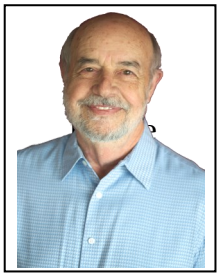
Data-Link Associates, Inc.

May 2022

DataGrams

What's New?

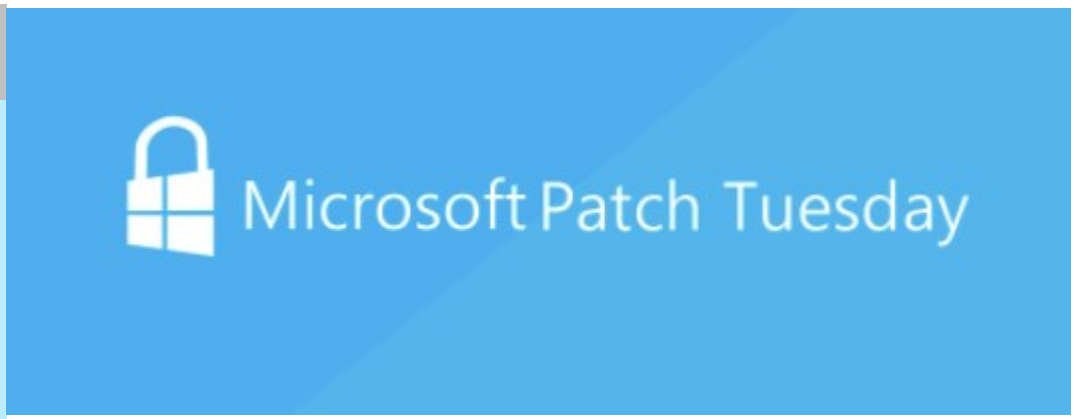
May 2022



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 We All Need PATCH TUESDAY

Have you heard of Patch Tuesday?

If not, you have probably at least experienced it. Have you noticed that sometimes when you turn on your computer in the morning it looks different?. All your windows and applications are closed or something doesn't work as it did yesterday? It's (probably) not your imagination and no one (probably) broke into your computer overnight.

Don't be alarmed, you just got PATCHED!

Although it seems counter-intuitive, if these strange things are happening to you, please know that someone out there is taking good care of your computer system.

Patch Tuesday is the name Microsoft gives to the second Tuesday of every month when they push out their newest critical and non-critical security patches, software corrections with updates and introduces new features. Patch Tuesday is an event around here! Adobe, Oracle and others regularly release their software patches on Patch Tuesday, too.

What is a "patch"?

A patch is just what is sounds like...it "patches up" security flaws and vulnerabilities—just like in the old days when folks would put a patch over a rip in jeans or a jacket instead of buying new. The caveat, as you get with most great things (am I right?), is that the patches can break something by impairing or completely disabling a function that worked prior to the patch. Good IT firms will accept and exercise the patches prior to releasing to your devices so they have time to try to "break" the patch. However, most IT companies will take exception to this rule if the patch contains a zero -day vulnerability (explained on pg 4).

With all the IT goodies in the patches, you want to make sure everyone at your company is diligently allowing patches to your devices every month. Whether you have a Head of IT on staff or a Managed Service Provider (like Data-Link) to push the patches through to your company's devices, there are steps each user should take to ensure the patch lands safely on their device each month. Keep in

Continued on pg.2

Continued from pg.1

mind, although Tuesday is the day of the week that Microsoft pushes out their patches, your device may receive the patch any day of the week.

Smooth Operator

Here is how every staff member with a computer or other device should adequately prepare their workstation to receive patches.

At the end of each workday:

1. CLOSE ALL APPLICATIONS via the 'X', don't just Minimize to clear your desktop… this means you, Cheryl. (Outlook, your CRM, your ERP, Adobe, Teams, Slack, close everything)
2. LEAVE COMPUTER ON ALWAYS, but you'll want to LOCK your workstation by pressing Ctrl, Alt, Delete and choosing the 'Lock' option. This will require a password to regain access and keep everyone else out.
3. KEEP CONNECTED TO THE INTERNET. Connection is done automatically these days so most won't need to worry about this, but this is a critical step.

When these steps are not taken, the patches cannot be completed and the device is left vulnerable to security breaches. For Data-Link clients, it is our opinion that the steps above should be written into each of our clients' company policy for the devices' main users. Even the most careful user can forget, so the device we are charged to protect isn't receiving the patch immediately and makes the patch fail. When a patch failure is detected, Data-Link attempts to take control of the device and force a reboot. In the rare case we cannot get through, we reach out to our client's main IT contact to resolve.

Exploit Wednesday

You guessed it! The day after Microsoft et al releases their patches, bad actors are chomping at the bit to exploit the security updates that were just released. They immediately scour the patches to take advantage of previously undisclosed vulnerabilities that will remain in unpatched systems. This is why it is so very important to ensure your users and devices are 'patch ready' every day. This allows your IT department to swiftly apply the patch to your device to protect it.

Immediate Release Patches Save The (Zero) Day!

An Out-Of-Band (OOB) Update is an unplanned but necessary security update that can be pushed out as often as needed.

To reduce the workload of IT staff everywhere, developers tend to wait to bundle the updates for release on Patch Tuesday.

The exception is a zero-day vulnerability or other critical security issue. An OOB can happen at any time.

So whether you're "a PC or a Mac" be sure to be ready for Patch Tuesday so you can receive critical patches for your devices!

For anything you need or if you have questions, you know where to find us. (630) 406-8969 and pbirchfield@datalinkmsp.com

FBI Wins 3-2 vs. Secret Service In Annual Charity Hockey Game

April 30th, Washington Capitals' ice rink—A day that residents within Arlington, Virginia surely behaved as law abiding citizens.

In what would have been a bad day for Al Capone, both the FBI and the U.S. Secret Service were in town to battle on the hockey rink for the Annual FBI vs. U.S. Secret Service Charity Hockey Game.

Both the FBI and Secret Service work in the cybersecurity arena and provide us with invaluable information to keep U.S. citizens cybersafe and aware.

In a close game, the FBI won 3-2.

Tickets were $10 and all proceeds benefit Heroes, Inc. (heroes.org) a non-profit that supports the spouses and children of law enforcement officers and firefighters who gave their lives in the line of duty to the greater Washington, D.C. community. Support for the family begins within 24 hours of the tragic loss and continues indefinitely.

The final donation amount was not available at time of publication but it is estimated that $20,000 was earned from this event.

5 Tips To Spot Candidates With The Right And Wrong Stuff

I recently had the opportunity to sit down with Carter Cast, the author behind *The Right – And Wrong – Stuff: How Brilliant Careers Are Made And Unmade.* Hiring success has a great influence on career success, and we discussed five negative archetypes that confront employers while filling a job opening. Together, we discovered some telltale signs that your interviewee may fall into one of these categories.

Captain Fantastic
While it might seem like "Captain Fantastic" would be a vital part of your team, they often cause division. Someone who is a Captain Fantastic is usually overambitious and has no qualms about stepping on others to get ahead. If you're interviewing a candidate and they mention that their greatest accomplishments revolve around beating others rather than delivering value or developing teams, you probably have a Captain Fantastic on your hands.

Solo Flier
Have you ever worked with someone who thinks their way is the best and only way to do something? It's very frustrating. While this type works well individually, they can be detrimental to a team environment. They usually claim to have no time or were too busy to accomplish their tasks; in reality, they may fail to hire and delegate properly. I've met with many people who fit this category and end up leaving their job due to burnout after taking on too much work.

Version 1.0
Change is a necessity in the workplace, but sometimes people prefer to stick to their routines. To spot these people in interviews, listen to their stories and pay attention if they mention changes in the workplace and how they responded. If they stayed on the same path, that's a red flag. I knew a manufacturing executive who failed to adapt to new technologies. This caused him to lose some of his biggest clients, and the business fell into a tailspin.

The One-Trick Pony
These people usually get stuck in a rut because they rely on their greatest strength to solve *all* problems. They will often aim for lateral moves rather than trying to broaden their horizons. I interviewed a one-trick pony recently who wrote amazing copy but struggled when meeting with clients in person. His communication skills weren't strong enough to work with clients or lead large teams. His career became stagnant even though he was eager to grow and move up.

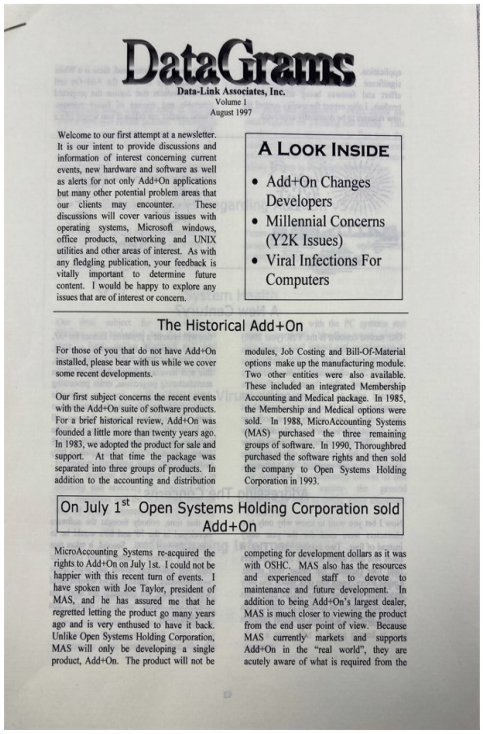
Whirling Dervish
Energetic employees improve morale and production in a workplace but sometimes lack the follow-through needed to complete projects. You can usually spot these people in interviews if you notice them avoiding your questions. They often come up with excuses for why they didn't achieve results. Great ideas and strong morale do not make up for a lack of completion.

With knowledge of these archetypes, you can avoid hiring the wrong candidate for your team and instead focus on finding the perfect fit.

Dr. Geoff Smart is the chairman and founder of ghSMART, a leadership consulting firm that exists to help leaders amplify their positive impact on the world. Dr. Smart and his firm have published multiple New York Times best-sellers. He stays active in his community and has advised many government officials.

Does Anyone Else Remember Word Perfect?

DataGrams Volume 1 Issue 1 was published in August 1997 using Word Perfect. Including writing and editing, this first issue took two weeks to produce. Today, we use Microsoft Publisher and takes us about two days, start to finish.



DataGrams
Data-Link Associates, Inc.
Volume 1
August 1997

Welcome to our first attempt at a newsletter. It is our intent to provide discussions and information of interest concerning current events, new hardware and software as well as alerts for not only Add+On applications but many other potential problem areas that our clients may encounter. These discussions will cover various issues with operating systems, Microsoft windows, office products, networking and UNIX utilities and other areas of interest. As with any fledgling publication, your feedback is vitally important to determine future content. I would be happy to explore any issues that are of interest or concern.

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

The Historical Add+On

For those of you that do not have Add+On installed, please bear with us while we cover some recent developments.

Our first subject concerns the recent events with the Add+On suite of software products. For a brief historical review, Add+On was founded a little more than twenty years ago. In 1983, we adopted the product for sale and support. At that time the package was separated into three groups of products. In addition to the accounting and distribution modules, Job Costing and Bill-Of-Material options make up the manufacturing module. Two other entities were also available. These included an integrated Membership Accounting and Medical package. In 1985, the Membership and Medical options were sold. In 1988, MicroAccounting Systems (MAS) purchased the three remaining groups of software. In 1990, Thoroughbred purchased the software rights and then sold the company to Open Systems Holding Corporation in 1993.

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

MicroAccounting Systems re-acquired the rights to Add+On on July 1st. I could not be happier with this recent turn of events. I have spoken with Joe Taylor, president of MAS, and he has assured me that he regretted letting the product go many years ago and is very enthused to have it back. Unlike Open Systems Holding Corporation, MAS will only be developing a single product, Add+On. The product will not be competing for development dollars as it was with OSHC. MAS also has the resources and experienced staff to devote to maintenance and future development. In addition to being Add+On's largest dealer, MAS is much closer to viewing the product from the end user point of view. Because MAS currently markets and supports Add+On in the "real world", they are acutely aware of what is required from the

Microsoft Seizes 7 Russian Domains During Ukraine War

After obtaining a court order, Microsoft seized seven internet domains used by Strontium, a Russian state-sponsored hacking group to commit cyber attacks on Ukrainian media outlets, and government agencies.

Because it is an extension of Russia's GRU, Strontium likely receives its objectives and orders from the Kremlin.

As the war in the Ukraine continues, and Russia is forced to pivot from its original military objectives, nation-state groups like Strontium are likely to launch more disruptive cyberattacks aimed at Ukrainian infrastructure, government and media sectors.

Before this seizure, Microsoft had already gone through this process 15 times to seize control of more than 100 Strontium-controlled domains.

Zero-Day Vulnerability Patches (cont'd from pg. 1)

Zero-day vulnerabilities are cybersecurity threats that do not yet have a patch to neutralize it. The term 'zero-day' refers to the the number of days the vendor or developer has to release a patch to fix the vulnerability—meaning a fix needs to be developed and pushed out *immediately*.

In the time between the public announcement of a zero-day and the release of a patch is prime time for hackers to try to exploit the holes and they do. Imagine a hacker out to lunch with friends, at the theatre, grabbing a Jamba Juice and suddenly they see a zero -day on their feed... "Sorry gotta go!"
It sounds funny, but it probably happens all the time.

You have a toolbox of information -courtesy of the Weekly IT Security Tips and mailed monthly newsletters- and a wingman (yours truly) to help get you though and survive a zero-day or any other breach or data loss.

If you implement our recommendations, you have a very good chance of not only surviving a breach but recovering quickly with little to no damage to your business and minimal downtime.

Next Month: The best Disaster Recovery documents to have and procedures to follow. >>>>>>>