Data-Link Associates, Inc.

September 2022

DataGrams

WHAT'S INSIDE?

If You See A Message Like This CALL US IMMEDIATELY

If you receive a message like the one above on your computer or other device, ***FREEZE! DON'T DO ANYTHING...*** *and call us at (630) 406-8969.*

This is not a typical phishing scam, it's mainly a phone scam.

DO NOT CALL THE NUMBER GIVEN

DO NOT CLICK ON BUTTONS/LINKS

DO NOT ATTEMPT TO CLOSE

The phone number connects to a scammer who will attempt to access your computer—and surely you will give them whatever info they want because they are trying to help you, right? ...

3 out of 5 consumers have encountered a tech support scam just like this in the past 12 months.

Legitimate hardware/software companies, including Microsoft/Apple, HP, Dell etc... WILL NEVER call, text, email or put a message on your screen telling you about a problem with your device. (But WE do, so call us if you're suspicious.)

How does it happen in the first place? You clicked on something you oughtn't. We have training for this. Call anytime.

DID YOU KNOW?

If you get a virus through a phishing email on your phone it can migrate through your company's entire network?

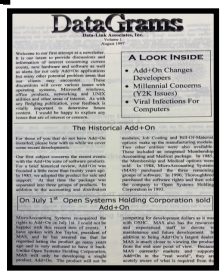
IF YOU'RE NOT A CLIENT...

You are receiving this complimentary copy of DataGrams because we would like to meet you!

Open this QR Code and send us answers to **5 Quick Questions** to start the conversation on how we can save you time, money and hassle on your cybersecurity and managed IT with our unmatched expertise and response time.

Happy Anniversary!

Andy Frielink
Vice President
35 Years

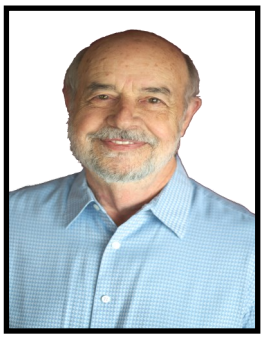

DataGrams

A LOOK INSIDE
- Add-On Changes Developers
- Millennial Concerns (Y2K Issues)
- Viral Infections For Computers

The Historical Add+On

On July 1st Open Systems Holding Corporation sold Add+On

DataGrams
25 Years



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.

Coming up in the next issue:

- Combat Cybersecurity Fatigue
- How Culture Assessments Can Level Up Your Security Program
- Crafting An Effective Shock & Awe

Become A **Mini-Celebrity** in Your Field to Attract The Best Clients

My favorite mini-celebrity is Shirley Temple. (ha!)

But really, none of us will EVER (really, never) be as famous as little "Bright Eyes", but you CAN position yourself as an expert in your field by promoting YOURSELF more than just your business logo, unique offerings, promos or discounts.

Everyone wants to work with the expert. And expert or not, the more often people see your face in ads and interviews, webinars and even in the ice cream social booklet, they gain more trust in you. Sadly, it will be regardless if someone is *actually* an expert or even a trustworthy person, but don't get me started.

There are many avenues you can take to celebrity but it usually factors in at least a handful of different media outlets:

- Author a book in your niche with a ghostwriter and send to your prospects.
- Guest write an article for a popular blog in your niche.
- Submit an article to a local paper or niche magazine.
- Advertise big at the local high school football games
- If you're good at social media, post DAILY
- Host webinars
- Conduct interviews of people your clients are interested in
- Start a podcast

Your celebrity POSITIONS you prior to the sale. Take every advantage to connect your dream clients to your "celebrity" and the best clients-to-be will be knocking on your door.

Get To Know: PII Protect Employee Security Training

Scan the QR Code (open your phone's camera> hover over code> tap link) to access a surprising infographic, a 2-minute training overview video and bullet-point breakdown about PII Protect.

PII Protect is the software we use to supplement our professional training in-house and offer to our clients as a one-stop solution for employee cybersecurity training requirements. Most cyber insurance policies now **require all employees with access to your network to receive ongoing cybersecurity training** as a requirement of cyber insurance coverage.

PII Protect

Do Yourself A Favor Refer Your Vendors

While it may sound self-serving, what I'm about to say is truly in your best interest.

REFER YOUR VENDORS TO DATA-LINK

Why?
Look what happened to Toyota!

The big picture: Multiple global manufacturers have been forced to shut down production due to attacks on their suppliers/vendors causing undeliverable goods and services required to finish goods to sell. You and yours should all utilize a trusted IT support firm.

Driving the news: In February 2022, Toyota was forced to suspend production at 14 plants in Japan for at least a day in response to a "system failure" at components supplier, Kojima Industries. Approx. 13,000 vehicles missed deadline that day.

The attack came just after Japan joined Western allies in clamping down on Russia in response to the invasion of Ukraine, although it was unclear if the attack was related.

If your vendor has cut-rate or (gasp!) **NO** IT management, you are essentially giving them the keys to the kingdom— production numbers for the day or the future of your business. You want to know you can TRUST that your vendor/supplier's IT firm is protecting them.

Do a favor for everyone involved and get them in touch with us!

Contact your favorite DLA rep, sales@datalinkmsp.com or (630) 406-8969

The Dangers of SpearPHishing

The first quarter of 2022 alone saw over 1 million phishing attacks with a 7% increase in credential theft, according to the Anti-Phishing Working Group (APWG). This accounts for all types of phishing, including the type we're talking about today called *spear phishing.*

While general phishing is a numbers game— email thousands of random people and surely some will bite– spear phishing is a highly-targeted, almost stalker-like, form of phishing. Cyber criminals investigate wealthy individuals or individuals with access to corporate or government financial accounts or sensitive data. Attackers use websites, blogs and social media to identify these high-value targets, dubbed *whales* or big catches.

CEO Fraud phishing attacks impersonate correspondence from executives to dupe employees who are responsible for finances to make wire transfer payments for fake invoices.

Oversharing on social media is the gateway to spear phishing.

Here is an excerpt of our April 5, 2022 Weekly IT Security Tip where we talked about oversharing on social media.

"My caption under a photo of a sunrise on a beach reads "My Hometown!"-Pam is in Bethesda, Florida
I tagged my mom in my photo - Pam is with Beth Dietrich Birchfield.
I bought my dog a new name tag and posted a picture of it on my Instagram.

So now, if a bad actor is after me they know my birthplace, mother's maiden name and favorite pet's name and they could confidently answer these common security questions on my behalf.

Instead of completely shutting down transparency on social media to protect your identity, how about the idea of giving false answers to your security questions?

Wish your birthplace was Athens, Greece? Went to grade school at Stanford University? Grew up on Rodeo Drive?... whatever suits you, but make sure to remember what fancy lie you told yourself!"

Understanding How They Attack

1. *Identify A Target*
Organized crime groups target business by using research to develop a profile on the company and its executives.

2. *Grooming*
Spearphishing emails and/or phone calls target who is typically in the financial department. Attackers use persuasion and pressure to manipulate and exploit the employee's human nature.

3. *Exchange of Information*
The victim is convinced they are conducting a legitimate business transaction and is provided wiring instructions.

4. *Wire Transfer*
Upon transfer, the funds are steered to a bank account controlled by the organized crime group.

As the CEO, when would you realize the money is missing? At the end of year meeting with your CPA? Your financial staff thinks the wire was legitimate so they wouldn't contact you. The amount of the transfer is reasonable as to not throw red flags.

Respect all, trust few.

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!

The Largest Password Manager In World –LastPass—HACKED!

This week, every one of the 25 million users of LastPass are surely wondering **"What happens if the vault that stores my passwords is breached?"**

The answer: Nothing. Password Managers require every user to create a Master Password to access their password portal for exactly this reason.

The Trick: This is the one password you never want to duplicate. Do not use for ANY other password anywhere. You must remember it. Keep a copy in safe deposit box.
Don't think twice about storing your passwords in a quality password manager. It is still the most secure, most efficient way to generate and lock down your passwords.

Coming Soon! Data Link has a short list and will be making a final decision on which password manager to officially offer to our clients. You'll love it!

DLA's "Weekly IT Security Tips" Used In Client's Company-Wide Mandatory Training

A few months ago I was approached by a client who asked us to add all 200+ managers and staff to our "Weekly IT Security Tip" email blasts.
Although the tip is written for an audience of CEOs and IT managers we were surely happy to get it in everyone's hands! They see the value in cybersecurity knowledge and the more the better.

Additionally, this company has been using the PII Protect training for about 4 years now. (see the bottom of page 2 for more info) They are serious about their cybersecurity.
Client confidentiality restricts me from saying who it is, but you know who you are and we give you a standing ovation for your commitment to cybersecurity and ongoing employee training.

Set Meaningful, Attainable Quarterly Goals and KPIs

Love it or hate it, we all know that setting business goals is necessary if you expect your business to grow—heck, to even keep up!
Inc.com reports that 92% of people who set goals never achieve them.

Goals: BHAG and other smaller goals
KPI: (Key Performance Indicator) a quantifiable measure of performance over time for a specific objective.

To set meaningful, achievable goals and KPIs, work backward from the vision. Example: To add 1 million in sales this year: +250,000 per quarter, 100 new clients @ 22 working days per month = 1.5 new customers per day at an average of $2,500/sale. Choose who will collect the data and how frequently. Make changes to the sales model or sales team as needed. At the end of the day, attaining the goal is all that matters to your business.

4-10 KPIs is an optimum number. Too many makes clutter and clouds focus.

Hire Talented Teams

Isn't hiring process is just awful? Newbies don't know the culture, they're gung-ho and *expensive—t*hey take up your team's valuable time. And the worst part is you don't know if they'll work out. Getting the right people in the door for the interview is your best chance at minimizing the cost.

When designing your ad,
reflect on past good hires.
Think about your culture and use culture assessments (see September DataGrams for "How Culture Assessments Can Level Up Your Security Program") prior to interview to build a cohesive team.

Thoughtful research and drafting of your want ad will get you the right fit.

Sign Up For Our
Weekly IT Security Tip

To receive timely, relevant cybersecurity tips and news every Tuesday morning.

We promise to NEVER spam.