the NetWork LeadingIT

Chicagoland CybersecurITy Support

June 2022

Cheap is Expensive: Cutting Corners in Cyber Security Will Backfire

A Guide to 'Zero Trust' Approach to Managing Cyber Risk

'Smishing' (SMS Phishing): A Rising Threat for Business Owners

Fast Growth, Fast Fun!

GoLeadingIT.com (815) 496-6300 @leadingit-solutions

CHEAP IS EXPENSIVE:

Cutting Corners in Cyber Security Will Backfire


Dale

Businesses are continually looking for ways to increase profits and minimize expenditures. Therefore, it's a no-brainer that we see a lot of cutting corners in cybersecurity. From not spending enough on data security to 'one-man hiring band' IT service providers and overlooking standard cybersecurity practices like staff training, it's not enough to say that businesses now sacrifice data security for profits. And reasonably so—without profits, they can't survive. What good is profitability without a functioning business?

4 Reasons You Shouldn't Leave Your IT to a 'One-man Band'

The IT guy is not a full-time employee, so they're not entitled to allowances or bonuses. Instead, you only call them on necessity, such as during a glitch or deployment of a new environment. This approach may seem like the perfect solution until you consider its downsides:

1. **A 'One-Man-Band' IT Provider May Not Have Enough Budget**
   One of the main reasons businesses outsource IT support is the cost factor—outsourcing shifts all the acquisition and maintenance expenditures to the service provider. For example, at LeadingIT, we spend hundreds of thousands of dollars annually to acquire the necessary tools, deploy layers, and maintain the best experts in the industry to ensure that we're doing things correctly.
   We can afford this because we have several customers, enabling us to benefit from the economy of scale. Unfortunately one-man-band IT providers can barely afford the state-of-the-art equipment necessary for delivering high-quality IT support.
2. **Cybersecurity Is a Vast and Dynamic Field**
   IT support is a vast field—from database design to network monitoring, endpoint protection, incident response, digital forensics, and penetration testing—nobody can master it all. That's why established IT companies like us hire experts with specialties in specific branches of IT support. Our helpdesk technicians focus on that and nothing else, giving them enough time to understand their area of focus and deliver the best service. And that's what differentiates us from solo IT providers.
3. **A One-man-Band IT Provider May Not Have Enough Time:** You never know when the bad guys will strike. Therefore, it's crucial to monitor your systems round-the-clock, continually update your intrusion detection and prevention protocols and occasionally audit your network for threats. These tasks are time-sensitive; they require experts dedicated to your systems fully. A 'one-man band' IT service provider may not have enough time to give all their clients this kind of support.
4. **IT Guys Are Often Reactive**
   Prevention is always better than cure, and it's not any different for cybersecurity. IBM estimates that the average cost of a data breach is $3.86 million, way higher than what it'd cost your organization to deploy preventive measures. Unfortunately, most one-man-band service providers typically wait to react after glitches.

Decisions Regarding Cybersecurity Must Weigh the Benefits Against Risk

Cybersecurity is not a luxury; it's do-or-die for your Chicagoland organization in the information age. Accenture estimates that security breaches have been up by 67% over the last decade and the SEC saying that over 60% of SMBs shut down within six months after surviving data breaches, we think it's cheaper to invest in cybersecurity than prioritizing profits and risking losing your entire business. Profits won't matter if ransomware hits your organization.

Pictured on the cover: Laura

A Guide to '**Zero Trust**' Approach to Managing Cyber Risk

Zero trust is one of the most popular buzzwords in today's cybersecurity industry. What is it? How does it work? What are its benefits? Why is everybody talking about it? How do you implement it? According to IBM, data breach costs have jumped to over $3.86 million per incident. All statistics point to one thing—hacks and breaches are increasing in volume and becoming more severe by the day.

What's Zero Trust Policy?

The earliest evidence of the term "zero trust" is in a 1994 paper on securing IT systems by an associate professor at the University of Ontario Institute of Technology called Stephen Marsh. However, the term only got famous after NIST's 2018 "Zero Trust Architecture" special publication. The publication described zero trust as a "term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources." It "assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned)."

Nathan

Zero Trust Is Both a Methodology and a Mindset

While zero trust loosely translates to "no trust," the term doesn't literally mean that. Instead, it means zero implicit trust where organizations do not automatically trust any user or anything, within or without its perimeter, based solely on ownership and network or physical location. Instead, the business develops policies to regulate when and how users or devices can access corporate resources.

Zero trust is not a technology tool you can install once and move on, but a philosophy. It often requires a culture shift and can significantly enhance your organization's cybersecurity posture.

The Most Crucial Line of Defense Against Cybercrime is Your Employees

Cybint estimates that 95% of data breaches arise from human error. You might be thinking—but am I not supposed to trust my team implicitly? Yes, you can, but you should also exercise caution. A zero trust security architecture won't authorize any user, whether the CEO or an entry-level intern if they don't meet the access prerequisites. It creates a level playing field and prevents cyber actors from using trusted devices or stolen logins to access your files. And more importantly, it instills a culture of security and empowers every employee to be more cyber-conscious.

How Can Organizations Turn Zero Trust Into Reality?

Introducing a zero-trust philosophy may require a substantial cultural shift, but it's doable. Below are some tips you can use to streamline the process:

- **Define what you're protecting**
- **Educate users in every step**
- **Make a flexible plan**
- **Don't go it alone**

'**Smishing' (SMS Phishing):** A Rising Threat for Business Owners

Proofpoint's 2022 State of the Phish report, 74% of businesses faced smishing attacks last year, up from 61% in 2020.

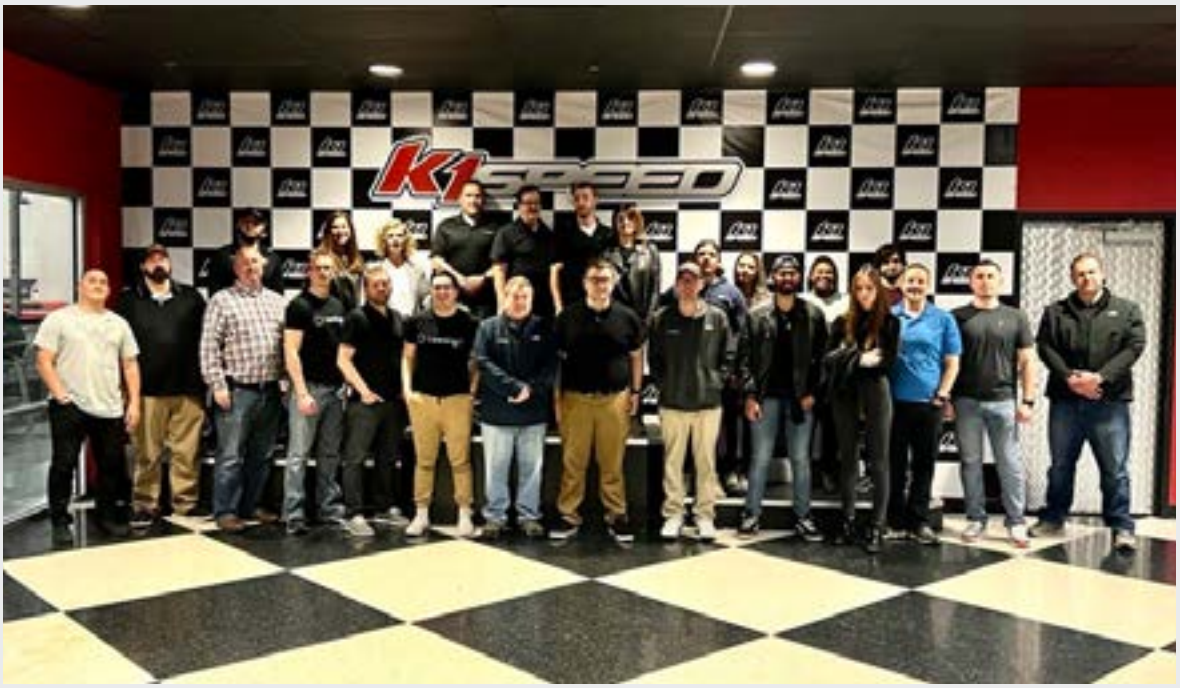
Smishing is SMS phishing. It's a variant of phishing where cyber actors send fraudulent texts to trick recipients into revealing their sensitive information or clicking malicious links. This type of social engineering often exploits human trust rather than technological faults. Like regular phishing actors, smishing artists always impersonate reputable individuals or companies, like your bank asking you for card details or your IT provider directing you to update passwords. As you key in this information or follow the instructions, the bad guys monitor your every move silently in the background.

Continue reading on back page

Fast Growth, Fast Fun!

We recently had the opportunity to bring our teams together for an evening of racing fun at K1 Speed. LeadingIT has seen exciting growth in the past 2 years as seen in our ever-expanding team photo!

Peter and Katelyn



WE ARE CELEBRATING

Birthdays

Scott Sola - June 4th
James Clayton - June 12th
Jeremiah Bird - June 15th

Anniversaries

Collin Saunders - 6/29/2021
Mallory Hale - 6/29/2021

'Smishing' continued...

The bad guys can use either of the following two methods or both:

1. Smishing through malware: Cyber actors can trick you into clicking malicious links or opening malware-infested attachments. When you click the links, malicious software automatically installs itself on your mobile phone, masquerades as a legitimate app, and tricks you into sharing personal information.

2. Smishing through malicious websites: It's similar to smishing through malware, only that the clicking of malicious attachments here redirects you to a fake website that mimics reputable ones. The site may automatically mine your data or ask you to type sensitive information as an attacker eavesdrops in the background.

Adopt Zero-Trust Approach To Manage Cyber Risk

As you must have noticed, smishing primarily relies on human error. Zero trust involves not implicitly trusting any user or device due to ownership and physical or network location. Instead, it defines the exact prerequisites users must meet to access your networks. For instance, you can use MFA as an extra authentication layer for all your sensitive databases. That way, the bad guys cannot compromise your networks even if they steal a trusted user's login.

LeadingIT

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

Check out our blog at goleadingit.com/blog