the NetWork

LeadingIT

Chicagoland CybersecurITy Support

January 2023

Cybersecurity Solutions You'll Need in 2023

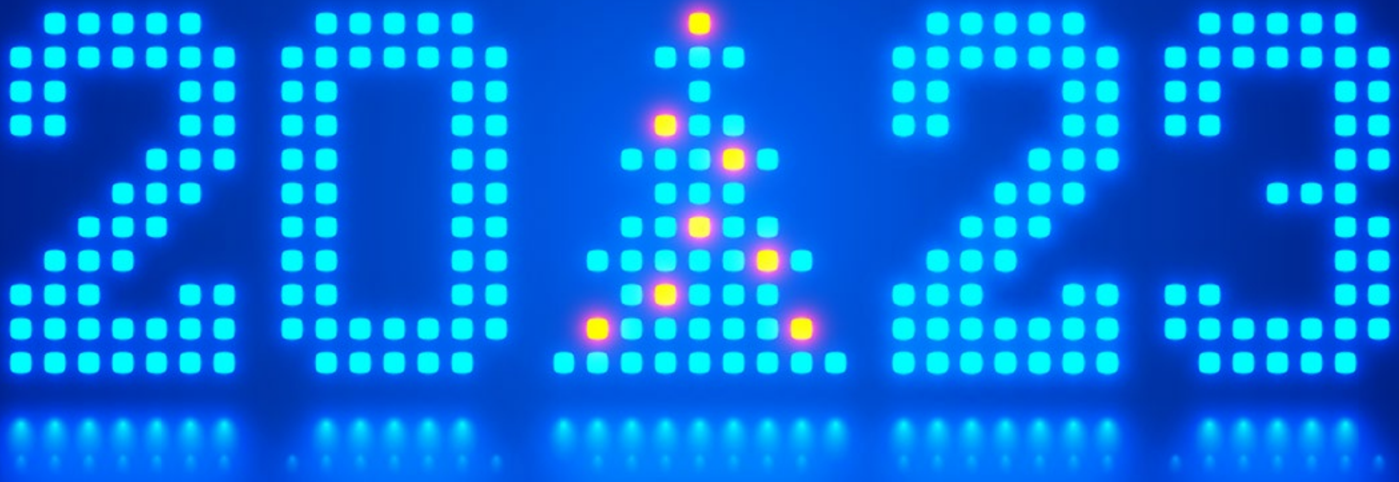
Granting Administrative Rights to Users Can Have Serious Repercussions

Is The Era Of Cyber Un-Insurability Upon Us?

New LeadingIT Services!

GoLeadingIT.com ☎ 815-893-2525 in @goleadingit

Cybersecurity Solutions You'll Need in



Cyberattacks across all industries increased by 28% in the third quarter of 2022, with the healthcare and education sectors being the groups targeted the most. What should we expect to come in 2023? New regulations? More attacks? As the internet continues to evolve, we will likely see changes coming that differ from your typical phishing or ransomware attack.

So what should you watch out for in 2023?

Increased Demand for Employee Education

Virtually every business in today's digital world operates online. As cyber threats become an increasing problem for companies of every shape and size, it's going to be imperative that employees are properly trained in how to spot threats.

After all, internal vulnerabilities (e.g. unsuspecting or careless employees) are one of the biggest contributors to data breaches. In fact, a 2019 report concluded that "your weakest link is your own employees" after finding them to be responsible for up to 50% of company data breaches.

Many cybersecurity companies already offer solutions tailored toward educating employees. Proper cyber education should help staff members navigate modern technology, spot threats, and show them what to avoid (e.g. questionable links).

IoT Introduces Vulnerabilities

The Internet of Things is responsible for bringing some incredible things to life. Smart watches, smart doorbells, wireless cameras, and even AI assistants like Amazon Alexa. Unfortunately, devices like these are becoming targets to get entry into secure networks.

Hackers love targeting these devices because companies often don't take the necessary steps to secure them. While your computer may have a firewall, anti-virus, and other software to protect it, these smart devices can be left without much security at all. Not only can a hacker access the smart device and its data, but it could also potentially be used to gain entry into your network and other devices.

New Governmental Regulations

In 2023, we can expect to see new government regulations to help combat the newest cyber threats. This will likely come in the form of new laws, additional cyber defense personnel to offer cybersecurity solutions, and security mandates by design.

In 2023, cybersecurity solutions will be more critical than ever. Attacks from hackers will happen more often and come from new directions. On top of that, expect new government regulations. Partnering with a small business IT support company is your best choice to stay safe.

Pictured on the cover, left to right: Matt, Scott, Jeremiah

Granting Administrative Rights to Users Can Have Serious Repercussions

Granting someone administrative rights to your company's computer system is certainly convenient. It helps speed up company workflows, but it can also reveal sensitive information within your database. As the number of administrative users increases, so does the risk of viruses, malware, and other vulnerabilities. In fact, employees don't have to act maliciously to expose a system, as most vulnerabilities are exposed accidentally.

What is Administrative Access?

Administrative (admin) access gives users the right to make significant alterations to a computer system. This includes adding or removing applications, changing passwords, changing network settings, or switching ownership status on files.

Restrict User Access to Avoid These Common Threats

You can't control everything users open or click on, which makes it incredibly difficult to control dangerous actions. If a user's account is compromised, hackers could gain access to their computer, email, data, and more. The issue can get even worse if that user has admin access and is able to access more intricate settings and data. This could introduce a whole slew of issues including:

- Phishing using actual employee email accounts
- Unintentionally passing information off to scammers and hackers
- Installing malicious software
- Locking other users out of a system

Continue reading on page 4

Is The Era Of Cyber Un-Insurability Upon Us?

When it comes to insurance, cyber coverage is one of the most sought-after categories currently available. But with cyber risks on the rise, and insurers struggling with their exposure to claims, there is concern over the rising costs of premiums and whether insurers will be able to continue selling this niche at all. So what does that mean for businesses?

Many small businesses may go without insurance because of rising premiums and stricter underwriting standards. Since small businesses already have a harder time protecting themselves from cyber threats due to limited resources, this is a particularly dangerous scenario.

In the wake of the uncertainty surrounding cyber insurance, businesses need to start taking proactive approaches to cybersecurity. While it is impossible to prevent breaches completely, companies can take measures to implement cyber risk management practices. These include things like:

- Developing a strong incident response plan
- Implementing ransomware protection and prevention
- Keeping software up to date
- Making sure employees are educated on how to recognize threats
- Staying educated on cybersecurity best practices

You can significantly aid your company's continued safety from cyber attacks by working with a cybersecurity partner who can evaluate your current state of security and recommend and implement appropriate safeguards.

New LeadingIT Services!

Our accountable concierge cyber + IT support means nothing is unsolvable. We are adding the following to better serve you:

- Business Telephone Systems
- Access Control Systems
- Voicemail Systems
- CCTV Camera Systems
- Sound Systems
- Telephone Bill Consulting

Let us help you select the right technology for your organization. Contact us today!

Scott

Scott, Nathan, Kyle

Administrative Rights continued...

Security Over Convenience

While many organizations opt to give employees admin access for more convenient workflows, this practice is very risky. The risks are far and wide and can be anything from changing passwords to downloading malicious files. Keep your company safe by granting administrative access as infrequently as possible.

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.

WE ARE CELEBRATING

Birthdays

Devin Lindelof - January 6th
Dave Gregory - January 7th

Anniversaries

Stephen Taylor - 1/1/2010
James Clayton - 1/25/2021