public communications, LinkedIn profiles, and social media to create hyper-targeted messages. Imagine receiving an email that perfectly mimics your CFO's writing style, references recent company events, and requests an urgent wire transfer. These attacks are particularly effective during high-stress periods like end-of-quarter financial closings or major company transitions.

2

Password Manager Impersonation

Cybercriminals have found a clever new angle: impersonating the very tools we use to stay secure. Password manager phishing scams exploit our trust in security software by sending convincing notifications about "compromised passwords" or "security alerts" that appear to come from popular password management services.

These attacks typically arrive via email or pop-up notifications, warning about expired licenses or security breaches that require immediate attention. The scammers count on users' quick reactions to security warnings — after all, who wants to risk a security breach? The messages often include urgent calls to action like "Reset Your Master Password Now" or "Verify Your Account to Prevent Lockout," leading to convincing but fake login pages that steal your master credentials.

3

Collaboration Tool Takeovers Are Rising

Business messaging platforms like Microsoft Teams and Slack have become prime targets for attackers. Why? Because employees tend to trust messages from these platforms more than emails. After all, we use them every day to chat with colleagues and share files. Bad actors exploit this trust by sending urgent meeting invites or file-sharing notifications that seem to come from coworkers. Once someone clicks, they might unknowingly hand over their login credentials or download malware, giving attackers access to your entire network.

4

QR Code Phishing Takes Advantage of Trust

Remember when QR codes were just for restaurant menus? Now they're everywhere in business, from payment systems to document sharing. Cybercriminals have noticed this trend and created "quishing" campaigns that exploit our comfort with scanning codes.

They send legitimate-looking emails with QR codes that supposedly link to invoices, shipping updates, or important company documents. Scan the code, and you're taken to a convincing but fake login page designed to steal your credentials.

Protecting Your Business From Advanced Phishing

Defending against these sophisticated attacks is about having the right partner, not just the technology. You need advanced email filtering, sure, but you also need a team that understands these evolving threats and can train your employees to recognize them.

How Much Should Your Business Spend on Cybersecurity?

Cyber threats are a big deal for businesses of all sizes. The average cost of a data breach has reached $4.88 million in 2024, marking a 10% increase from the previous year.

This rise shows how important it is for companies to invest in cybersecurity. But how much should your business spend to stay safe?

Let’s dive in.

Why Cybersecurity Spending Matters

Cyber threats continue to evolve, putting businesses of all sizes at risk. In 2023, 43% of cyberattacks targeted small businesses, according to Verizon's Data Breach Investigations Report. Additionally, the cost of ransomware attacks has skyrocketed, with global damages expected to reach $30 billion by 2024. Small businesses are especially vulnerable—only 14% are prepared to defend themselves against a cyberattack, as reported by Accenture. These figures demonstrate that cybersecurity shouldn’t be treated as an IT issue, but as a business-critical priority.

How Much Do Businesses Typically Spend on Cybersecurity?

Determining the right cybersecurity budget depends on factors like company size and industry. On average, businesses spend 13.2% of IT budgets on cybersecurity. Larger organizations or those in regulated industries, like healthcare or finance, may allocate 15-20% of their IT budgets to security, as they hold much more sensitive information — and thus have more to lose.

Comparatively, a lack of investment can be far more costly, as according to IBM’s report, businesses on average will save over $2 million by investing in robust cybersecurity measures.

Factors That Influence Cybersecurity Costs

Not every business needs the same level of cybersecurity investment. Your costs will largely depend on your unique situation. For example, if you're in healthcare, you'll need to meet HIPAA requirements, while government contractors must achieve CMMC compliance.

Each of these regulations comes with its own set of security demands (and associated costs).

The type of data you handle matters too. If you're storing sensitive financial records or personal information, you'll need more robust protection than a company dealing mostly with public data. Company size plays a big role — more employees mean more potential entry points for cyber threats.

And here's something many businesses overlook: location matters. Companies in the Chicagoland area often face different threats than those in rural regions, and your security budget should reflect these regional risks.

Warning Signs and Smart Solutions

Is your cybersecurity investment falling short? Watch for these warning signs: outdated systems that haven't seen updates in months, no dedicated IT security team, or a "fix it when it breaks" approach to security. If you're struggling to pass security audits or meet industry regulations, that's another clear signal it's time for a change.

4 Ways Hackers Can Infiltrate Your Business Using Email

continued from page 2...

software, including operating systems, email clients, and server software, is essential for mitigating security risks.

4. Human Negligence: The Inside Job

Even the best security technology can't prevent breaches caused by human error. Human error accounts for 74% of data breaches, according to a 2023 InfoSec report.

Employees may:

- Fall for phishing scams
- Use weak or reused passwords
- Share login credentials
- Leave devices unlocked
- Use unsecured networks

Comprehensive security awareness training is crucial for educating employees about the latest threats and best practices for protecting email accounts. Training should cover topics such as identifying phishing emails, recognizing social engineering tactics, practicing strong password hygiene, and following security protocols. Regularly reinforcing these messages through ongoing training and reminders can help create a culture of security awareness within the organization.

Cyber Resilience is Multi-Layered

In conclusion, protecting email systems requires a multi-layered approach that addresses both technical and human vulnerabilities. By understanding the common tactics hackers use, organizations and individuals can take proactive steps to strengthen their defenses and prevent email breaches. Implementing strong authentication, keeping systems up-to-date, and fostering a culture of security awareness is essential for safeguarding email communications and protecting sensitive information.

The Largest Student Data Breach in U.S. History: What Schools and Parents Need to Know

continued from page 3...

- Review Vendor Security Practices: Ensure that third-party vendors, like PowerSchool, have robust security measures in place.
- Communicate Transparently: Keep parents and students informed about data breaches and the steps being taken to protect their information.

What Parents Need to Do

Parents also have a role to play in protecting their children's data. Here are some actions parents can take:

- Stay Informed: Pay attention to communications from your child's school about data breaches.
- Monitor Your Child's Online Activity: Be aware of what information your child is sharing online.
- Teach Your Child About Online Safety: Educate your child about the risks of sharing personal information online and how to identify phishing scams.
- Review School Privacy Policies: Familiarize yourself with your school's data protection policies and procedures.
- Advocate for Stronger Security: Urge your school district to prioritize data security and implement robust protection measures.
- Freeze Your Child’s Credit: Consider placing a credit freeze on your child's credit report to prevent identity thieves from opening accounts in their name.

Conclusion: Be Proactive

The PowerSchool breach is a stark reminder of the importance of data security in education. Schools and parents must work together to protect student information and ensure that technology is used responsibly and securely. By taking proactive steps, we can mitigate the risks of future data breaches and safeguard the privacy and well-being of our students.

LeadingIT Core Values Victor of the Month

Kyle Funk, Senior L1 Bench Technician, is this month's Values Victor for staying positive!

During our busiest times, Kyle has been a powerhouse of hard work and relentless optimism. He always keeps a positive outlook and focuses on solutions, turning the most challenging days into opportunities for growth and success.

Big thanks to Kyle for showing us the power of a positive mindset, especially when the pressure is on.

LEADINGIT VALUES:

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

WE ARE CELEBRATING!

Birthdays

Matthew Perry - March 12th

Anniversaries

Christa Gibbons - 3/11/20

Jose Ledesma - 3/1/21

Dustin Looper - 3/21/23

Kelly Kontaxis - 3/18/24

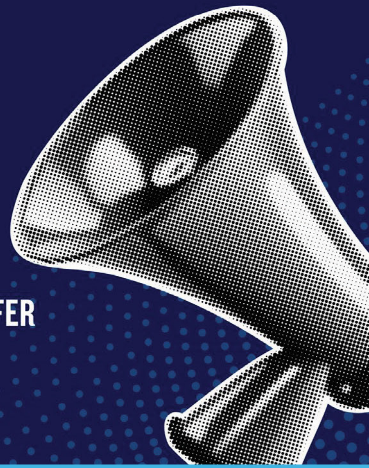
LeadingIT

$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