ANTISYPHON TRAINING
POWERED BY BHIS

SOC SUMMIT TALKS

STATIC EMAIL ANALYSIS

March 25, 2026 | 12:00 pm ET

CHED WIGGINS

disclaimer

Nothing in the following presentation represents my employer.

Any technical mistakes or misstatements in this presentation are attributed to me alone.

prepare yourself for adventure!

https://en.wikipedia.org/wiki/It%27s_dangerous_to_go_alone!

whoami

LOUISIANA TECH UNIVERSITY

COLLEGE OF ENGINEERING & SCIENCE

NAVAL NUCLEAR POWER — NNPTC — KNOWLEDGE • INTEGRITY EXCELLENCE — TRAINING COMMAND

CyberNow Labs

A NATIONAL CYBER GROUP COMPANY

2005	2006	2010	2011	2012	2020	2022	2023
B.S. Comp. Sci.	Navy Nuke School	USN Officer	LPD Deployment	Help Desk	Help Desk	Security Analyst Intern	SOC Lead

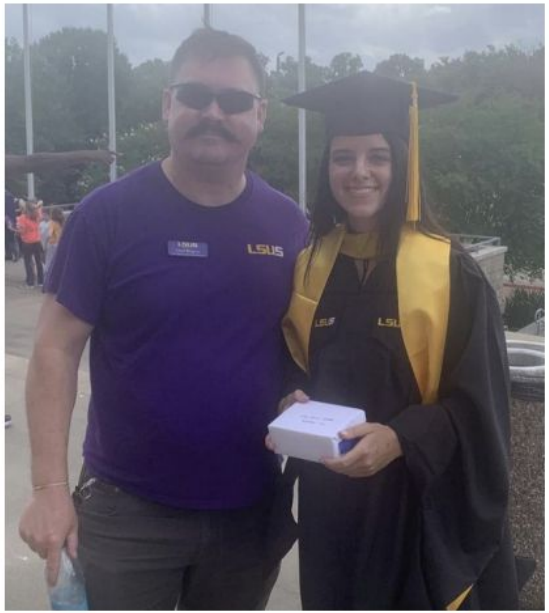
whoarethey

Senior computer science student Keya [redacted] is one of six LSUS student analysts that protect the university's network in the Security Operations Center. [redacted] is interested in a career in governance and regulatory compliance. Student analysts gain valuable cybersecurity experience in an industry in which entry-level positions are rare. CREDIT: LSUS Media Relations

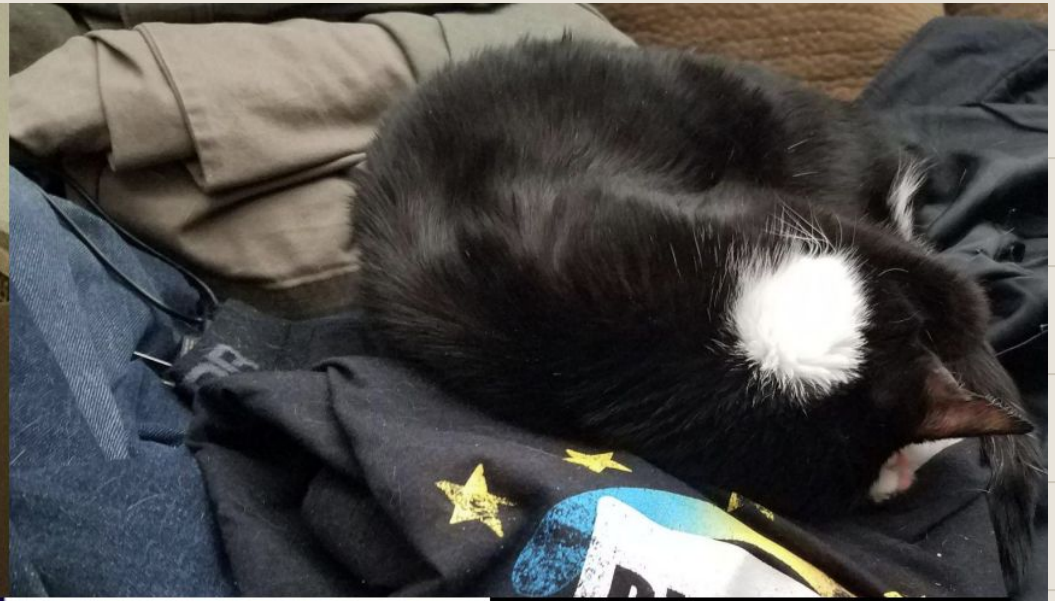
News

LSUS students developing essential cybersecurity skills protecting University's network

Senior computer science student [redacted] is one of six LSUS student analysts that protect the university's network in the Security Operations Center. Student analysts gain valuable cybersecurity experience in an industry in which entry-level positions are rare.



whoarethey



PRE-CON TRAINING FEB. 4-5, 2025

WILD WEST HACKIN FEST @Mile High

CONFERENCE FEB. 5-7, 2025

Try Hack Me

MetaCTF

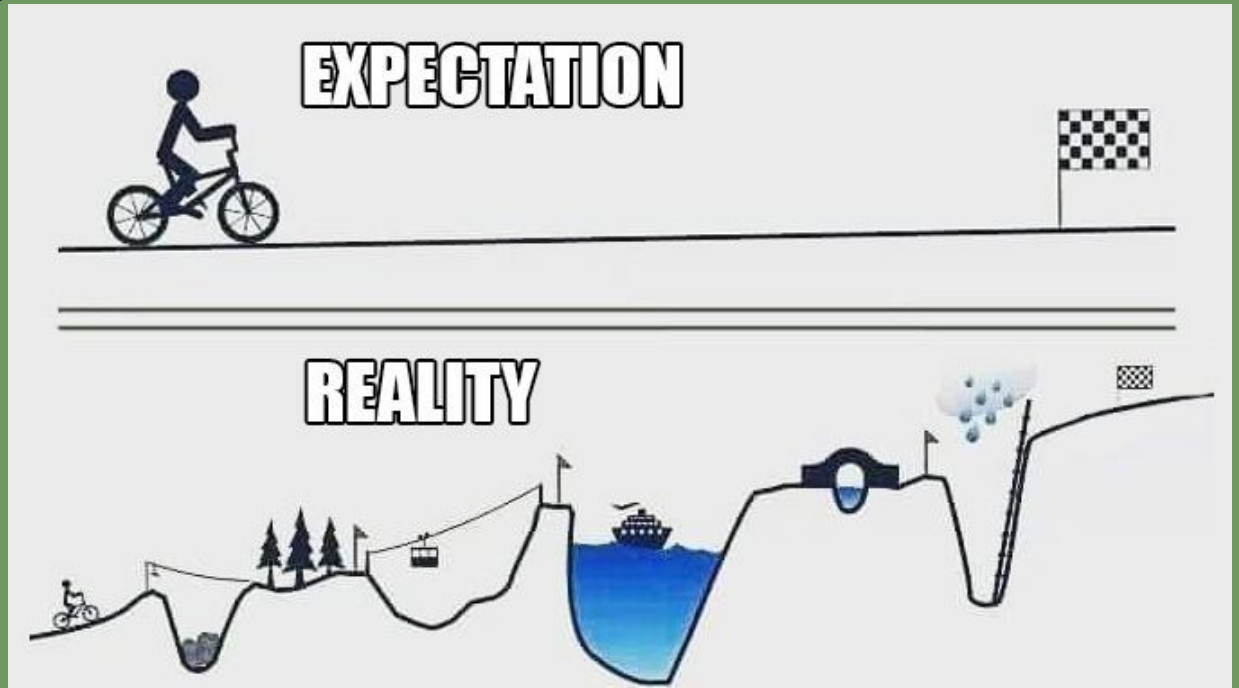
BLACK HILLS Information Security

agenda

0x00 = expectation management
0x01 = why do we still use email?
0x02 = business risk and email
0x03 = analyzing samples 👾
0x04 = email attack/defense future
0x05 = wrap up
0x06 = Q&A (time permitting)

https://heelsdownmag.com/managing-expectations-the-highs-and-lows-of-horses/

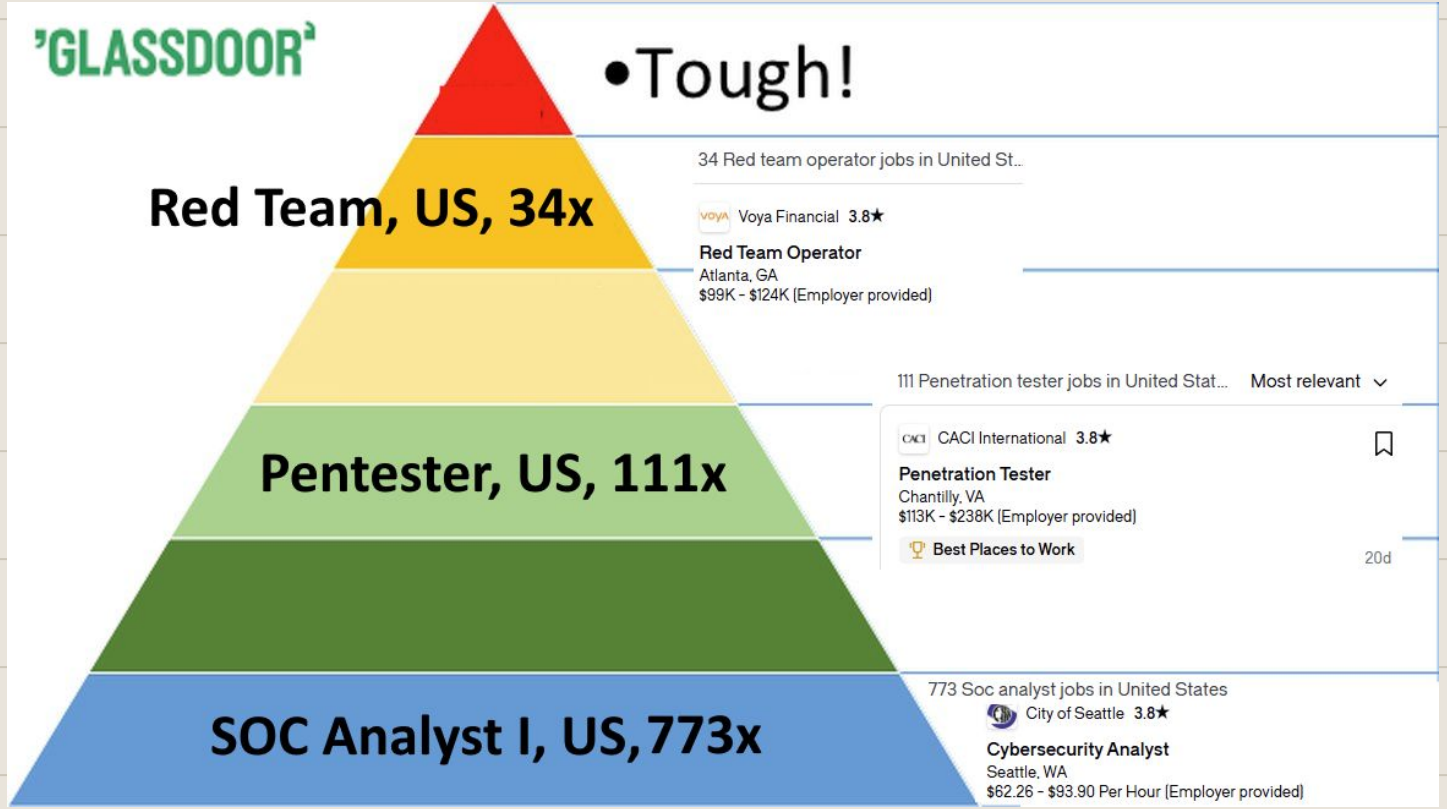
0x00 = expectation management



boring

Email is a rather dry topic, but we must **endure** to fortify our client, the SMB, against email as an Initial Access vector.
(you may discover that some roles & skills in infosec are not as glamorous as exploit dev but are nevertheless important to operations)

boring... ...can be good! ...can get you paid



Thank you AttackIQ for the original image.

0x01 = why do we still use email?

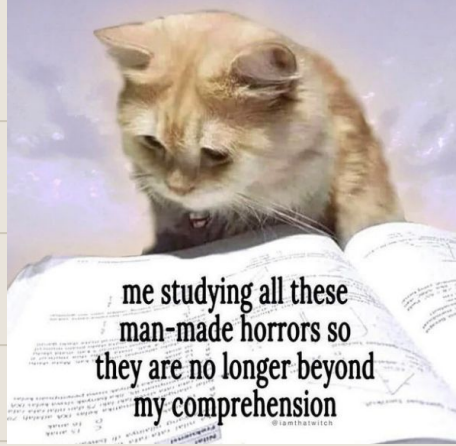
https://nationalcioreview.com/articles-insights/leadership/weve-always-done-it-this-way/

why? because...

"According to the Project Management Institute (PMI) Pulse of the Profession® (2013a) **poor communication** is the leading reason for project failure, citing poor communications as a **contributing factor in 56%** of the projects that failed."

https://www.pmi.org/learning/library/communication-method-content-in-project-9937

0x01 a brief history noone's favorite tool (pt. 1)



ARPANET

1960s — MIT

Electronic messaging begins with Compatible Time-Sharing System (CTSS)

1969

1971 — BBN

Ray Tomlinson sent first email across ARPANET using name@host

70s & 80s — ARPANET

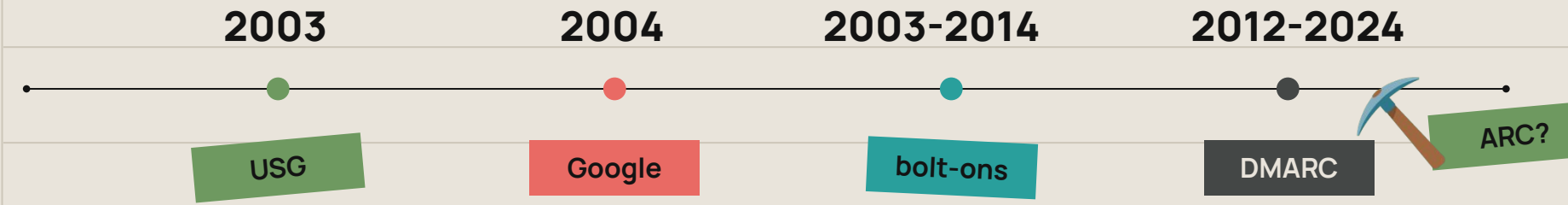
university, gov agency, and defense contractor adoption. 1987 "Cuckoo's Egg"

1990s — Home LAN

Free services Hotmail & Yahoo, and paid service AOL bring widespread email use to many homes

can we go back somehow?

0x01 a brief history noone's favorite tool (pt. 2)



Congress passed the "CAN-SPAM" act.

clearly ineffective! 🧀

Google launches the free "GMail" service, you needed a code from a friend (I got one)

Sender Policy Framework, b.2003, gets RFC 7208 in 2014. DomainKeys Identified Mail gets RFC 6376 in 2011.

Domain-based Message Authentication, Reporting, and Conformance, RFC 7489, adoption grows 2010s-2024.

0x02 = business risk and email

https://www.flickr.com/photos/65367656@N08/5964832054

Anecdotes

CISO at Georgetown: “50% of my SOC Analyst’s time is spent on emails.”

Colleague at TekStream Solutions: “Yes, I also spent 50% of my SOC time on email, so I would say that is accurate.”

CIS Controls

CIS Control 9 - Email and Web Browser Protections

- [x] Safeguard 9.1: Ensure Use of Only Fully Supported Browsers and Email Clients
- [x] Safeguard 9.2: Use DNS Filtering Services
- [x] Safeguard 9.3: Maintain and Enforce Network-Based URL Filters
- [x] Safeguard 9.4: Restrict Unnecessary or Unauthorized Browser and Email Client Extensions
- [x] Safeguard 9.5: Implement DMARC
- [x] Safeguard 9.6: Block Unnecessary File Types
- [x] Safeguard 9.7: Deploy and Maintain Email Server Anti-Malware Protections

Story Time

THE GEORGETOWN ENVIRONMENTAL
LAW REVIEW

Cybersecurity Policy Responses to the Colonial Pipeline Ransomware Attack

March 7, 2023 | *by Kimberly Wood*

The Colonial Pipeline transports refined oil products to the East Coast.

https://www.law.georgetown.edu/environmental-law-review/blog/cybersecurity-policy-responses-to-the-colonial-pipeline-ransomware-attack/

Impact

What is the potential **business impact** to even one compromised business email account?
Hint: it's the beginning of the Cyber Kill Chain.

0x03 = analyzing samples 👾

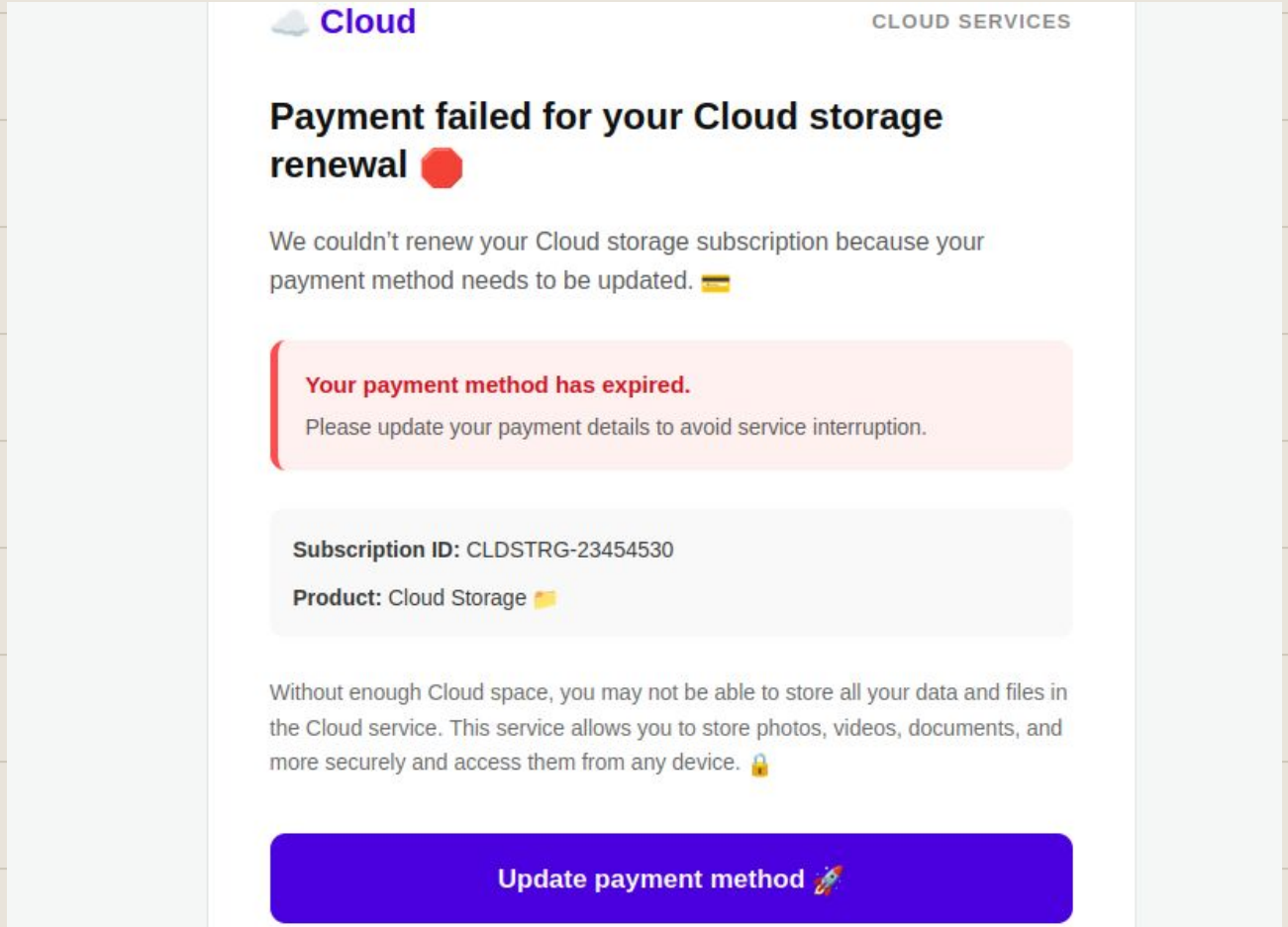
https://9gag.com/gag/aW1nwz2

Scenario 1

Situation: a local business owner reached out to us, due to our reputation as the discoverable “good at computers” person, to assist with email troubles.

“My assistant is getting these annoying emails constantly!”

Scenario 1



☁️ Cloud

CLOUD SERVICES

Payment failed for your Cloud storage renewal 🛑

We couldn't renew your Cloud storage subscription because your payment method needs to be updated. 💳

Your payment method has expired.

Please update your payment details to avoid service interruption.

Subscription ID: CLDSTRG-23454530

Product: Cloud Storage 📁

Without enough Cloud space, you may not be able to store all your data and files in the Cloud service. This service allows you to store photos, videos, documents, and more securely and access them from any device. 🔒

Update payment method 🚀

Who (what) sent this? Why?

Scenario 1

Determination

At this point, I have enough indicators to consider the email suspicious at a minimum. Then we can delete it or perform other mitigations.

Let’s gather more information. For science.

URL analysis

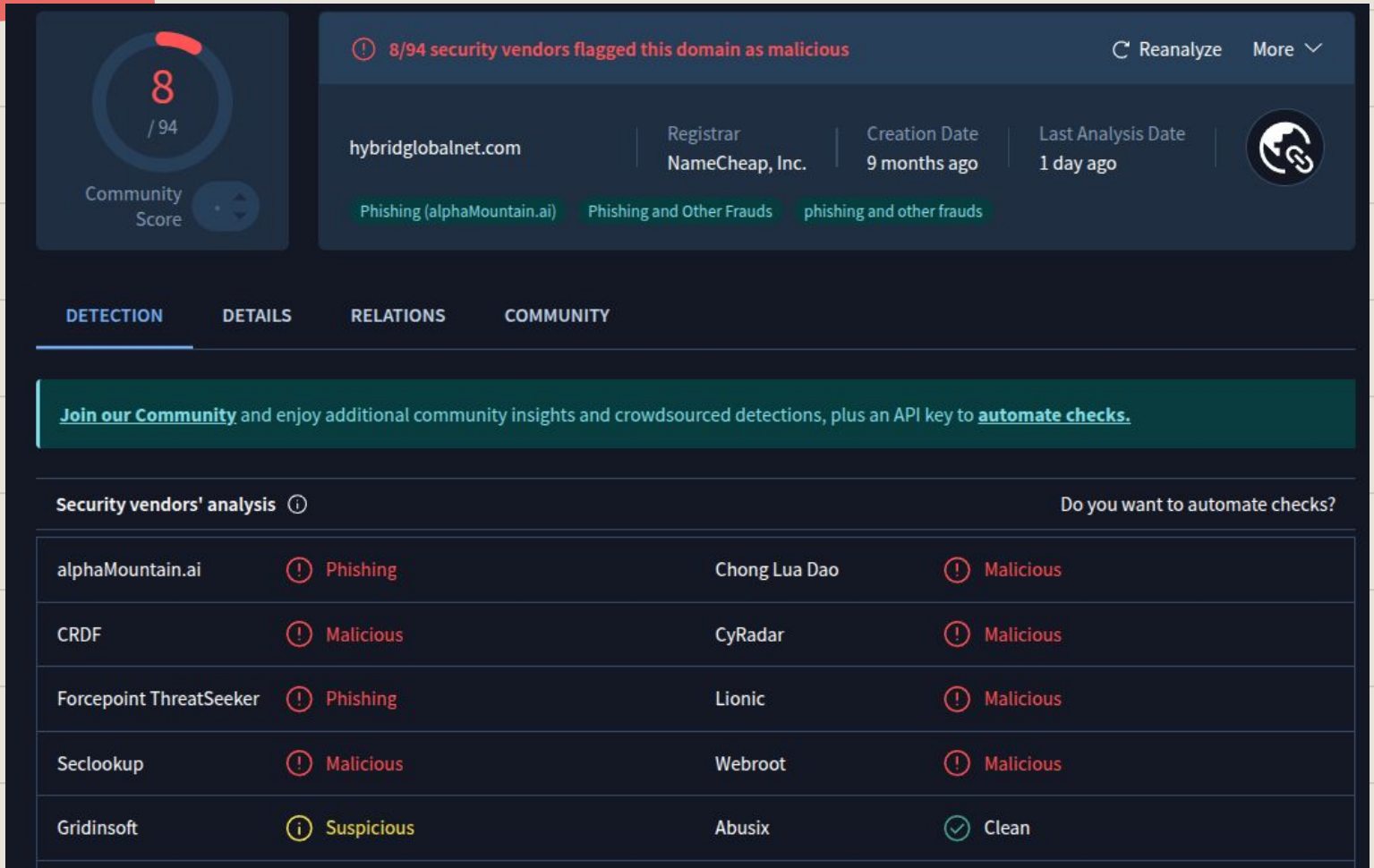
Question: what does the button in the email do? It probably has a URL behind it...

Behind the button:

hxxps[://]storage[.]googleapis[.]com/strow/strw_v2.html#?act=cl&pid=16740_md&uid=4&vid=444648&ofid=387&lid=338&cid=850574

URL analysis

use your tools to dig⛏️



other tools

https://www.abuseipdb.com/
https://urlscan.io/
https://hybrid-analysis.com/

dig safely

The goal is to conduct an investigation to gather evidence and make a determination safely:

- Use a different web browser.
- Use a virtual machine.
- Use third party tools.
- Use a sandbox, like Any Run.

further digging ideas⛏️

Analysis

header analysis:

- Sender (what is shown by default)
- From vs Return-to comparison
- SPF, DKIM, DMARC, ARC
- domain analysis: age, reputation,etc
- email message body (lures, URLs)
- attachments, other indicators

Who (what) sent this? Why?

Scenario 2

Situation: a local SMB owner reached out to us stating they believe some money was tricked out of them. Their lawyer asked for evidence. We must find it.

“Please help us get our money back!”

Scenario 2

We recently spotted activity on your PayPal account that may not be yours. If this isn't recognized, please contact us by phone. Otherwise, $1025.44 will be charged today.

Your request is already under processing. Reach out for any queries.

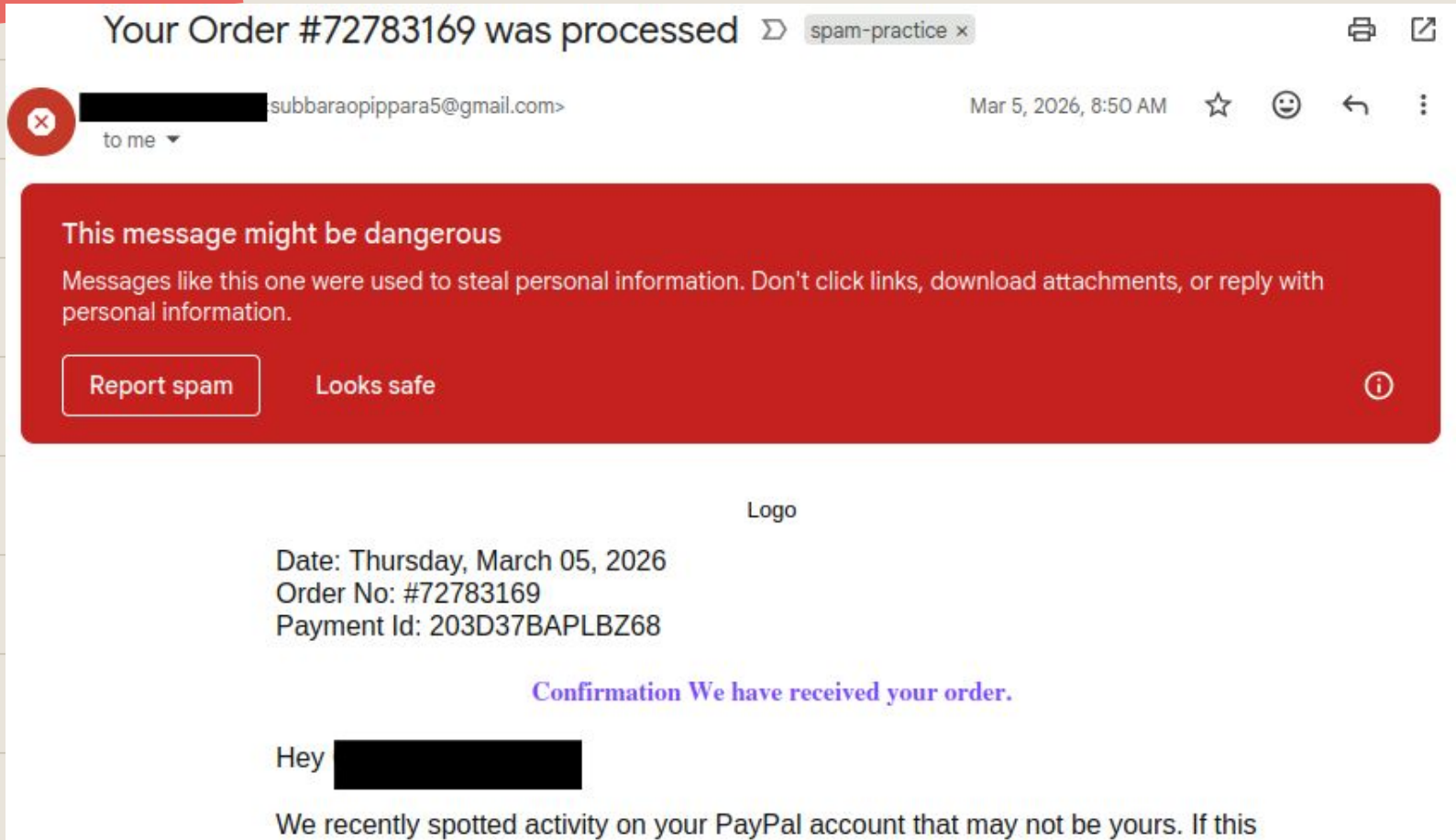
Order Summary
Purchase: Doge
Quantity: 0002065
Wallet Address: 5cf281e6-52e4-4d13-b499-b3195e8f06a6
Amount: $1025.44

Order concerns?
Call to raise an immediate complaint.

PayPal actively prevents scam-related emails. Please avoid replying here and use the provided number.

Warmest regards
PayPal Business
+1 (828) 259-2373
+1 (803) 223-8429

Scenario 2



Your Order #72783169 was processed spam-practice ×

[redacted]subbaraopippara5@gmail.com> Mar 5, 2026, 8:50 AM

to me

This message might be dangerous

Messages like this one were used to steal personal information. Don't click links, download attachments, or reply with personal information.

Report spam Looks safe

Logo

Date: Thursday, March 05, 2026
Order No: #72783169
Payment Id: 203D37BAPLBZ68

Confirmation We have received your order.

Hey [redacted]

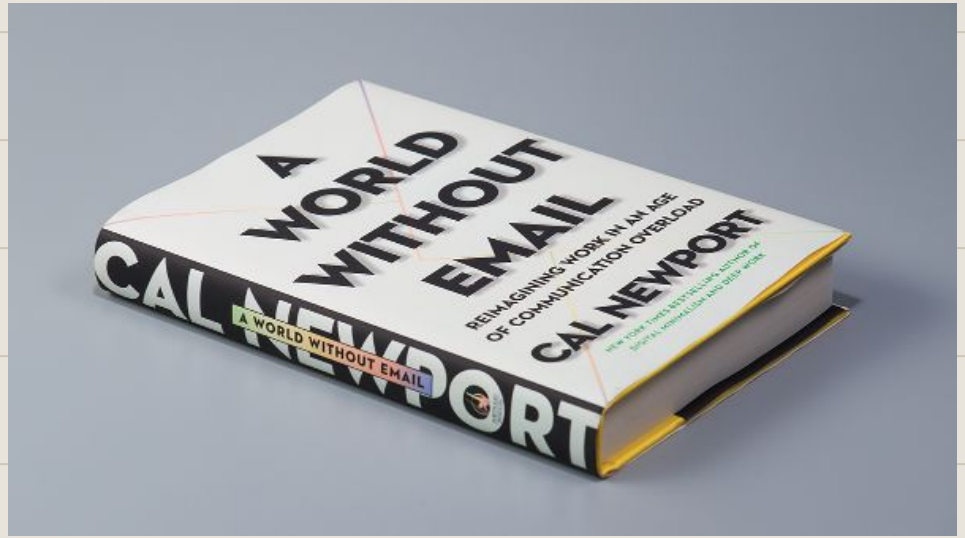
We recently spotted activity on your PayPal account that may not be yours. If this

Scenario 2

Message ID	<69a99829.630a0220.23703a.3378@mx.google.com>
Created at:	Thu, Mar 5, 2026 at 8:50 AM (Delivered after 2 seconds)
From:	[redacted]subbaraopippara5@gmail.com>
To:	[redacted]gmail.com>
Subject:	Your Order #72783169 was processed
SPF:	PASS with IP 209.85.220.41 Learn more
DKIM:	'PASS' with domain gmail.com Learn more
DMARC:	'PASS' Learn more

0x04 = the future of email attack & defense

the future of email is no email at all?



Images: Chronicle of Higher Education,
https://www.chronicle.com/article/is-ai-making-us-stupid-cal-newport-is-worried
Brent Fuchs. Images in this presentation adhere to Fair Use and are transformative.

Lunch is near, and this is deliberate torment.

0x05 = wrap up

https://www.brakebush.com/recipes/thai-chicken-tender-wrap/

wrap up

Business Risk Analysis: email will persist into the near future due to its familiarity. It will remain a **favored Initial Access vector** used by a panoply of Threat Actors to surveil, steal from, degrade, or even destroy your Small to Medium Business.
Action: implement controls now.

0x06 = Q&A

0x07 = secret slides of Resources, References, and future ~~schemes~~ plans

refs

This is not intended to be presented, rather to be referenced.

https://attack.mitre.org
https://www.microsoft.com/en-us/security/business/security-101/what-is-business-email-compromise-bec
https://imgflip.com/