

DataGrams

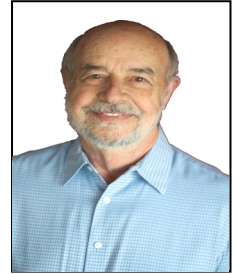
What's New

Happy Anniversary!

Adam Frielink: 26 years

Our Mission

To provide IT solutions and services that allow our clients to succeed in an ever changing and challenging business environment.



This monthly publication provided courtesy of Richard Frielink, Founder & President of Data-Link

- FREE REPORT: Protecting Critical Data..... pg 2
- Email Marketing: Getting past the new spam filters.pg 3
- AWS Bucket Mistake Cause 120,000 IDs leaked....pg 4
- How to pick the sweetest, juiciest watermelon.....pg 4
- Common passwords found in data breaches.....pg 4

Anatomy Of A Phishing Email

Your new salary

Alana <d26d8433857394f75c3ed492cc62fac9@google.com>

To:

EMPLOYMENT_AGR...
87.7 KB

Download All · Preview All

Hi,

As discussed, you'll be getting a [20%] increase in your salary. Your salary will be officially updated on [July 1st] so you'll see the boost on your [July] paycheck.

Please re-sign employment agreement before this weekend.

Thank you for all your hard work. Appreciates your efforts and achievements so far. This pay raise is well-deserved.

Keep it up!

Alana

Local government employees were recently targeted by cybercriminals using this phishing email lure promising a salary increase. The bogus email appeared to come from within the organization and contained a call-to-action to click the attachment within. When the attachment was clicked, the user's system became infected by malware.

At the time of publication, Microsoft had just released a patch for this vulnerability target, known as Follina, within the June 2022 Patch Tuesday Windows Updates. Follina was in the wild without a patch from Microsoft for about a month. During that time, since Data-Link

managed services clients are covered by spam filters and EDR (Endpoint Detection and Response), our clients' network and devices had the best protections possible.

RED FLAGS IN THIS EMAIL

- Social norms not followed. Employees are typically pulled into a meeting, not emailed, when a raise is announced. If an email was going after the meeting, the recipient would have been expecting it.
- Special characters before the word "Hi" and recipients name not used.

Continued on pg.2

Continued from pg.1

- “As discussed” implies a conversation took place recently.
- The brackets are out of place for this email subject. It looks like a template.
- “Re-sign employment agreement” and “Appreciates” are used awkwardly or incorrectly.
- No last name of sender or signature block present. Many would expect a company signature block to accompany an email discussing a raise.
- Strange email address – generic and not internal. No last name.

In hindsight, it is easy to identify the mistakes the cybercriminal made while drafting this email.

In real time, you may be quickly scanning email to get through the 100 unopened or could be fueled by the excitement of a raise and click open the email quicker than you can think about cybersecurity and prevention of a cyber attack.

If every user in your company treats every email as a cyberthreat, nearly 100% of cyberattacks can be avoided.

Many staff feel pressure to root through their inbox as quickly as possible because checking email does not seem like a “productive task”. There are no metrics taken on how much time is spent checking emails.

“If every user in your company treats every email as a cyberthreat, nearly 100% of cyberattacks can be avoided.”




If you come across a suspicious email, don't open it, and call us right away (630) 406-8969

It is important that you, as CEO, relay the importance of checking email carefully because one mistake, one email, one click can cause serious, possibly unrecoverable harm to your business.

What would happen if one of your staff opened a phishing email and the company's data was held for ransom? Surely the employee would need to be terminated due to liability and they would be out of a living. But what is the root cause? Whose fault is it *really*? By not providing training, tools and time to safely check email, it seems management would be at fault.

Tomorrow, take 15 seconds per email to use good cyber judgement. (Go ahead, run a stopwatch for 15 seconds to feel how long that actually is.)

Then, as you go to open each email, check the sender, subject line, sender email address for red flags. If you see anything suspicious, contact your IT department.

Data-Link works with  PII Protect for introductory and on-going phishing email training and simulations available to everyone in your company. Call for info!

Free Report: What Every Business Owner Must Know About Protecting And Preserving Their Company's Critical Data And Computer Systems



This report will outline in plain, nontechnical English the common mistakes that many small-business owners make with their computer networks that cost them thousands in lost sales, productivity and computer repair bills, and will provide an easy, proven way to reduce or completely eliminate the financial expense and frustration caused by these oversights. Go To: [Datalinkmsp.com/Protect](https://datalinkmsp.com/Protect)

“YOUR AD HERE!” Client Spotlight

*This space reserved for a
monthly Client Spotlight!*

Data-Link’s clients are invited to draft a profile/advertisement for their company and we’ll feature it in this space!

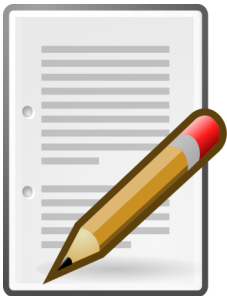
Our DataGrams newsletter reaches 200+ CEOs and C-Suite executives of manufacturers and medical practices every month who trust Data-Link Associates to manage their cybersecurity, managed services and business continuity.

Do you have a product or a service you would like this group to know about?

The profile/advertisement should include a brief history of your company, standard information about your company/product/service, contact information and a blurb about your experience with Data-Link as your IT provider.

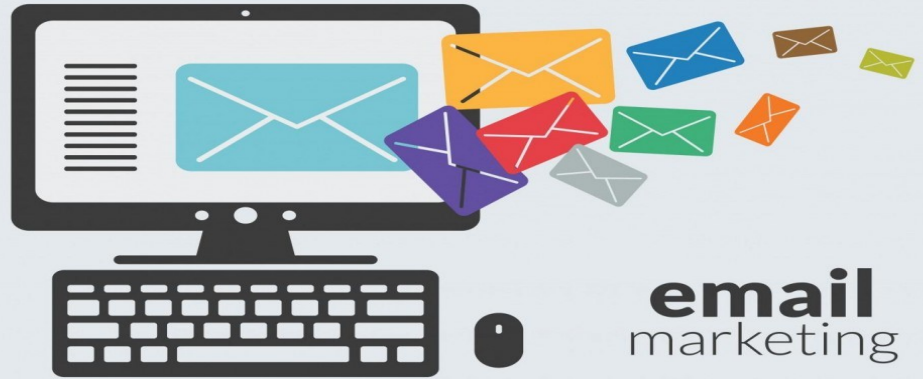
Data-Link reserves the right to edit for grammar, content-type and space. Any recommended changes will be discussed with the client prior to final edits and printing.

**Email entries to Pam at
pbirchfield@datalinkmsp.com**



Entries should be 200 words maximum.

There is no deadline for entries, this offer is ongoing.



**email
marketing**

Are your marketing emails landing in spam and junk folders more than ever before? Email filters became highly restrictive toward the end of 2019 with the Office 365 rollout and again in 2020 during the covid shutdown due to pandemic scams and increased phishing attempts when workforces began working from home on insecure computers and networks. The new rules began to filter even legitimate email traffic .

Did you know? You have about 70% control over whether or not your email lands safely in an inbox – but those are still good enough odds to make email marketing worth your time and effort.

A good response to an email marketing campaign is 10% and costs next to nothing to create and send out as many emails as your heart desires. The ROI is fantastic but it takes know-how and practice to properly implement a good email campaign. (See August 2022 DataGrams for *Designing a Fool-Proof Email Campaign*)

How can you ensure your email marketing lands safely in your recipient’s inbox? Be sure to follow the “ARC of Deliverability”:

Authentication: Are you who you say you are? For example, are you sending an email with PayPal logos and verbiage but you are not PayPal?

Reputation: Is your email address from a proper website domain with security certificates etc...? Has your IP address received too many complaints in the past?

Content: Does your content look “spammy” to the filters? All capital letters, too many repeated words and use of spam phrases will all get caught up in the spam filters.

Most of us are not in the business of spamming, or sending mass email to unsuspecting people who are not leads and have never raised their hand to say “I’m interested”.

Obviously “\$\$\$” and “Meet Singles” are known spam phrases, but I have a list of spam words/phrases that may surprise you: (case-sensitive) Profits, Price, Quote, US dollars, Make money, Work from home, Mortgage rates, beneficiary, FRIENDS, BUY, No credit check, Full refund, Consolidate debt and credit, No age restrictions, Performance, Open, Web traffic, Billion dollars, 100% FREE, 100% SATISFIED, Per day, CALL, The best rates, Prizes, Only, Check, Income.

Other factors come into play but the best way to ensure your email pass through the spam filters is to always have permission to email. There are many ways to legitimately collect email addresses including: via a webform for a free offer or download on your website, an application, a trade show contact form or simply by asking for it.

Be sure to have an OPT OUT/ UNSUBSCRIBE link on all marketing email communications. It’s the law.

■ Mobike's Customer ID Info Made Public Through Error In Granting Permissions on AWS Bucket

In February, a security researcher came across an unsecured Amazon-hosted storage bucket that appeared to belong to Mobike, a once promising bike sharing company in China.

In attempt to secure the data, the researcher requested help from a well-respected online tech newspaper, TechCrunch.

TechCrunch reached out to a spokesperson of a company that previously owned Mobike who said they were no longer involved in Mobike since they sold it.

It seemed no one wanted to take responsibility for the 120,000 documents identifying Mobike users contained in the bucket—a number that was growing by the day.

When accessed in May, it appeared the Mobike data storage bucket had been secured. It is not known how long the bucket was public, but Amazon's default is private, so someone with administrative privileges to the bucket must have corrected the permissions.

We would like to assume this permissions mishap was an oversight but you never know what a rogue employee is capable of. Instead of trying to handle your company's data storage and security yourself, it's best to leave it to the professional like us.

■ How to Pick The Juiciest, Sweetest Watermelon

Southern Living magazine uncovers the 5,000 year old mystery — yes, that's how long our ancestors have been enjoying watermelon, since 3000 BC — just in time for you to pick the best tasting watermelons for your gatherings this summer!

Attributes to look for:

- If it has a bit of stem, choose one that is more brown than crisp green.
- Patch of yellow on the underside
- Brownish/Black spots known as "sugar spots"
- Dull rind
- A light thump on the bottom sounds hollow

Avoid:

- Green stem
- White patch on the underside
- **Black and white specks (mold)**
- Shiny rind

- A light thump on the bottom sounds dull
- Rind feels soft
- Cuts or soft spots

We don't do this here in the Midwest, but anyone who hails from the South knows that watermelon is best served with salt! Salt balances the bitter, sour and sweet flavors of the melon and makes the watermelon taste juicier by activating the salivary glands (think salt on steak). And you can leave the Gatorade in the fridge because the salt replenishes electrolytes and hydrates which is great for those weekend-long summer barbecues spent under the hot sun.

In Latin America, watermelon is sprinkled with savory chili powder and lime.

So now that you have some good tips on finding the perfect watermelon, remember the best treat of the summer is spending time with family and friends. Enjoy!

■ The 10 Most Common Passwords Discovered In Data Breaches, according to NordPass

NordPass, a password manager and generator, reports the Top 10 worst passwords you can use. (ranked)

- #1. 123456
- #2 123456789
- #3 12345 *
- #4 qwerty
- #5 password
- #6 12345678
- #7 111111
- #8 123123
- #9 1234567890
- #10 1234567

It is no coincidence these passwords are found in data breaches. People who do not take cyber security seriously are destined to suffer a breach. It was funny in the movie, *Spaceballs* *, but using any of these passwords in a real life situation shows a dangerous complacency toward network security.



"Is that computer, down there, the one you were having problems with?"