Data-Link Associates, Inc.

October 2022

DataGrams

ONE YEAR LEFT…

October 10, 2023 marks the End Of Support for Server 2012 Operating Systems.

Aging systems can make your company a target for cybercrime.

WHAT'S INSIDE?

The MFA Fatigue Attack: What Every CEO Should Know

Microsoft, Cisco and now Uber have been victims of a social engineering technique called The MFA Fatigue Attack used by hackers to gain access to devices protected by multi-factor authentication (MFA).

Best cybersecurity "defense in depth" practices say to enable MFA on as many sites and portals as possible for an extra layer of security. This practice has been adopted by most of the business world over the past year and you likely have this implemented in most areas of your company.

When an attacker is blocked by the MFA and is asked to provide the MFA credentials, they cannot hack their way through that—they need the legitimate code to proceed.

Hackers are parents and spouses too and in this social scheme they harness the power of "nagging". They know that nagging works and will attempt to use it to their advantage.

Imagine receiving hundreds of requests for MFA to your phone. You press DENY and then an identical prompt pops up a few seconds later. This continues for hours and you give in at some point of exhaustion—or accidentally hit Approve.

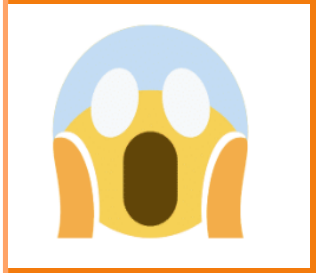
The hacker is in. Game over.

Because MFA is newer to mainstream business, staff may think the relentless requests are a glitch or an authorized administrator is attempting to access their device to perform maintenance.

If this happens to you, please call us right away for help. **This is an active, brute force attempt to take over your device.**

P.S. If you use MFA Authenticator apps to generate a passcode (instead of a push notification) there will never be a case when a legitimate authorized administrator will ask for your MFA passcode. Password protect your phone and give MFA creds/codes to NO ONE.

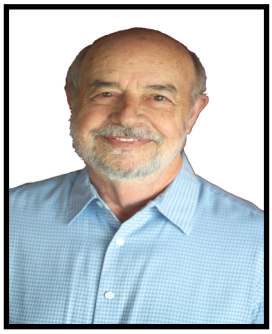
Does The Thought Of Your In-House Computer Expert Leaving Scare You To Death?



Here's a scary question a lot of businesses don't think about: what would happen if your computer guy suddenly quit?

Drop me a line to discuss your network and business goals to decide on some IT coverage options to fit your business "just in case". It can be a plan to take over your IT entirely, or just for the short-term. Seamless transition is key. Your IT expert might need to go but we're not going anywhere.

-Pam (Client Relations) pbirchfield@datalinkmsp.com (630) 406-8969 ext 574



This monthly publication provided courtesy of Richard Frielink, Founder & President of Data-Link.

Our Mission

To provide IT solutions and services that allow our clients to succeed in an ever changing and challenging business

EMERGENCY

(630) 406-8969

24/7

Coming up in the next issue:

- Network Endpoint Best Practices
- Toss That Stack of Business Cards?
- Are You A Wiz at WORDLE? What your solve rate says about your intelligence
- Is Masterclass worth the $180/year?

Cyberattack Increase Warning Issued for Schools

Back-to-school time is in full swing and imagine if the only threat that schools faced would be running out of tissues during sniffle season? Unfortunately, that isn't the case. A cyberattack warning from the FBI, CISA , and MS-ISAC has been issued indicating that cybersecurity attacks may increase as the 2022/2023 school year begins and criminal ransomware groups perceive opportunities for successful attacks. A recent attack on the Los Angeles school district deployed malware over Labor Day weekend. The attack was followed up with government-issued announcements that included the warning of an increased threat.

Why Cyberattack Schools?

Limited funding goes beyond having enough school supplies. There are constraints on the cybersecurity resources and staffing capabilities as well. This makes a cyber attack much easier if there aren't people and policies in place to respond quickly. Additionally, the acquisition of sensitive data, like that of school-aged children, is lucrative to hackers. They may gain access not only to the students but to parent information as well.

A year ago, NBC News collected and analyzed school files from dark web pages and found they are littered with personal information of children. Although they don't have bank passwords or credit scores yet, parts of the internet are awash in the personal information of millions of school children. They found that in 2021, ransomware gangs published data from more than 1,200 American K-12 schools. And even after schools are able to resume operations following an attack, parents have little recourse if their children's information is leaked. Some of the data is personal, like medical conditions, social security numbers and birthdays, all permanent indicators that can set them up for a lifetime of potential identity theft.

Scammers can act quickly after information is posted. In February, just a few months after Toledo Public Schools in Ohio was hit by ransomware hackers who published students' names and social security numbers online, a parent told Toledo's WTVG-TV that someone who had that information had attempted to take out a credit card and a car loan in his elementary school son's name.

It's (almost) Technology Business Review Season!

Pam will be contacting all clients to schedule.

Topics: Industry breaches 2022, Security in 2023, Phishing email training, Cyber insurance requirements, Business expansion and Disaster Recovery Plans.

sales@datalinkmsp.com
(630) 406-8969 ext 574

HACK ALERT!

If you do business with either of the following companies, take measures to protect your personal information… they've been HACKED!

Uber: A revisit from a recent Weekly IT Security Tip I sent out, a teenager hacked Uber after they obtained the corporate password of an Uber contractor. They gained access to at least the company's internal Slack messages, a finance tool for invoices and the dashboard where the company's researchers report bugs and vulnerabilities. In the lawsuits that will invariably result, we will learn more about what happened. **This is a great time to change the password to your Uber apps.**

INC.com: Their website is shut down with a message "As a result of the Fast-Company.com breach, Mansueto Ventures (which also owns Inc.) is temporarily shutting down Inc.com out of an abundance of caution while the investigation is underway."

After the hack, Apple News was promptly shut down after the hacker pushed obscene notifications to users' home screens on Tuesday, September 20th.

MICROSOFT TEAMS PHISHING ATTACKS

New Microsoft Defender for Office 365 capabilities build on improvements announced in July 2021, allowing Microsoft Teams to automatically block phishing attempts.

Hackers have started to drop malicious executable files into chat conversations on Microsoft Teams. Once executed (post -click) the malware writes data into the system registry on the machine. The file will eventually take over the user's computer.

How do they get in your Teams? Some possibilities includes stealing credentials for email or Microsoft 365 via phishing or compromising a partner organization.

A roll-out to allow end-users with desktops to report suspicious messages from inside the Teams app is expected in January 2023.

Since 2004, the President of the United States and Congress have declared October to be Cybersecurity Awareness Month, helping individuals protect themselves online as threats to technology and confidential data become more commonplace. The Cybersecurity and Infrastructure Security Agency (CISA) and the National Cybersecurity Alliance (NCA) lead a collaborative effort between government and industry to raise cybersecurity awareness nationally and internationally.

See Yourself In Cyber

This year's campaign theme—"*See Yourself In Cyber"* demonstrates that while cybersecurity may seem like a complex subject, ultimately, it's really all about people. This October will focus on the "people" part of cybersecurity, providing information and resources to help educate CISA partners and the public, and ensure all individuals and organizations make smart decisions whether on the job, at home or at school—now and in the future.

7 Things You Can Do

Throughout October, take this time to put extra effort toward your company's cybersecurity.

1. Enable Multi-Factor Authentication
2. Use Strong Passwords
3. Recognize and Report Phishing
4. Update Your Software
5. Sign up for continuous cyber training for your entire staff, including the c-suite.
6. Don't share passwords internally.
7. Remember, if your gut tells you it's off, don't talk yourself out of it. Pick up the phone and call someone who can verify a non-routine request.

Your Role

When we say *See Yourself In Cyber*, we mean see yourself in cyber no matter what role you play. As an individual or consumer, take basic steps to protect your online information and privacy. Vendors and suppliers can take ownership of their role, while protecting their brand and reputation, by putting strong cybersecurity in place at work to help prevent an incident at your location or further down the supply chain. Critical infrastructure owners and operators, you are part of a larger network of functions and systems that rely on or support critical infrastructure.

In the month of October,
Data-Link is giving away a
FREE Fake Phishing Email Campaign
sent to your ENTIRE COMPANY!

From this test we can tell you:

- Who opened the email?
- Who CLICKED a link inside the email (danger!!)
- Who deleted without opening

Without a test like this, you will only know if someone in your company clicked on a phishing email after it's too late.

Scan to start ———>

sales@datalinkmsp.com
(630) 406-8969 ext 574

Thank You For Calling!

Thank you to those who called in a referral this month, sent topic requests for the Weekly IT Tip emails, requested more information or sat for an appointment. We appreciate you!

Combat Cybersecurity Fatigue

Cybersecurity fatigue refers to a decreasing awareness or interest in cybersecurity and a correlating increase in risky behavior. It frequently occurs when people feel overloaded by too much information. One of the most common examples of this fatigue is people using the same password across multiple sites or portals.

How to combat cyber-fatigue and keep your staff aware

- Education creates a broader sense of individual responsibility and frequent training will allow best cybersecurity practices to become second-nature.
- Run drills like phishing tests and incident response drills.
- Recruit a 'white hat' hacker to attempt to break in to your system so staff can see exactly how weak security can lead to easy access.
- Try not to answer emails from unfamiliar senders after lunch. This is the danger zone of poor judgement. If you're in a food coma just trying to function and get through the rest of the day, it's easy to let your guard slip.
  It only takes ONE mis-click.

Sign Up For Our
Weekly IT Security Tips
to receive timely, relevant cybersecurity tips and news every Tuesday morning.

We promise to NEVER spam.

How Culture Assessments Can Level Up Your Security Program

People are the new perimeter and prime target for hackers. 82% of data breaches involve a human element.

A culture assessment (like Culture Index) measures what a person believes and their innate tendencies. Culture assessments are becoming a standard pre-hire practice.

The assessments generally show basic tendencies like autonomy, social ability, pace/patience, conformity and attention to detail. Companies use these tests to understand and build their desired culture and place new hires in roles they will thrive.

As it relates to cybersecurity, the following scores are ideal.
High in Autonomy (work on their own)
High Attention to Detail
Moderate Pace/High Patience

By knowing your staff's natural tendencies, you can tailor training and give network access accordingly to best protect your network.

Global Mega Trends for Technology To Year 2030

By the year 2030, technology will be everywhere. The IoT (Internet of Things) will continue to grow. We've seen Amazon Alexa, smart watches and the Amazon Go Store et al emerge since 2010 and the landscape will continue to get wider—affecting convenience in daily routines and the greater good of humanity.

- Smartphone storage will continue to grow to TERABYTE storage chips that can process massive amounts of data and power 5G and artificial intelligence (AI).
- AI will continue to emerge. Robotics are already being commissioned locally to bridge the employment gap. Industrial, aerospace, smart home infrastructure and automotive industries will become fully automated and intelligent.
- Peer-to-peer services (like Uber) are expected to transform and penetrate several non-traditional applications.
- Augmented and virtual reality technology will evolve toward a total reality-virtuality continuum.
- Seamless integration of video, voice and data services will provide access and ubiquitous connectivity anytime and anywhere by 2030.
- Intelligent assistants will optimize and personalize daily experiences across all activities and environments.

What will these changes mean for the future of YOUR industry? Your company?

Craft An Effective Shock & Awe

A Shock & Awe package is sent to a qualified prospect prior to a scheduled sales call where you may be up against several other companies and/or the incumbent to create POSITIVE ANTICIPATION of meeting with you. A good Shock & Awe will overcome doubts and objections and position you for the sale.

What to include (any/all):
(*include at minimum)

- Cover letter confirming the appointment*
- Instruction sheet for the materials inside
- Overview of relevant services the prospect is interested in.
- Relevant client testimonials/ case studies*
- FAQs
- Copies of your newsletter
- Copies or list of awards you've won
- Articles or books you've written
- Your Guarantee of product/service*
- Things you do better than your competition. (USP)*
- Logo items (pen, mug, etc..)
- Business card*
- A free report or ebook
- The other guys v.s. you comparison chart

Send your Shock & Awe in time to land on your prospect's desk a couple days before your meeting so they have time to review the materials before your meeting.

sales@datalinkmsp.com
(630) 406-8969 ext 574