

DataGrams

What's New

WELCOME SPRING!

Do you want DLA's timely and valuable blog posts in your feed?



Follow Data-Link Associates on Facebook

WHAT'S INSIDE?

It's Time To Prepare For Growth (and Disaster)..... 1

The Pain of Discipline or the Pain of Regret.....2

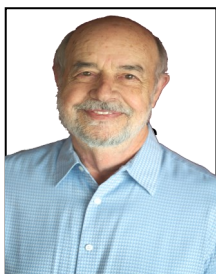
What is "Hacktivism"3

How To Make Time Work For You3

The 5 Great Cyber Powers of the World..... 4

Quotes, Fun & Utility.....4

April 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.



It's Time To Prepare for Growth (and Disaster)

Current events in Eastern Europe are not only one of the most devastating humanitarian crises of our time but is also causing a stir in the cyber community. At the hearts of c-suites and investment companies around the world, corporations are simultaneously preparing for growth, as every company does going into Q2, while preparing for a cyber disaster.

As you know, cybersecurity is a long game; it does not work as a band-aid to stop the bleeding. Infrastructures need to be investigated and security holes identified. Old equipment needs replacement and the entire staff needs to be trained on cybersecurity. It is nearly impossible to implement a working cybersecurity system overnight.

Many reading this article have been clients of ours for years. A handful of you have completed your annual

Technology Business Review this month and are budgeting sufficient funds to update infrastructure and devices that will be expiring in the next couple of years to make sure your environment stays safe and operations stay up and running, day-in-day-out. We applaud your efforts and commitment to your business's growth and preparedness for disaster.

Eastern Europe is a well-known hub for sophisticated hackers, but as push as they are, they tend to resort to phishing emails as their number one way to breach a network. It takes **just one click** to let malware in.

Here are **two barriers** you can start **TODAY** to prevent hackers from infiltrating your network:

- 1) Scan your Network and complete a Technology Business Review

Continued on pg.2

Continued from pg.1

- 2) **Start Cybersecurity and Phishing email training for you and your staff.**

How to Scan Your Network/TBR – \$450 (reg \$550)

Well, you don't do it... we do it for you. Then, we compile and present the results to you.

Email or call me pbirchfield@datalinkmsp.com or (630) 406-8969 x 574 to initiate a scan. We'll scan your network for devices, holes in security and dive into the Dark Web looking for compromised passwords on your domain. The scan takes about 48 hours to complete, then the scans are reviewed over the course of about 3 days. When the review is done, I will contact you to set up a video call or in-person meeting to discuss what we found and talk about solutions.

Sticker shocked? We're running a Russia special for this service during the month of April. The fee pays for our time. The scan is no cost.

How to Start PII Protect – \$150 per month

We use PII Protect to train our clients' staff on cybersecurity. Staff training is proven to be THE #1 WAY to avoid a malware infection. Many companies attach an awards system and a progressive discipline

“Corporations are simultaneously preparing for growth... while preparing for... disaster.”

system to the trainings and phishing campaign results due to their actions being a potential security risk to the company.

- 1) **Initial** cybersecurity training is emailed to your staff.
- 2) **Once per month**, a short, relevant video with a micro quiz is emailed to your staff. Scores are totaled and ranked for the organization.
- 3) **Once per quarter**, a fake phishing email campaign is emailed to your staff. I will notify the head of IT that the email is coming. After a week of the campaign run, I will send the results. The report tells us 4 pertinent pieces of information: who received the email, if they opened it, if they clicked on the link and if they entered credentials.
- 4) **Every two weeks**, a fake phishing email is sent to random users as an additional “sneak attack”.

DLA recommends both a Network Scan/Technology Business Review and an on-going Phishing email training for every business who accesses the internet.

DataGrams are typically for informational and entertainment purposes only, and not for selling services. We are taking exception to the rule to let you know about these 2 crucial services that we highly recommend everyone implement.



“We all must suffer from one of two pains:

the pain of discipline or the pain of regret.

The difference is discipline weighs ounces while regret weighs tons.” **Jim Rohn**

NOW Is The Time To Create Your BACKUP & DISASTER RECOVERY PLAN

Why Not Take 4 Seconds Now To Protect Yourself, Protect Your Company And Protect Your Customers?

In the event of a data breach or natural disaster that takes out your network, do your employees know who they should call? The CEO? The police? The fire department? Data-Link?

Does your cyber insurance policy require your company to have a documented system in place to recover your data?

If the person in charge of IT is unreachable, who is on-point to ensure quick data recovery to get your operations back up and running?

Get your FREE Backup & Disaster Recovery Plan TEMPLATE! Email Pam at pbirchfield@datalinkmsp.com

Get More Free Tips, Tools and Services At Our Website: datalinkmsp.com

(630) 406-8969 x574

What is “Hacktivism”?

Not all hacks are motivated by money or to prove a hacker’s skill.

Some hackers are known as “hacktivists” - people who hack to achieve a social or political outcome.

The most notable example of hacktivism comes from a group called *Anonymous*- a loosely affiliated group of hackers from around the world that banded together to attack organizations they feel are against their ideals.

Anonymous is reported to have attacked U.S. government agencies, the Church of Scientology and copyright protection services as well as PayPal, Mastercard, Visa, Sony, media companies, military personnel and police officers.

Supporters have called the group “digital Robin Hoods” while critics have described them as “cyber terrorists”.

Hacktivism typically use a denial-of-service attack – where a group of hackers encourage spamming the target company with emails and phone calls to cripple their network

In 2012, *Time Magazine* called *Anonymous* one of the “100 Most Influential People” in the world, alongside Warren Buffett, Catherine, Duchess of Cambridge and Rihanna.

How To Make Time Work For You



No matter how much money or influence you have, we are all limited by time. It seems the most successful people we know are able to *bend* time to make it work in their favor. They always show up pressed and dressed, you see them at every after-work function, every children’s concert and they seem to float through daily life obstacles without the added stress of time.

Your kids won’t learn how to “bend time” in physics class and Albert Einstein would probably have a stroke if he heard me now – Einstein stated that time was an illusion, that the past and future are already written for us. Stay with me, I think the concept of bending time is a valuable tool to know and to teach.

I am writing this article on a hard deadline of 30 minutes when it takes about 45 to write and edit an article of this size and minimal complexity.

How will I cut down this task by 15 minutes? The answer is not by cutting corners...

The television is off, no radio, no coffee (so no bathroom breaks), no snacks, my phone is 10 feet away from me on the coffee table on silent, email and Teams are signed out and the house is completely quiet.

Tick tock... 21 minutes to go...

If you commit yourself to QUIET... quiet the workspace, quiet the mind.

If you commit yourself to ORGANIZATION...it’s difficult to think while your home, desk, mind, or even your life is cluttered. It takes much less time to organize than to reel in thoughts of “am I forgetting something” or, perish the thought, miss doing something *completely*.

If you commit yourself to FOCUS...shut off all distractions. Email, apps, Facebook, Teams, everything.

If you commit yourself to a RESULT....make a time-bound commitment to yourself and try to exceed it.

If you commit yourself to diligent practice of quiet, organization, focus and committing to a result you can bend time and make time work *for* you, not against you.

Do you have any time or organization hacks?

Do you know a great focus technique?

Do you have a tip for working while at home and the house is bustling?

LET ME KNOW!

Can’t wait until the next month’s newsletter for more cyber news?



Find us on:
facebook®

Follow Data-Link Associates
for valuable and timely IT blog posts

■ The 5 Great Cyber Powers of the World

According to the team at Belfer Center for Science and International Affairs at Harvard's Kennedy School, the most powerful cyber countries in the world (meaning a strong cyber power in defense, military, economy and intelligence) are the United States, China, the UK, Russia, Netherlands, France, Germany, Canada, Japan and Australia.

We have had the debate here at Data-Link and ultimately compiled a list of the countries we would put in our TOP 5. (We tied on China and Russia)

1. United States of America

The United States is THE most dominant cyber power in the world with formidable strength in cyber offense, defense, resilience and intelligence. We'll put a boot in your ass, for sure. Don't mess with the U.S.

2. Russia — a tie with China

Russia is no stranger to cyber warfare. They have armies of hackers and have successfully breached the U.S.'s defenses in the past. Russia is the grandfather of cyber surveillance and has put much effort into its cyber infrastructure.

3. China — a tie with Russia

As the king of industrial espionage and as a global economic powerhouse, it is no surprise that China has risen to embrace cyber technology in the digitalization of its industries. They are considered to be the only state currently on a trajectory to join the U.S. in the first tier of cyber powers but they are nowhere near closing the gap with the U.S.

4. United Kingdom- (England, Scotland, Wales and Northern Ireland)

The UK has developed National Cyber Security Strategies that focuses on building resilience to cyber attacks. By 2025, they have goals to strengthen the UK's cyber ecosystem and go digital to reduce cyber risk and maximize the economic benefits of digital technologies.

5. The Netherlands

Just a stone's throw across the North Sea from England, the Netherlands boasts an impressive cyber offense. They proved they could play in 2014 when they successfully infiltrated Russian hacker group, Cozy. The World Economic Forum's 2016 Networked Readiness Index — measures the cyber competitiveness, innovation and well-being of 139 world economies-ranked The Netherlands number 6.

■ QUOTES, FUN & UTILITY

"Don't make decisions when you're angry; Don't make promises when you're happy."

When microwaving pizza, put in a glass of water with it. It will keep the pizza from getting spongy.

The shortcut to Undo on your PC is CTRL+ Z. Redo by pressing CTRL + Y.

The quotation marks on feet and inches (ex. 5'0") are actually called primes. Foot uses a single prime and inch uses a double prime.

Eminem is the best-selling rapper in history.

Only about 1% of people in the world are naturally ambidextrous. That's 70 million people out of the world's population of 7 billion. 10%-12% of the world's population are left-handed.

Quick handwriting is a sign of intelligence. It indicates quick-learning and the mind working faster than the hand can write.

Here are a few of the new words Merriam-Webster Dictionary added in October 2021:

TBH: an abbreviation for "to be honest"

VACCINE PASSPORT: a physical or digital document providing proof of vaccination (such as COVID-19)

OUBLECK: a mixture of corn starch and water that behaves like a liquid when at rest and a solid when pressure is applied. A favorite kids science experiment.
Fun Tip: Add food coloring!

DOORBELL CAMERA: like a Ring doorbell

BIT ROT: the tendency for digital information to degrade or become unusable over time.

