DataGrams

Merry Christmas and Happy Holidays!
From our family to yours, we wish you a very happy holiday season.

WHAT'S INSIDE?

DATA-LINK INTRODUCES 2 NEW SECURITY PRODUCTS

DNS Filter

We are excited to announce the newest addition to our tech stack, DNS Filter, an advanced DNS filtering technology that elevates a network from secure to a next-generation ready, AI-intelligent force that keeps hackers away from your company's network.

CEO favorite features:

- Website Reporting on employee activity
- Remote worker protection when not on the corporate network
- Enhanced internal corporate security

THREATLOCKER

As a part of an ongoing effort to ensure all systems are secure for our clients, we are now adding a zero-trust approach to your security stack. As attackers become more sophisticated, so do the complexities in stopping software-based threats.

ThreatLocker helps with:

⇒ Layered Security

⇒ Ransomware Prevention

⇒ Compliance

⇒ Internal Disputes

⇒ Storage Control

⇒ Data Privacy

Pairing DNS Filter with ThreatLocker delivers a ONE-TWO PUNCH!

---

info@datalinkmsp.com   (630) 406-8969 ext 574

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:

- Cyber-Security Trends for 2023
- A Glimpse Into DLA's Onboarding Process

SECTION179.ORG

Visit section179.org for info.

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

DNS FILTER:
Data-Link's Newest Addition

Key features include website reporting to solidify termination cases, advanced protection for remote workers, and enhanced internal corporate security

Data-Link Associates is excited to announce the newest addition to our tech stack, Advanced DNS Filtering by DNS Filter.

What is a DNS? The DNS (Domain Name System) is the phonebook of the Internet. Humans access information through domain names like nytimes.com or espn.com. Web browsers (like Chrome or Edge) understand what to load when given an IP (Internet Protocol) address. DNS translates domain names to the IP addresses so browsers can load Internet sources. Each device connected to the Internet has a unique IP address which other machines use to find the device. DNS servers eliminate the need for humans to memorize the IP addresses such as 192.168.1.1.

What is DNS filtering? If the DNS is the phonebook of IP addresses, then DNS Filtering is the Caller ID and the Call Blocker. Most companies typically have DNS filtering in place to block employees and guest Wi-Fi users from specific sites. Some block social media or illegal content sites for some or all users.

What is ADVANCED DNS Filtering by DNS Filter? DNS Filter is leading the DNS filtering industry with next-generation AI (artificial intelligence) that can:

- Block access to websites created in the last 24 hours (hackers and scammers create fly-by-night malicious websites).
- Block phishing, viruses and other cyberthreats, including zero-day attacks, with smart identification of malicious domains.
- Identifies malicious websites in real time using AI categorization.
- Helps prevent zero-day threats using advanced scanning technology.
- Blocks previously uncategorized phishing threats with imagery-based anti-phishing tactics.
- Mitigates botnet, malicious crypto-mining and malware threats via threat feed augmentation.

*************** CEOs Especially Love These 3 Features! ***************

- WEBSITE REPORTING
  Now you can see what your employees are actually doing all day!
  Pull website visit reports for a specific user in your network.

- ADVANCED PROTECTION FOR REMOTE WORKERS
  Remote employee devices are not always connected to the corporate network. Advanced DNS Filtering protects those devices 24/7/365.

- ENHANCED INTERNAL CORPORATE SECURITY
  Enhances existing protections in your current technology stack.

For Clients with Managed Services: DNS Filter is *INCLUDED in your program for 2023.* We will contact you prior to rollout to discuss security level options. Rollouts will start in January 2023.

DNS Filter is available to non-managed clients, too! Please contact us for pricing.

Shopping Tips

'Tis the season for gifting! … and scammers… *especially* scams via the internet.

Though the main message is basically the same every year, we have a different driving force for deal-hunting this year that can make folks less diligent in protecting their personal information.

And due to **inflation and recession fears this year**, consumer price-consciousness will be magnified driving many shoppers to look for the best deals, some in a desperate fashion. Scammers dream about struggling economic times like these because consumers are thinking less clearly, many with blinders on to suspicious activity, eyeing the prize of a plentiful grab of gifts for their loved ones.

Here is my compilation of Top 5 Tips for Holiday Shopping in 2022:

1. **Shop with reputable retailers**— stick with tried and true. Resist a deep discount from a retailer you've never heard of.

2. **Beware of amazing deals**— Thoroughly investigate a deal that's too good to be true. A scammer will take your personal information and ship you nothing.

3. **Don't browse on public WiFi unless you're using a VPN**— including a password protected "Guest" Wi-Fi at hotels and malls, they're not safe for sending sensitive data.

4. **Don't click through on social media**— Go directly to their website via a web-browser. This includes retailers and charities.

5. **Check bank/ credit card accounts routinely, at least once per week.** — It's best to use a credit card instead of a debit card when shopping online so you can easily dispute the transaction if needed.

Victims of holiday scams are encouraged to file a complaint with the FBI at www.ic3.gov.

Data-Link Adopts THREATLOCKER As Mandatory Cybersecurity Measure

"We need three forms of ID before we let you in, Mr. IP address."

The cybersecurity paradigm is shifting to a "zero-trust" model. Zero-trust says "if we don't specifically let you into a network, you aren't getting in."

ThreatLocker will
Allow what you need and block everything else...including ransomware.
Ringfence™ your applications. Stop them from being weaponized against you.
Only allow specified applications to run as administrator with Elevation Control.

ThreatLocker benefits:
Allowlisting: Only permits approved files and applications to execute and blocks everything else.

Ringfencing™: Allows for granular control over what applications are allowed to do. Enables you to limit interaction between applications, their access to files, the registry, and the internet. It helps protect you against the weaponization of trusted applications while mitigating the risks posed by application vulnerabilities.

Elevation Control: Just-in-time elevation on a temporary or per-application basis allows organizations to remove local admin permissions without stopping productivity. This allows non-admins to download/run pre-approved applications without an admin password.

Storage Control: Storage Control gives you control over all storage device access-including USB devices, network shares, and even individual files to help protect data. The solution limits access to data by application, controls data exfiltration, and minimizes the damage caused by cyberattacks. Every file is tracked and can be easily located if moved or deleted.

For Clients with Managed Services: ThreatLocker is *INCLUDED* in your program for 2023 for Windows devices. We will contact you prior to rollout to discuss the impacts on the system. Rollouts will start in January 2023.

Please contact us with any questions!
We are thrilled to be offering ThreatLocker to our clients.

If you're new here…we invite you to:
Scan To Sign Up For Our
Weekly IT Security Tips
to receive timely, relevant cybersecurity tips and news via email
every Tuesday morning.

Thank you for your support! Our list has reached 1,021—consisting of 361 CEOs/ principals and 600 support staff who receive these tips each week. Congratulation on your commitment to cybersecurity. We promise to NEVER spam.

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!

What Hackers Want MORE Than Your Credit Card Information

Your medical information is much more valuable to a hacker than your credit card number. Stolen medical info sells for 10x more than CC numbers.
Your medical records provide extensive personal information that can be used to commit identity theft, financial or insurance fraud and extortion. Stolen credit card funds are easy to dispute and the physical card easy to replace; but once someone has your SSN or medical history, that's a problem you could have for life.

You Are More Likely To Be Hacked On A WEDNESDAY (Thursday is second)

Why Wednesday?
To up the odds of infecting a target, cyber criminals target the middle of the week, when most people are likely to be at work. If you think about it, if you're going to take a day off it's usually Friday or Monday.

It Takes Forever To Detect A Breach

On average, it takes 229 days (that's almost 8 months) before a company that is not managed by an IT professional utilizing next-gen EDR to realize it's been hacked. In addition to the time it takes to spot a breach, companies are also allowed to wait before notifying victims. (Most states require notice within 30-days)

What We're Reading...

ADAM: "The Necromancer" - Terry Nacour

PAM: "Discipline Equals Freedom" - Jocko Willink

MIKE: "The Actor's Life"- Jenna Fischer

ANDY: The Wheel Of Time series - Robert Jordan

BRIAN: "Devil In The White City" - Erik Larson

I.T. MOVES FAST!
HERE'S A (CURRENT) LIST OF DATA-LINK'S SERVICES & PRODUCTS

SERVICES

- Cybersecurity consult and management
- Fully Managed IT Services
- IT Wingman (Co-Managed IT)- Helpdesk support for Head on-staff IT person includes 2 weeks per year of vacation backup coverage.
- Business Consulting
- M365 Migration
- SAGE ERP– sales and support
- AddOnSoftware– sales and support
- Break/Fix (Time & Materials)
- Technology Business Review
- Weekly IT Security Tips
- Monthly Client Newsletter
- IT Disaster Recovery Planning
- Hardware & Software recommendations and sales
- M365, Duo MFA, TaskFire and Datto license recommendations
- Diagnostic Network Scan
- Identity and access management (2FA)
- Server & Workstation backup
- Dark-Web monitoring
- Cloud-application backup
- Firewall monitoring and updates
- General network monitoring and maintenance
- Software patching and updates
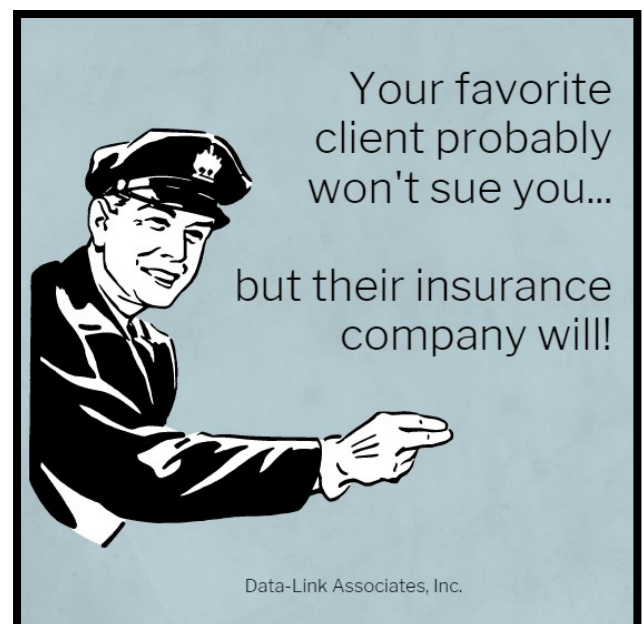- On-Site support
- Email backup

If we think your company would benefit from an additional service or product this year, we'll discuss it during your Technology Business Review.

OUR STACK

- N-Central RMM
- SentinalOne EDR
- Datto backup solutions
- AutoTask ticketing
- THREATLOCKER zero-trust
- DNS Filter (advanced)
- SonicWall firewall
- BreachSecureNow/PII Protect phishing email training
- HP computers

PRODUCTS WE OFFER

- SAGE ERP
- AddOnSoftware
- HP hardware
- SonicWall firewall
- Datto backup appliances
- Diagnostic Network Scan
- Breach Secure Now/ PII Protect
- MS Office 365

Your favorite client probably won't sue you...

but their insurance company will!

Data-Link Associates, Inc.