



# The Network

## IN THIS EDITION:



CAN SOMEONE HACK YOUR EMAIL WITHOUT THE PASSWORD? WHAT CHICAGO BUSINESSES NEED TO KNOW



WHAT ARE THE DUTIES OF A VCIO? STRATEGIC IT LEADERSHIP WITHOUT THE FULL-TIME COST ON TECHNOLOGY PROFESSIONALS DO?



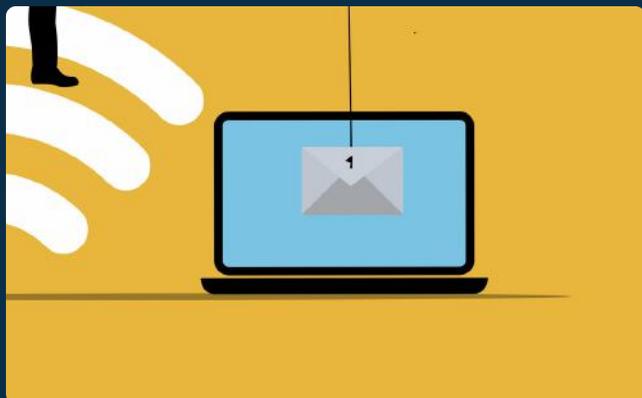
IS THERE GROWTH IN TECHNICAL SUPPORT? STRONG GROWTH AHEAD FOR CHICAGOLAND BUSINESSES

# Can Someone Hack Your Email Without the Password? What Chicago Businesses Need to Know

Yes, hackers can compromise your email account without ever knowing your password. In fact, most modern email attacks don't rely on brute-force password guessing at all. Instead, attackers exploit phishing, social engineering, and account recovery features to gain access.

According to [Verizon's 2025 Data Breach Investigations Report](#), 68% of breaches involved a human element, including phishing, stolen credentials, or social engineering.

For Chicagoland businesses, email security is no longer just an IT issue, it's a business risk.



## How Hackers Access Email Without a Password

The most common method is phishing. Attackers send emails that appear legitimate like password resets, shared documents, or urgent requests, leading victims to fake login pages that steal credentials. Even advanced users fall for these attacks, especially as phishing emails become more convincing with AI-generated content.

Another major risk is password reset manipulation. Hackers intercept reset links, exploit weak security questions using publicly available information, or trick users into approving access. In many cases, attackers bypass two-factor authentication using techniques like session hijacking or SIM swapping.

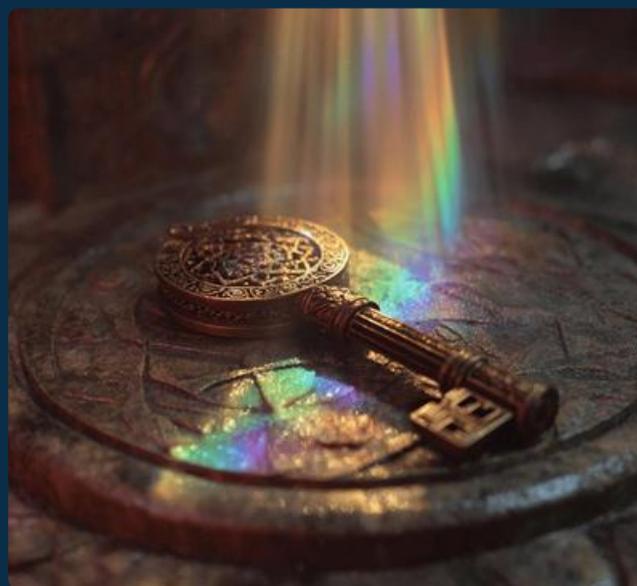
*Once email access is gained, attackers rarely stop there.*

## Why Email Is the "Master Key"

Your email account controls access to nearly every connected service, from banking, to payroll, cloud platforms, social media, and even vendor accounts. If attackers compromise your email, they can:

- Reset passwords across financial and business accounts
- Intercept security alerts and bank notifications
- Set up forwarding rules to monitor communications silently
- Launch phishing attacks from your account to clients and coworkers

[Business Email Compromise \(BEC\) attacks](#) caused \$2.77 billion in losses in 2024 alone, according to the FBI's Internet Crime Complaint Center, often by impersonating executives and authorizing fraudulent payments.





## Warning Signs Your Email May Be Compromised

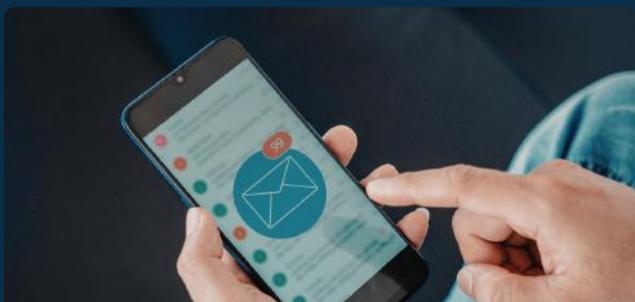
Common red flags include login alerts from unfamiliar locations, emails in your sent folder you didn't send, unexpected password reset notifications, or changes to account settings like forwarding rules. These signs often appear only after attackers already have access.

## How Chicago Businesses Can Reduce Risk

Strong email security requires layers, not just passwords. Best practices include:

- Enabling multi-factor authentication using authenticator apps or hardware keys
- Using unique passwords for every account with a password manager
- Training employees to recognize phishing and suspicious emails
- Monitoring login activity and email rules regularly
- Implementing email protections like spam filtering and anti-spoofing controls

Separating personal and business email use and limiting what accounts rely on a single inbox can also reduce exposure.



# Protecting Your Digital Identity

Email hacking doesn't require stolen passwords, only one mistake or weak control. Understanding how attackers operate is the first step toward prevention.

For Chicagoland businesses, proactive email security protects more than inboxes, it protects revenue, reputation, and customer trust.

At LeadingIT, we help organizations secure their email environments with layered defenses, employee training, and proactive monitoring to stop threats before they become breaches. [Reach out to our Chicago IT security team](#) to strengthen your email security and protect what matters most.



# What Are the Duties of a vCIO? Strategic IT Leadership Without the Full-Time Cost

For many Chicago-area organizations, technology decisions are happening, but not always strategically. Someone is approving purchases, reacting to outages, and dealing with security concerns, yet no one truly owns IT direction. That's where a virtual Chief Information Officer (vCIO) comes in.

A vCIO provides CIO-level leadership on a fractional basis, giving small and midsize organizations access to strategic IT guidance without the cost of a full-time executive. For businesses, nonprofits, schools, law firms, manufacturers, and professional services firms with **25-200 employees**, a vCIO fills a critical leadership gap.

## What Is a vCIO?

A vCIO is an outsourced technology executive, typically delivered through a managed IT provider. Unlike help desk technicians or MSP engineers, a vCIO is not focused on day-to-day troubleshooting. Their role is strategic: aligning technology with business goals, planning future investments, managing risk, and communicating clearly with leadership.

Think of the vCIO as your organization's IT quarterback. They coordinate people, platforms, budgets, and priorities so technology supports growth instead of creating constant surprises.



## Core Duties of a vCIO

### Aligning IT with business goals

The vCIO starts by understanding your organization's plans over the next 1-3 years. Whether you're expanding locations, supporting remote work, preparing for audits, or modernizing operations, the vCIO ensures technology decisions directly support those objectives.



### Creating and managing a technology roadmap

A vCIO builds a clear 12-36 month roadmap outlining hardware refreshes, security improvements, cloud initiatives, and major projects. This eliminates surprise failures and turns IT into a predictable, planned investment.



### Budgeting and financial planning

One of the most valuable vCIO duties is transforming IT from emergency spending into structured budgeting. The vCIO builds annual and multi-year IT budgets, tracks spending, justifies costs in business terms, and identifies waste. Many organizations reduce IT costs by 20-40% through better vendor and license management alone.



### **Cybersecurity, risk, and compliance oversight**

The vCIO owns cybersecurity strategy, not just tools. This includes defining security standards, overseeing backups and disaster recovery, conducting risk assessments, and guiding compliance with regulations like HIPAA, PCI, or FTC Safeguards. When incidents occur, the vCIO leads response and communication at the executive level.

### **Policy and standards governance**

From acceptable use policies to remote work and password standards, the vCIO ensures policies exist, are updated, and are followed. Standardization reduces risk and improves support efficiency.



### **How a vCIO Works with Your IT and MSP**

Strategy only matters if it's executed. A vCIO works alongside your internal IT staff and managed service provider to ensure alignment and accountability.

They review performance metrics like response times, system uptime, and backup success. They help prioritize projects so resources go to what matters most, not whoever complains the loudest. In co-managed environments, the vCIO clarifies roles and ensures everyone follows the same playbook.

### **Communication: Turning IT Into Business Language**

A critical vCIO duty is communication with non-technical leaders. Instead of jargon, the vCIO explains risks in terms of revenue, productivity, and liability. Regular quarterly reviews, IT scorecards, and strategy meetings keep leadership informed and confident in technology decisions.

### **When Does an Organization Need a vCIO?**

Common signs include repeated surprise IT costs, frequent downtime, inconsistent security practices, unclear compliance readiness, or leadership feeling "in the dark" about IT. These issues usually signal a planning gap, not a technology failure.



## **Strategic IT Leadership That Scales**

A vCIO delivers the same strategic responsibilities as a full-time CIO, but at a fraction of the cost, and with cross-industry insight gained from working with multiple organizations.

# Is There Growth in Technical Support? Strong Growth Ahead for Chicagoland Businesses

Is there growth in technical support? Absolutely. Technical support and IT services continue to expand across market revenue, employment demand, and business investment, especially for small and mid-sized companies.

According to **Grand View Research**, the global IT services market reached \$1.50 trillion in 2024 and is projected to grow to \$2.59 trillion by 2030, representing a 9.4% compound annual growth rate. This momentum is fueled by rising cybersecurity risks, cloud adoption, and increased reliance on technology across every industry. For Chicagoland businesses, reliable technical support is no longer optional, it's essential for competitiveness.

## What's Driving Technical Support Growth?

While some entry-level support roles may see modest declines, the overall IT workforce remains strong. The Bureau of Labor Statistics projects over 317,000 annual job openings in computer and IT occupations through 2034, driven by growth, turnover, and the need to replace retiring workers.



## Several factors are accelerating demand:

- **Cybersecurity threats:** Businesses increasingly rely on security monitoring, incident response, and compliance support.
- **Cloud computing:** Managing cloud platforms, hybrid environments, and remote work infrastructure requires specialized expertise.
- **Technology complexity:** Artificial intelligence, automation, and advanced software systems create new support and management needs.
- **Skills shortages:** Companies struggle to hire in-house professionals with both technical expertise and strong problem-solving skills.
- **Business continuity:** Proactive IT support helps prevent downtime, data loss, and operational disruptions.

As systems grow more complex, businesses are shifting away from reactive, break-fix models toward managed IT services that deliver predictable costs and broader expertise.



## SMBs Are Leading IT Investment

Small and medium-sized businesses are driving much of this growth. According to the [GTIA SMB Technology and Buying Trends 2025 report](#), nearly two-thirds of SMBs plan to spend between \$25,000 and \$1 million on technology this year, with 9 out of 10 increasing their IT budgets.

Additionally, **61% of SMBs** outsource IT services either regularly or occasionally. Outsourcing provides:

- Access to experienced specialists across networking, security, and cloud systems
- 24/7 monitoring and support without expanding internal headcount
- Predictable monthly costs instead of unpredictable hiring and replacement expenses
- Compliance and security guidance aligned with industry standards

For organizations with 25 to 250 employees, **managed IT services** deliver enterprise-level capabilities without enterprise-level overhead.

## What This Means for Chicagoland Businesses

Market expansion benefits local companies by increasing access to advanced tools and experienced providers. Modern technical support now includes AI-driven monitoring, automated patching, proactive threat detection, and data management, far beyond traditional help desk services.

Today's technical support specialists combine hardware and software knowledge with strong communication and problem-solving skills. This evolution reflects a broader industry shift toward proactive IT management that supports growth, security, and resilience.

## Position Your Business for Growth

The growth of technical support services reflects a fundamental change in how businesses manage technology. IT is no longer just a cost, it's a competitive advantage.



# \$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!**

**815-788-6041**    **GOLEADINGIT.COM/REFER**



**SCAN TO  
LEARN MORE**

## WHAT'S NEW AT LEADINGIT We're excited to share a few team updates as LeadingIT continues to grow and invest in our people.



**Promotion News!** Alex has been promoted to Level 1 Senior Technician! This promotion is a direct reflection of the accountability Alex brings every day and the drive we love to see at LeadingIT. Congratulations, we're excited to see you step into this next level.

### Introducing The LeadingIT Reek Values Award

At one of our leadership offsites, our EOS Implementor said something that stuck with us: *"Your people should reek of your core values."* And honestly... yes. That is the bar.

So we created a new annual recognition: The LIT Reek Values Award. We honor a team member who doesn't just talk about our values but lives them so consistently in how they show up for clients and teammates.

Our first-ever winner is **James Clayton**, our **Level 3 Lead Technician!** James consistently shows up accountable, driven, and humbly confident, while pushing excellence and keeping a positive mindset even when things get tough. He's the guy people look to when it's complex, urgent, or "unsolvable." James doesn't just represent our values, he absolutely reeks of them. Congratulations!

