Data-Link Associates, Inc.

June 2022

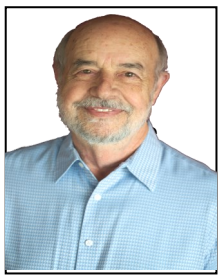
DataGrams

What's New

HAPPY ANNIVERSARY!
Mike Lamczyk: 29 years

WHAT'S INSIDE:

June 2022



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 environment.

Why Gen Z Could Pose A Threat To Your Company's Security How To Prepare

As we progress through 2022, more and more Gen Zers will be entering the workforce. When millennials entered the workforce, we saw different attitudes and behaviors than ever before, and we should expect Gen Zers to come with their own uniqueness and differences. You may think that since they are the first full generation to grow up in the digital age they will be well-prepared for any technological challenges and security issues that arise, but that isn't always the case.

Since most Gen Zers grew up with a smartphone and social media, they're more likely to share information without any regard for security. According to Entrepreneur, many Gen Zers struggle to distinguish between friends they met online and in real life. Cybercriminals could use this knowledge to carefully craft social media profiles to gain access to valuable information about the individual and possibly even their workplace.

There are many common issues that plague Gen Zers when it comes to cyber security. Password issues seem to be the most prevalent. According to a recent Harris Poll, 78% of Gen Zers use the same password across multiple accounts. That's up 10% to 20% when compared to millennials, Gen Xers and baby boomers. Other common issues include safe browsing habits and tracking basics.

Continued on pg.2

Continued from pg.1

Over the next few years, there's a good chance that you will hire a Gen Zer for some role in your business. You're probably wondering how you can prepare your cyber security so it's ready to handle whatever the next generation brings. It's important that you're proactive in your strategy. Waiting until you already have Gen Zers in your workplace could leave your information unprotected or make your company open to cyber-attacks.

Before anything else, you need to develop an information security training program. It's imperative that your company have a well-established cyber-secure culture that everyone has bought into. That way, when you have new hires, you can put them through the same training while your other employees demonstrate proper techniques through behavior. Make sure your training is up-to-date and that you continue to update it whenever new software or technology is released.

Remember when I said that many Gen Zers struggle with password security and often use the same password for every account? If they continue to do that and use the same password for their personal and professional accounts, it could leave your business vulnerable. Start implementing password manager programs in your business as soon as possible to avoid this dilemma with any current or future employees. Password managers generate complicated and secure passwords that your average hacker can't crack.

> **"78% of Gen Zers use the same password across multiple accounts."**

If you truly want to keep your business protected from cybercriminals, you can hire a managed services provider to take care of your IT needs. But please be aware, not all MSPs are alike. Good MSPs are all about being proactive. You'll get around-the-clock monitoring, data encryption and backup, network and firewall protection, security awareness training and so much more. Basically, all of your cyber security concerns will be covered when you hire an experienced MSP, and you won't even have to worry about the next generation making things more difficult.

As Gen Zers enter the workforce, it's important that business owners across the country prepare for their arrival. Don't wait for them to start at your business to make changes to your cyber security plan. Be proactive and do what you need to ensure that your business is fully prepared.

Free Report: What Every Small-Business Owner Must Know About Protecting And Preserving Their Company's Critical Data And Computer Systems

This report will outline in plain, nontechnical English the common mistakes that many small-business owners make with their computer networks that cost them thousands in lost sales, productivity and computer repair bills, and will provide an easy, proven way to reduce or completely eliminate the financial expense and frustration caused by these oversights.

Download your FREE copy today at
www.datalinkmsp.com/protect

"YOUR AD HERE!" Client Spotlight

This space is now reserved for a monthly Client Spotlight!

You are invited to draft a profile/ advertisement for your company and we'll feature you in this space!

Our DataGrams newsletter reaches 200+ CEOs and C-Suite executives of manufacturers and medical practices every month who trust Data-Link Associates to manage their cybersecurity, managed services and business continuity.

Do you have a product or a service you would like this group to know about?

The profile/advertisement should include a brief history of your company, standard information about your company/product/ service, contact information and a blurb about your experience with Data-Link as your IT provider.

Data-Link reserves the right to edit for grammar, content-type and space. Any recommended changes will be discussed with the client prior to final edits and printing.

Email entries to Pam at pbirchfield@datalinkmsp.com

Entries should be 200 words maximum.

There is no deadline for entries, this offer is ongoing.

I can't wait to see who responds!

Best Disaster Procedures/Docs

A disaster to your business can be anything from acts of god to a cyber attack or deleted files from a disgruntled employee, utility outage or even absenteeism of an essential employee.

To ensure business continuity, every business needs a plan to ensure mission-critical processes continue even in the event of a disaster.

Here are the best disaster procedures and documents to start implementing today (not after a disaster happens) to guarantee your business is able to quickly recover after a disaster.

BEFORE A DISASTER

1. Conduct a Business Impact Analysis to identify time-sensitive or critical business functions and processes and the resources to support them.

2. Organize a Business Continuity Team to spear-head creation of the Business Continuity Plan, its subsequent edits and to manage a business disruption as it plays out.

3. Create the Binder. The Business Continuity Plan is a physical, documented procedure placed in binders and given to the principals of the company to make sure the plan can be executed from anywhere at any time.

4. Conduct training and testing exercises to familiarize staff on the procedures.

DURING A DISASTER

1. Locate the binder. Start from page 1 and put the plan in motion. The binder should be very clear so that a juinior employee can implement the plan if needed. You never know who will be on-site at the time of a disaster. Just make sure you train him, too!

AFTER A DISASTER

1. You should be breathing a sigh of relief. If you prepared and had a business continuity plan, the aftermath should be business as usual.

Best Documents To Create For Your Business Continuity Plan

1. Recover Personnel—Build from the C-Suite down. Contact info
2. Recovery Prodecure—Vendors/ Utilities to Contact
3. Data Backup—Call your IT company for access to your backed up data to resume ops.

Can't wait until next month's newsletter for more cyber news?

Find us on: facebook®

Follow Data-Link Associates
for valuable and timely IT blog posts

3 Big Technology Trends For Businesses In 2022

Many of the changes brought forth by the pandemic are here to stay and may even evolve further. The year 2022 is shaping up to be a big one for technology, and you'll want to stay informed if you plan to keep up with any changes in your business.

With more people working remotely than ever before, there's been a greater focus on Internet speeds and usage. Over the next year, we'll experience an increase in 5G coverage as well as rapid development for 6G. Additionally, we're likely to see some growth in the AI sector. It's also imperative that you pay attention to the Metaverse and any impending developments, as the Metaverse has the potential to majorly impact a lot of industries.

Avoid These E-mail Marketing Tactics

E-mail marketing campaigns are performed by almost every company because they're a cost-effective way to reach a large number of potential customers. However, have you ever felt like your campaign was not getting the attention it deserves? Is it possible you did something that actually turned people away from your campaign? You'll want to reconsider your approach if you're doing any of the following:

- Using clickbait subject lines
- Using your e-mails only as a platform to sell
- Sending too many e-mails too often
- Failing to personalize any of your e-mails
- Focusing on company-related content instead of making it relatable

Make sure you are getting approvals to email from everyone and offering opt-outs.

Get The Most Out Of Your Products

When you first start a business or develop a product, you're probably trying to figure out a way to maximize its value. Sometimes it's not enough to simply create a great product or service. You need to inject it with the spirit of your company. When you first started your business, you should have written out some core values you never want to forget. Your products should also follow these values and, at times, be the greatest representation of them. Oftentimes, you can showcase this through the design of the product itself and its packaging. When someone first uses your product or service, it should look flawless and work perfectly. When a potential customer first sees your product and uses it, they should have no qualms about the quality or design. They should view your product the same way you ideally view it – like it's the best thing since sliced bread.

"'Unexpected error.' It stopped being 'unexpected' after the first ten times