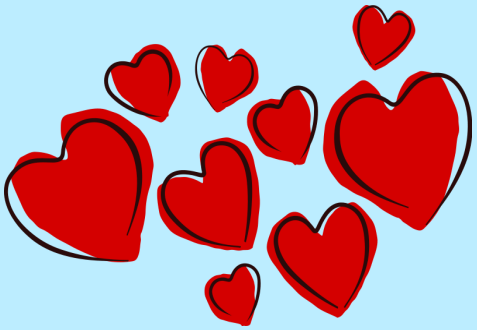
Data-Link Associates, Inc.

February 2022

DataGrams

What's New

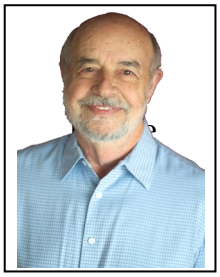


LOVE
IS IN THE AIR AT
DATA-LINK!

See what's going on at:

DATALINKMSP.COM
/FEELTHELOVE

February 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.

Cyber Security Is More Important Now Than Ever – Is Your Business Prepared?

Over the past few years, instances of cyber threats have increased at an alarming rate, and they don't seem to be slowing down anytime soon. Awareness around cyber security has certainly improved over the past year, with 9 in 10 Americans stating that they are somewhat concerned about hacking that involves their personal information, financial institutions, government agencies or certain utilities. But while awareness has increased, so have the rates of cyber-attacks.

Last year, people had more data breaches from January to October 2021 than in all of 2020. As we continue through 2022, there's no reason to assume this year will be any different. In order to ensure that your business is protected this year and every year after, you should take the proper precautions regarding cyber security. If your business falls prey to a cyber-attack, you risk tarnishing your brand's reputation and will have customers questioning whether it's safe to do business with you.

Below are a couple of the best cyber security practices you can put in place to fully prepare for cyber-attacks and threats.

HIRE A MANAGED SERVICES PROVIDER (like Data-Link)
Small and mid-size businesses have seen an increase in cyber-attacks since 2018, but larger corporations are no exception for hackers. The NBA, Kia Motors and the Colonial Pipeline are just a few examples of big businesses that fell victim to cyber-attacks last year. No matter the size of your business, hiring an

Continued on pg.2

Continued from pg.1

MSP is the most affordable and best way to protect your business.

MSP services are designed to identify and resolve the weak points in your IT infrastructure. MSPs are focused on being proactive and will also focus on IT support and advanced security. You'll get monitoring, data encryption and backup, network and firewall protection, security awareness training and so much more. With MSPs, you get a team of dedicated IT professionals who are available to assist with any tech dilemmas that may arise. It's the quickest and most cost-efficient way to fully protect your business.

TRAIN YOUR EMPLOYEES
Visit: datalinkmsp.com/FEELTHELOVE

If your employees have not been trained to be cyber-secure, they need to be trained on this subject immediately. Security should also be built into the devices they use to access company data. This becomes even more important if your employees are working remotely. Multifactor identification and ensuring that your employees create complex and non-repetitive passwords is the critical first step to keep your business

protected. *For more info on MFA and selecting the best Password Manager for your business and personal devices, continue on page 3.*

Educate your employees about the most common forms of cyber-attacks. They should be aware of phishing e-mails and texts and should be taught to never open any links if they don't know who the sender is. Hackers have also started to frequent social media, and they often target small businesses through various platforms. Make sure your employees aren't clicking on any social media spam links that could put your network at risk. Lastly, make sure they aren't accidentally downloading any malware that could create disastrous outcomes for your company.

A cyber-attack can have cataclysmic effects on a small business, and every business owner needs to make sure their network is protected. If you don't know

"Multifactor identification and ensuring that your employees create complex and non-repetitive passwords is the critical first step to keep your business protected."

'I DIDN'T KNOW'

Unfortunately, That Excuse Doesn't Replenish Your Bank Account, Resolve A Data Breach Or Erase Any Fines And Lawsuits.

It's coming ...

- That day a hacker steals critical data, rendering your office useless
- That day when your bank account or credit card is compromised
- Or that day when your customers' private lives are uprooted

Cybercriminals and hackers are constantly inventing NEW ways to infiltrate your company, steal your assets and disrupt your life. The ONLY way to STOP THEM is this:

You Must Constantly Educate Yourself On How To Protect What's Yours!

Now, for a limited time, we have the perfect way to help reduce your risk and keep you safe! Simply sign up to receive our FREE "IT Security Tip of the Week." We'll send these byte-sized quick-read tips to your e-mail inbox. Every tip is packed with a unique and up-to-date real-world solution that keeps you one step ahead of the bad guys. And because so few people know about these security secrets, every week you'll learn something new!

Get your **FREE** "IT Security Tip of the Week"
https://www.datalinkmsp.com/category/blog

Use MFAs and Password Managers to Protect Your Account Information

MFAs (Multifactor Authentication/ Authenticators) need two or three layers of identification to prove who you say you are to gain access to an account. The MFA will verify at least two of the following:

√ You have knowledge
(i.e. your password or PIN)

√ You have possession
(i.e. your cell phone with an MFA/2FA app or email)

√ You are inherently YOU!
(i.e thumbprint or facial recognition)

This authentication process can be prompted to perform either 1) when signing on from a new device or 2) your device can ask you every time you log in. It will depend on the type of account and the security settings applied.

Examples of MFA are Microsoft Authenticator, Google Authenticator, Duo Security, Last Pass and OneLogin.

Password Managers are a secure place to store your passwords for all of your accounts. You no longer have to remember your passwords!

I will pretend none of our readers *ever* writes down their password so I can sleep tonight.

Our staff at Data-Link can help you choose a Password Manager that is best for your needs, business or personal. Drop me a line at pbirchfield@datalinkmsp.com

Insurance For Your Business' Future

As a local business owner, I'm sure you wish you could buy insurance that would secure the future of your business.

Hire a Managed Service Provider (MSP)– THEY are your "insurance policy".

Currently, How do you ensure the website is up? How do you make sure the phones are working? Payments can always be accepted? Do you have software and hardware to grow and evolve as the market grows? How do you know if your data is secure and can be recalled if a tornado takes out the office or if staff needs to suddenly work from home because another reason caused the world to shut down.? How would you handle a hacker? You should have a clear answer for each one of these questions if you want your business to survive now and evolve in the future.

Think of the MSP as the best insurance policy- who happens to be an employee, who's not on your payroll, can't sue you, won't file a Worker's Comp claim and won't *ever* show up late. They don't get sick or go on vacation. And if at any time you feel like they're not adding value, and you can take the risk of not having the services they offer, they'll leave and you don't need to worry about an unemployment claim.

Only, they're not just another one of your team members– sure, they can give you advice but what they can do more than anything else is they can help protect you from going out of business. Ultimately, for the local business owner, it's everything they have.

Claim your FREE NETWORK SCAN at datalinkmsp.com/feelthelove to start your MSP relationship with Data-Link . We have client relationships that have lasted 30+ years and look forward to starting that journey with you.

If you let us, we'll help you make more money by ensuring your systems are up and running all hours of the day. We're the best IT employee you could hire with 128 years of experience combined.

If you already have an IT person (or team) we offer Co-Managed IT services.

*** Note: If you don't already have it, get Cyber Insurance. Call and introduce yourself to our guy Justin Smitherman (630) 934-4910. He's happy to answer questions and talk policy rates on Cyber Insurance. Tell him "Pam sent ya!" ***

Break Through The Digital Dilemma And Take Your Business To The Next Level

In the digital age, companies are growing faster than ever before, and the companies that are succeeding all have one thing in common: a growth mindset.

Companies that aren't looking to grow get stale quickly, and this becomes more apparent with each technological advancement. In order for your business to succeed, you will need to develop a growth mindset within your company. There are a few things you can do to adapt and create a mindset that will catapult you to the top of your industry.

The first thing is to continue promoting a learning and mentoring ideology within your business. There's always room for growth; you just need to encourage it. You should also encourage innovation by establishing areas where external and internal sources can communicate. Also, stay informed and ahead of your industry by paying attention to new technology. Lastly, don't be afraid of feedback. It can help your company grow and help you to discover any shortcomings.

Facebook Recently Launched Its Metaverse, And it's A Privacy Nightmare!

Facebook is in the process of unveiling hardware and other technology to support its metaverse, even calling this new network "Meta." The social media platform has seen a recent decrease in users who cite mistrust as a key factor in their departure. A Facebook whistleblower, Frances Haugen, has stated that the virtual reality world could give Facebook another opportunity to steal even more personal information from its users. Haugen said users will be required to set up many sensors throughout their home, which will encourage them to detract from reality and enter the virtual world. The idea of adding sensors into users' homes is a privacy nightmare. It gets even worse if you consider the fact that employers who use Meta may require their employees to have the sensors in their homes so they can participate in meetings. Trust in Facebook is already low, and Meta will have to ensure their system is safe if they hope for success.

It's Been Coined The 'Great Resignation,' But Why Are Employees Walking Out In Droves?

Everywhere you look, it seems like more businesses are putting out "Help Wanted" signs. Limeade, an organization that specializes in employee well-being, recently released the results of a study that focused on why people were leaving their jobs. Burnout was the top reason most employees quit. Through surveys and conversations with your team, you can discover if burnout is an issue in your business. Introducing mental health days and finding ways to equally distribute workloads can help prevent burnout.

People who recently left their jobs also stated that they wanted a more flexible or caring culture. Employees need time for themselves and will become unhappy if they feel work is taking away from that time.