2023

Issue 9 Volume 13

frogworks

Managing Your Technology So Your Business Doesn't Croak.

Ribb"IT" Review

LinkedIn User Accounts Have Been Hijacked

As cybercriminals continue to take advantage of people who use social media, many LinkedIn accounts are at the center of a hijacking scheme. This targeted attack is very dangerous for professionals and business owners who use the platform. Hackers can take over your account and send damaging messages to your connections, among other malicious activities.

Learn more about this issue and how you can protect your LinkedIn account.

Why Hackers Are Turning to LinkedIn

Data shows how many compromised LinkedIn accounts exist. In fact, according to Google Trends, searches like "LinkedIn account hacked" and "LinkedIn account recovery" grew more than 5000% in 2023. But why are hackers targeting this social media site for their attacks?

LinkedIn is all about making business connections, which hackers can quickly ruin if they get access to your account. They can send hurtful messages to your many connections in an attempt to hurt your image or spread harmful content to your network. The accounts of well-known business owners and their workers need to be kept safe.

Has Your LinkedIn Account Been Hacked? Here's What To Do

If you can't access your LinkedIn account or hear from others that your account has been hacked, you can report the issue to LinkedIn. The site's Help page allows you to submit your concerns and work with an employee to resolve them. Some users end up paying hackers ransom to regain control of their accounts. Rather than endure a financial loss, there are better ways that you can safeguard your LinkedIn account. The best way to navigate this issue is to take steps that protect your account. This way, it's harder for hackers to retrieve your login information and access your account.

(See page 2)

This monthly publication provided courtesy of:
Alex Bleam,
Owner of Frogworks

Get More Free Tips, Tools, and Services At Our Web Site: www.GetFrogworks.com
Or call: (240) 880-1944

User Accounts Have Been Hijacked (cont)

Has Your LinkedIn Account Been Hacked? Here's What To Do

If you can't access your LinkedIn account or hear from others that your account has been hacked, you can report the issue to LinkedIn. The site's Help page allows you to submit your concerns and work with an employee to resolve them.

Some users end up paying hackers ransom to regain control of their accounts. Rather than endure a financial loss, there are better ways that you can safeguard your LinkedIn account.

The best way to navigate this issue is to take steps that protect your account. This way, it's harder for hackers to retrieve your login information and access your account.

How To Protect LinkedIn Accounts

One of the best things you can do to protect your LinkedIn account is to enable two-factor authentication. In other words, you'll have to input your email address, password to log in, and one other credential. Ways to verify an account through two-factor authentication include:

- Giving a correct answer to a security question
- Entering a one-time passcode
- Entering an account PIN

Even if hackers have your email address and password, your account will be more secure when you require another form of verification to log in. Experts also recommend setting a unique password that will be difficult for someone to retrieve. If you receive any reports of attempted logins, change your password immediately to enhance your security. Don't become one of the many LinkedIn accounts that hackers take over.

How To Stay Ahead of Cyber Attacks With Managed IT Services

With hackers and cyber threats on the rise, it's all your business can do to stay safe in today's digital climate. Managed IT services are integral for protecting businesses from cyber-attacks. Learn more about what these third-party cloud services do and how they can keep your business safe from outside threats. (see page 3)

How To Stay Ahead of Cyber Attacks With Managed IT Services (cont)

What Are Managed IT Services?

A managed IT service is a third-party resource that oversees your company's information technology. While managed IT experts are readily available to address any issues with your network, their main goal is to avoid destructive threats.

Outsourcing these concerns to an IT service provider ensures your business is in the best position against cyber-attacks. It also means you can save money by reducing the need for in-house IT staff. Your business

Application Service Providers (ASPs)

An ASP is responsible for delivering application software across a business network. This provider will oversee your specific applications, which is extremely helpful for your developers and vendors.

Managed Service Providers (MSPs)

An MSP can help small and medium-sized companies maintain a secure network. The managed IT services model's main point is handling your daily IT operations. This option is great if your company wants to reduce your time devoted to fixing service interruptions or network issues.

How Managed IT Services Prevent Cyber Threats

ASPs and MSPs are excellent resources for different business models. However, the main benefit of these services is their protection against cyber-attacks. Your IT service provider will offer expert support and take action in the following areas.

Advanced Network Security Measures

Any outsourced IT service will do everything possible to protect your network from threats. This includes activating firewalls and antivirus software. The ultimate goal is to keep hackers from infiltrating and compromising your network.

Your IT service provider will also keep your security software up to date to avoid dangerous hacks. You'll have peace of mind that your business can run smoothly if your network is secure.

Data Backup and Recovery

Heightened security measures aren't always enough. If a hacker obtains any sensitive data, you want to be able to access it during an unexpected breach. Managed IT services perform routine data backups so you can easily recover from a potential breach.

Research shows that the average cost of a data breach is over $3.9 million. With a managed IT service backing up your data, you can minimize financial loss and maintain customer trust.

Threat Management

Managed IT services actively monitor potential cyber threats to your computer network. This will give you another layer of protection since an in-house IT team may not be as watchful. Any signs of a threat, such as a suspicious phishing email, will be flagged.

Understanding Microsoft Phishing Attacks: How to Protect Yourself

Microsoft is now the go-to disguise for cybercriminals launching phishing attacks. But a closer look can save you and your business from falling prey. It's all about slowing down, observing, and analyzing.

The Rising Phishing Tide

The latest data from Check Point's Threat Intelligence rings the alarm bells. Microsoft has shot up to the top spot for brand phishing attempts in the second quarter of 2023. It accounts for 29% of these attempts, up from third place in the earlier quarter. Microsoft now outpaces Google and Apple.

Over half of the brand imitation attacks came from these three tech companies.

Windows and Microsoft 365 customers around the globe are the targets of a new surge of fake emails. The phishing hooks dangle tempting baits. They imitate Microsoft's look, hoping you'll bite. One recent phishing scam spotted by Check Point analysts involved a false Microsoft account sign-in alert. It lured users into clicking a harmful link. These links are designed to grab anything they can. From login details to payment information, nothing is off-limits.

How to Spot and Avoid Phishing Attacks

Phishing tricks come in many forms. Emails, texts, and social media messages all serve as lures. They look real and urgent, playing on your fears. Once you click on a link, a fake login portal appears. It might look compelling. If you enter your details, it gives them the chance to steal your sensitive data.

Here's how you can protect yourself:

Look for Errors: Spotting errors in the URL, domain, and message can help. If anything seems off, it could be a phishing attempt.

Slow Down: Don't let a sense of urgency force you into hasty actions. Take your time to assess unexpected alerts or requests.

Analyze: Make sure to examine any message carefully before taking action. Legitimate entities typically avoid asking for sensitive information via email or text.

Standing Guard Against Phishing

Phishing isn't a new problem, but it keeps evolving. And as the Microsoft phishing attack shows, it's growing more sophisticated. But you're not helpless. Spotting discrepancies and being mindful of the signs can go a long way in keeping critical information about your business, customers, and partners safe. Slowing down, observing, and analyzing is the key to outsmarting phishing attempts. It's your best defense in the face of this persistent online threat.

We Have an E-Newsletter!!!

Do we have your e-mail address??? If you would like to receive our newsletter though email please visit us at:

www.getfrogworks.com/newsletter

Channel Futures
Leading Channel Partners Forward

NEXTGEN 101

MSP TO WATCH • 2021 WINNER