Data-Link Associates, Inc.

February 2023

DataGrams

Proven, Field-Tested **Network Security Strategies** To Help Our Clients Make **Confident, Real-Time** Decisions For Their Company's Cybersecurity

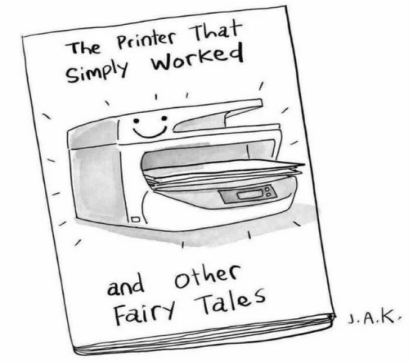
WHAT'S NEW?

Please Help Us Welcome **Brian Phillips** to the Team!

bphillips@dlainc.com

ThreatLocker is deployed in Learning Mode, mapping clients' Approved List of frequented applications.

WHAT'S INSIDE:



If Your Website Is Managed With WordPress

Take These Precautions Right Away

If you hired an independent developer to build/manage your website, they probably used WordPress—it has a learning curve but allows high levels of customization.

As of 2022, 2 in 5 websites are built and managed with WordPress and attacks on websites (in general) average an estimated 2,800 attacks per SECOND.

WordPress Core is safe WHEN you keep it updated to the latest version. There is only ONE Core and it is maintained by a world-class security team. Themes and plug-ins, however, are open-sourced and are not always safe to use.

Card-skimming is a frequent cyber attack on websites. They gain access to a device and/or network and install malware that collects all the credit card information entered on your site.

It's best to research reviews on a theme or plug-in before installing it on your website.

5 tips to keep your WordPress website safe:

1. Use a strong password for your login (Alpha-numeric with symbols) and MFA.

2. Install a trusted WordPress security plugin that can scan for malware. Run these scans regularly.

3. Enable SSL

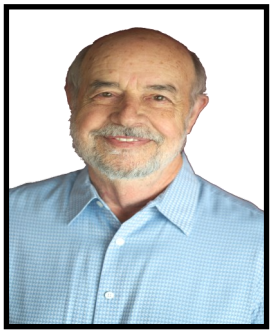
4. Host your website with a secure provider.

5. Only use reputable, legitimate WordPress plug-ins and update them when prompted.

The same way a mouse gets in the house, hackers will find the tiniest hole to enter your network and can cause major, sometimes unrecoverable, issues.

WELCOME BRIAN PHILLIPS TO DATA-LINK!

Brian is our newest Help Desk Engineer—responsible for distributing security patches to the devices in our network, troubleshooting device issues and has been delegated to Lead our ThreatLocker (zero trust) product. He is a graduate of the Cybersecurity program at Waubonsee Community College and came highly recommended from their IT Professor when we inquired to speak with outstanding recent graduates. He has been training with us since September 1st and it's time to make him official! Brian is a musician, cooks, and was recently engaged to be married! Congrats Brian, we're glad to have you as part of our exclusive team!



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.

EMERGENCY

(630) 406-8969

24/7

Coming up in the next issue:

- DNS Filter deep dive
- Digital Marketing for Manufacturers

SECTION179.ORG

Visit section179.org for info.

Don't forget to get all those tax breaks in for the computer hardware and software you purchased in 2022!

As Promised

What Every CEO Must Know About 2FA Bypass & Credential Stuffing

Before we dive in, let's review a couple of terms:

2FA/MFA—Two-factor (multi-factor) credential requirement. Most people enable this option (usually now required) in banking apps and company databases. Amazon even has an option for it.

Credential Stuffing—A type of cyberattack in which the hacker collects stolen account credentials (typically username/password combinations).

Brute Force attack— guessing credentials, usually based on previous personal knowledge of the target.

Many believe enabling 2FA will prevent an attack on their login 100% of the time, even if a hacker enters a correct username/password combo. The FACT is that 2FA slows them down, but unfortunately, is not a silver bullet fix.

To break into an account with a username/password AND 2FA enabled, a hacker first needs your valid username/password combination. Like the majority of us, hackers will use an economical option first, then move to the more expensive tactics if needed: they will send a bot and/or utilize a credential stuffing list. This process can be automated to make it very easy and cheap for them to gain access to many accounts in a short timeframe. Yes, they are efficient.

Weak protection against brute force attacks— by using easily guessable usernames, passwords and/or reused credentials as with credential stuffing— are the main reasons why 2FA is bypassed. In these cases, the first hurdle of entering correct credentials is already cleared.

Seems obvious, but let me say that a different way: If you protect your usernames and passwords, use unique passwords as often as possible, keep an eye out for major hacks (Twitter, Microsoft, banks, socials et al… where your credentials might have been compromised) and you are diligent about changing your passwords at that time, you will NOT need to worry as much about your credentials being a part of a credential stuffing hack because they cannot easily access your account. Without a brute-force or credential stuffing hack, your account is safe from a 2FA bypass. There are exceptions we'll talk about another time.

Bottom line: Use unique passwords, don't reuse and keep them secret, and you won't have to worry about 2FA bypass. Without the correct credentials, 2FA is irrelevant.

Are You New Here?

If we haven't met yet, contact us to schedule a

10-MINUTE Discovery Call

https://www.datalinkmsp.com/discoverycall/
Or call Pam at (630) 406-8969 x 574

Notable HACKS

We, consumers, expect big companies like the ones listed below to have excellent cybersecurity cultures due to their size, reach and global impact, YET here are a few that were burned in a cyberattack in the past year and everyone's talking about it. Embarrassing and costly.

Twitter— 200 million users' email addresses stolen according to initial reports. The company is now denying the emails were obtained via a hack on their servers. **Outside investigations are pending.**

Red Cross— Servers were infiltrated and exposed the personal information of more than 500,000 people receiving services from the Red Cross. **The culprit has not been found.**

Rackspace—Hosted Exchange customers are SMBs that don't have the need or staff to run a dedicated on-premise Exchange server. Rackspace was ransomed in December 2022. $30 million of Hosted Exchange business has been affected. **Time to switch to Microsoft 365 Exchange?—we can help.**

CashApp– A **former employee** breached its servers and stole names, stock trading info, account numbers, portfolio values and other financial info of 8 million customers.

(you won't believe this one...)

Microsoft– In March 2022, Lapsus$ (hacking group) compromised Microsoft, Bing, Cortana and several other products. Because Microsoft is HIGHLY secure and has around-the-clock cybersecurity teams, hackers only gained access to **ONE account**, and they were not able to retrieve any personal information.

Disinfect Your Digital Devices

You bring your phone and laptop with you everywhere. But when you bring along a device, make sure you're not bringing along bacteria and viruses.

Disconnect power, accessories, and turn off the device *before cleaning.*

1 Clean

Remove any dust and debris with compressed air, dry lens towel, or lint-free cloth.

2 Sanitize

Use a 70% isopropyl alcohol wipe or Clorox cleaning wipe and wring out the excess moisture. Lightly wipe the surfaces of your device, including the screen.

3 Dry

Allow the surfaces of your device to air dry for a few minutes before turning the device back on.

Did you know?

Researchers found **10 x MORE** bacteria on a phone screen than on a toilet seat or handle.

Only 1 in 20 clean their phone more than **twice per year.**

Clean, Sanitize and Dry to get rid of biological viruses.
But to prevent a computer virus…

APPLY UPDATES

Most malware used by cybercriminals won't work on an updated computer.

Follow us on LinkedIn for more tips:
Linkedin.com/company/data-linkassociatesinc.

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!

Cybersecurity Is Critical To Your Childrens' Education

On January 10th, the largest school district in Iowa (Des Moines Public Schools) canceled all classes after taking their network systems offline in response to "unusual activity" detected on its network the day before. DMPS has 60 schools with 31,000 enrolled students (pre-k to high school) and 5,000 employees. Don't let this happen to your children! You can help by advocating to budget for a "Pen (penetration) Test" for your school district— where the district hires an ethical hacker who attempts to hack into the network. The process will identify, test and highlight vulnerabilities and can also be used to evaluate adherence to compliance regulations. Find an IT firm that specializes in cybersecurity for education. In 2022, the top cyber-threats to schools were phishing, ransomware, SQL injections, data breaches and outdated technology.

Vent To A Peer Before Heading Into A Scheduled Negotiation

Doing this will allow you to prepare your mindset and get ready for what you are about to experience. A clear head can help you feel more confident because your insecurities won't be top of mind.

A Fun Marketing Tip For All Of Us From A Curmudgeon Named Kennedy

Dan Kennedy is a marketing guru and mentor to many contemporary marketing and sales greats. (Joe Polish, Dean Jackson, Russell Brunson et al) He's a 'NO BS' kind-of-guy (it's in the title of some of his books). Dan ends every email and letter he sends to his customers with this no-BS postscript:

P.S. Don't forget, whoever can spend the most money to get a customer wins.

LinkedIN's "Talks About" feature

allows up to 5 hashtags to describe your expertise and interests to display near the top of your profile. This feature was introduced in Spring 2021 but I don't see it used often. It's a cool "speed date" version of your profile. Check it out!

Co-Managed IT

What If Your Internal IT Department Is Overwhelmed, Unable To Keep Up And Facing Projects They Cannot Handle On Their Own, Putting You At Risk For A Significant, Expensive IT Failure?

I know you're tempted to think, "We don't need more IT. Our internal IT department has it handled."

Fact is, your IT department might not be as prepared and capable as you may think to handle the rising complexity of IT systems for your growing company and the overwhelming sophistication of cyberthreats with the current resources, time and skill sets they have.

If true, **your organization IS AT RISK for a significant IT failure**.

To be crystal clear, I'm not suggesting your IT lead and staff aren't smart, dedicated, capable, hardworking people. Fact is, nobody likes to go to the CEO with "bad news" or to constantly ask for more money or help, particularly if they've already been told "there's no budget." Further, it takes a small army to run an IT department for a company of your size and growth – and you may be unfairly expecting too much of them, setting them up for failure.

If (when?) your company is breached and your IT department doesn't have the requisite knowledge and/or resources to correct it, you can't blame them

You're big enough to need a professional-grade IT department but can't afford to add significant overhead in IT tools and staff – particularly IT specialists with skills and tools that are only needed part-time.

That's where we can help!

FREE SPECIAL REPORT

The CEO/CFO's Guide To Co-Managed I.T.

- We don't replace your IT staff, we add to their skill set.
- This is NOT about taking over your IT leader's job or replacing your IT department.
- You don't need to add to your head count
- Your IT team gets instant access to the *same* powerful IT tools we use to make them more efficient.
- "9-1-1 On-Site" in the unexpected event your IT leader was unable to perform their job or a disaster were to strike.
- You Get A TEAM of smart, experienced IT pros. No one person can know it all.
- Stop worrying (or worry less!) about falling victim to a major cyber-attack, outage or data-erasing event.

Contact Pam to sign-up or upgrade to Co-MIT today!