# 10 Cybersecurity Practices

Keeping Special Districts safe in the age of AI threats.

Tom Bragg thomas@getstreamline.com

STREAMLINE

SAFE-D
Texas State Association of
Fire and Emergency Districts

# How We Got Here

## *Cybersecurity & Districts Today*

# OLDSMAR FL

Source: © Suzanne Tennant. | GAO-18-102

February 2021:

**100 PPM => 11,100 PPM of Lye**

# Cyber Insurance is becoming harder to get

- The average price rose by ? % in the second quarter of 2022 alone[1]
- Reduction of cyber coverage from $5M to ?
- Nearly ? % of all attacks are against organizations of 250 employees or less[2]
- Enhanced security measures are now required by organizations to get coverage (training, scanning, MFA)

https://biztechmagazine.com/article/2023/03/what-small-businesses-need-know-about-cyber-insurance
https://www.insurancebusinessmag.com/us/news/cyber/cyber-insurers-hiking-premiums-lowering-coverage-limits--report-312738.aspx

# Cyber Insurance is becoming harder to get

- The average price rose by 79% in the second quarter of 2022 alone[1]
- Reduction of cyber coverage from $5M to $3M or $1M
- Nearly 50% of all attacks are against organizations of 250 employees or less[2]
- Enhanced security measures are now required by organizations to get coverage (training, scanning, MFA)

https://biztechmagazine.com/article/2023/03/what-small-businesses-need-know-about-cyber-insurance
https://www.insurancebusinessmag.com/us/news/cyber/cyber-insurers-hiking-premiums-lowering-coverage-limits--report-312738.aspx

# What's at stake?

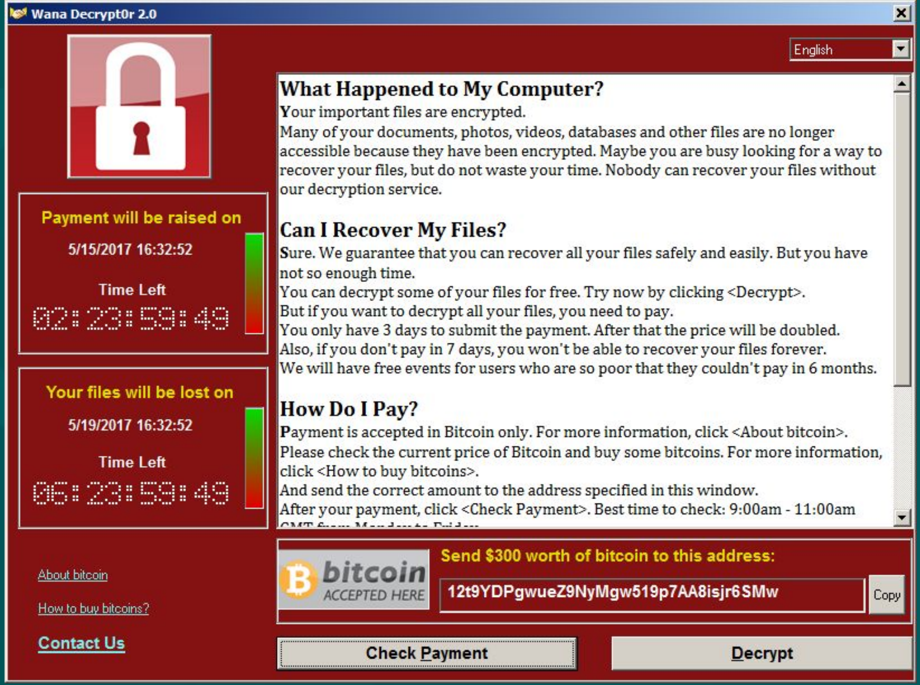
- Physical safety of community infrastructure
- Destruction of data
- Stolen money
- Lost productivity
- Theft of intellectual property
- Theft of personal and financial data
- Embezzlement

- Fraud
- Post-attack disruption to the normal course of business
- Forensic investigation
- Restoration and deletion of hacked data and systems
- Reputational harm

https://cybersecurityventures.com/hackerpocalypse-cybercrime-report/

# Ransomware

- Designed to block access to a computer system or encrypt its data until a ransom is paid
- Average 2023 payment = $1,542,333 (up from $812,380 in 2022)[1]
- 69% of state and local governments reporting ransomware incidents[2]



Payment will be raised on
5/15/2017 16:32:52
Time Left
02:23:59:49

Your files will be lost on
5/19/2017 16:32:52
Time Left
06:23:59:49

**What Happened to My Computer?**

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

**Can I Recover My Files?**

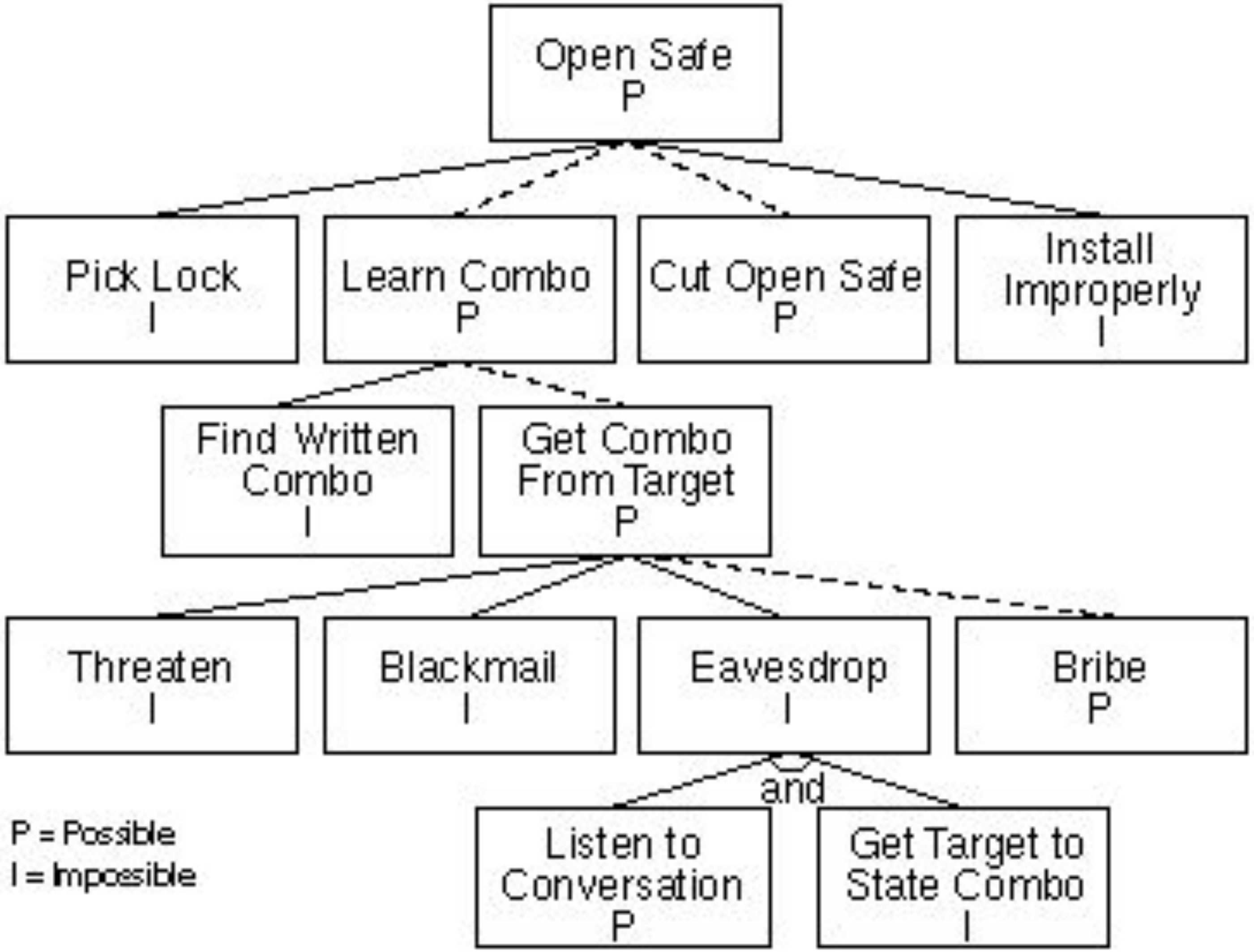
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

**How Do I Pay?**

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

https://www.cloudwards.net/ransomware-statistics/
https://news.sophos.com/en-us/2023/08/01/the-state-of-ransomware-in-state-and-local-government-2023/


Open Safe P

Pick Lock I

Learn Combo P

Cut Open Safe P

Install Improperly I

Find Written Combo I

Get Combo From Target P

Threaten I

Blackmail I

Eavesdrop I

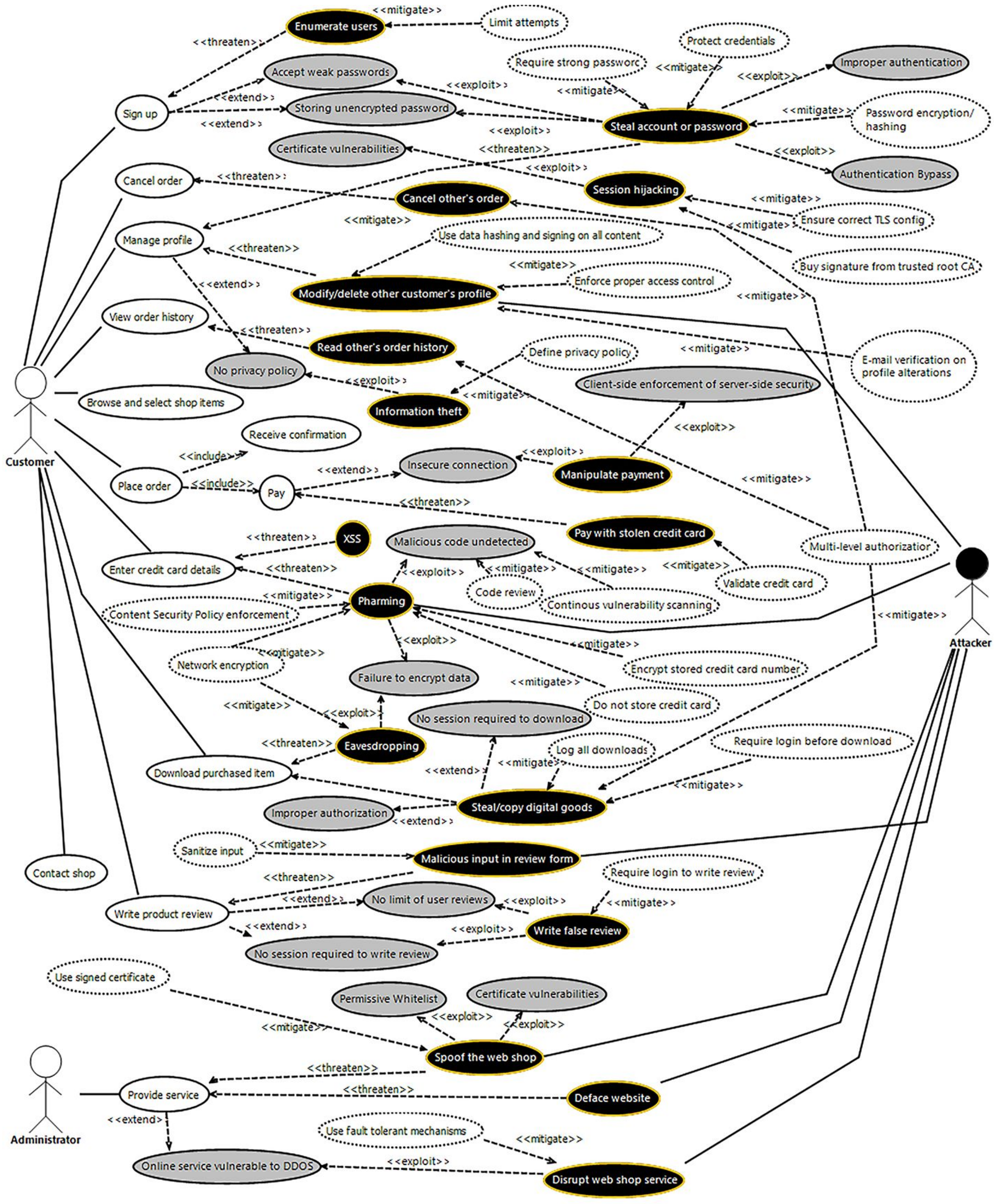
Bribe P

and

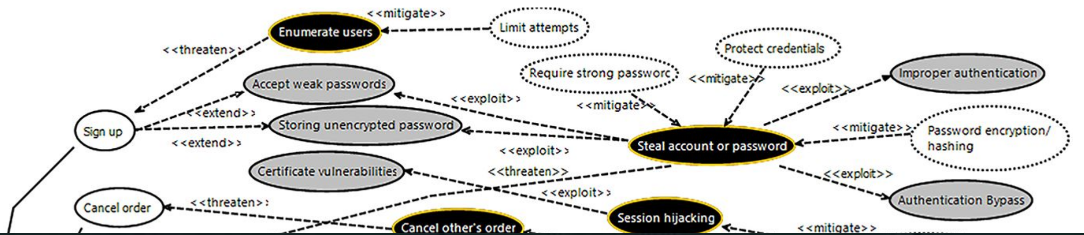
Listen to Conversation P

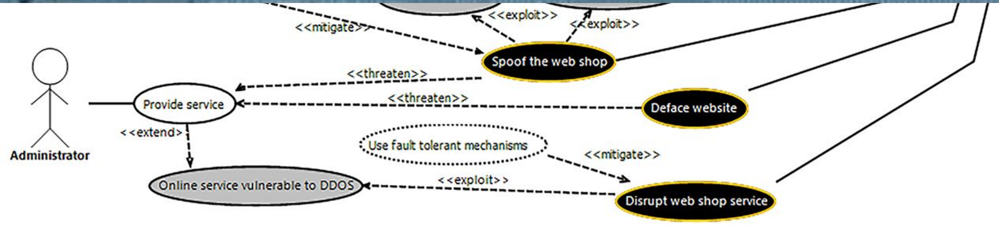
Get Target to State Combo I

P = Possible
I = Impossible



Customer
Attacker
Administrator
Sign up
Cancel order
Manage profile
View order history
Browse and select shop items
Receive confirmation
Place order
Pay
Enter credit card details
Download purchased item
Contact shop
Write product review
Provide service
Enumerate users
Limit attempts
Accept weak passwords
Storing unencrypted password
Require strong password
Protect credentials
Improper authentication
Steal account or password
Password encryption/ hashing
Certificate vulnerabilities
Authentication Bypass
Session hijacking
Cancel other's order
Ensure correct TLS config
Buy signature from trusted root CA
Use data hashing and signing on all content
Enforce proper access control
Modify/delete other customer's profile
E-mail verification on profile alterations
Read other's order history
No privacy policy
Define privacy policy
Information theft
Client-side enforcement of server-side security
Insecure connection
Manipulate payment
Pay with stolen credit card
Multi-level authorization
XSS
Malicious code undetected
Validate credit card
Code review
Continous vulnerability scanning
Pharming
Content Security Policy enforcement
Network encryption
Failure to encrypt data
Encrypt stored credit card number
Do not store credit card
No session required to download
Eavesdropping
Log all downloads
Require login before download
Steal/copy digital goods
Improper authorization
Sanitize input
Malicious input in review form
Require login to write review
No limit of user reviews
Write false review
No session required to write review
Use signed certificate
Permissive Whitelist
Certificate vulnerabilities
Spoof the web shop
Deface website
Use fault tolerant mechanisms
Online service vulnerable to DDOS
Disrupt web shop service
<<mitigate>>
<<threaten>>
<<extend>>
<<exploit>>
<<include>>

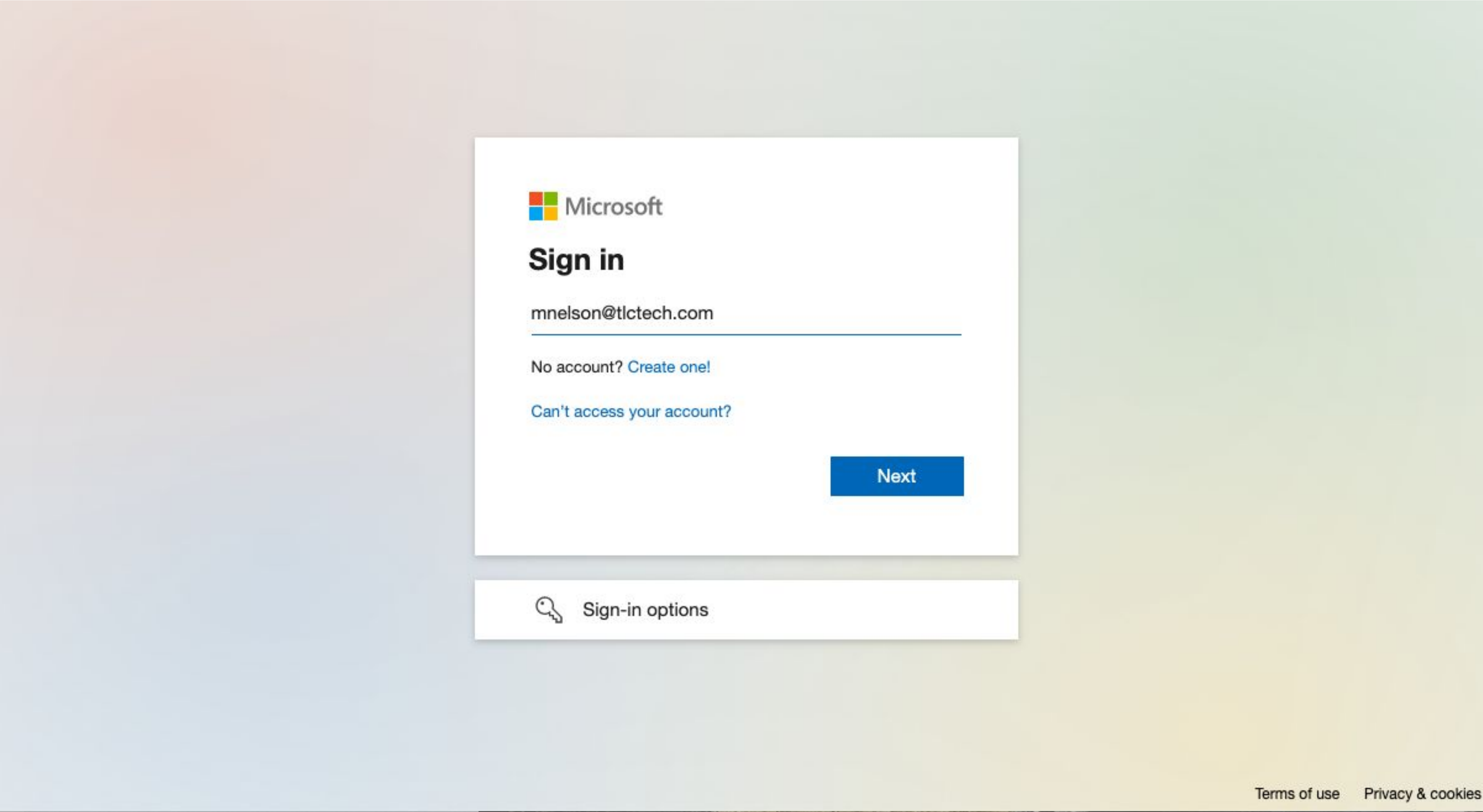

Enumerate users
<<mitigate>>
Limit attempts
<<threaten>>
Protect credentials
Require strong passworc
<<mitigate>>
Accept weak passwords
<<exploit>>
Improper authentication
<<extend>>
<<mitigate>>
Sign up
Storing unencrypted password
<<mitigate>>
Password encryption/
hashing
<<extend>>
Steal account or password
<<exploit>>
Certificate vulnerabilities
<<threaten>>
<<exploit>>
<<exploit>>
Authentication Bypass
Cancel order
<<threaten>>
Cancel other's order
Session hijacking
<<mitigate>>


<<exploit>>
<<mitigate>>
<<exploit>>
Spoof the web shop
<<threaten>>
Provide service
<<threaten>>
Deface website
Administrator
<<extend>
Use fault tolerant mechanisms
<<mitigate>>
Online service vulnerable to DDOS
<<exploit>>
Disrupt web shop service

# Don't worry!

# 1. Enable 2-factor (MFA)

MFA and why you want to enable it on your Office 365 or Google Workspace

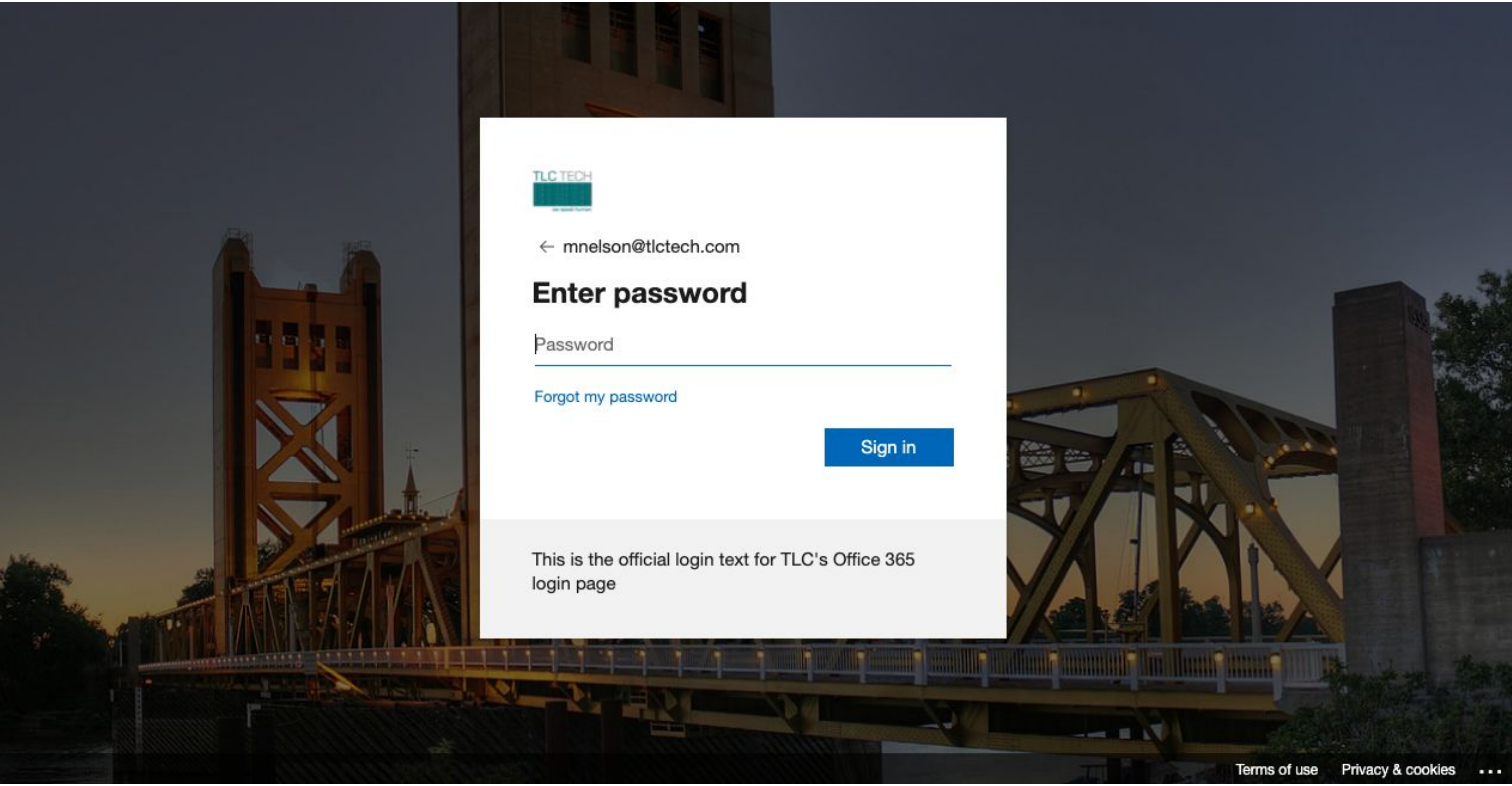


Sign in

mnelson@tlctech.com

No account? Create one!

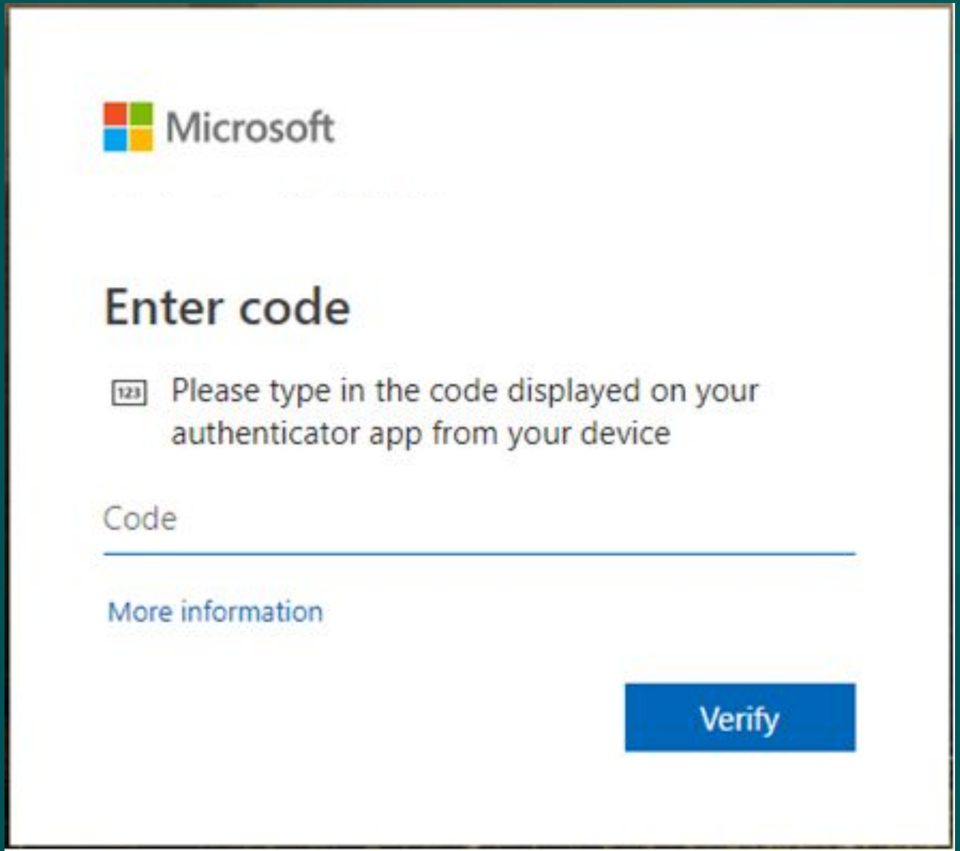
Can't access your account?



← mnelson@tlctech.com

Enter password

This is the official login text for TLC's Office 365 login page



Enter code

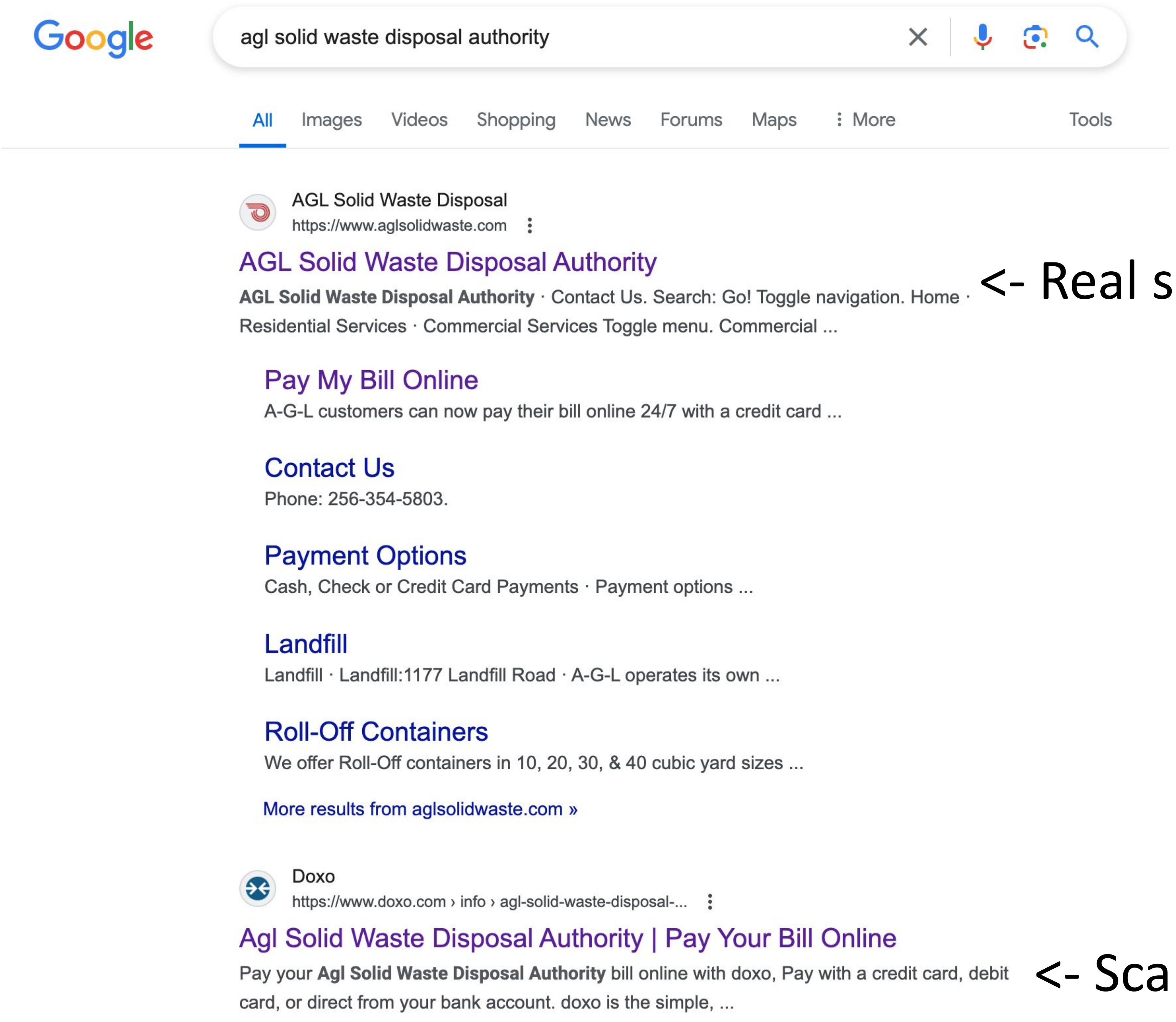
Please type in the code displayed on your authenticator app from your device

# 2. Get a .gov

*What Is it?*

- *Free get.gov*
- *Helps protect against spam*
- *Rank higher in search results*

Get Guide



AGL Solid Waste Disposal
https://www.aglsolidwaste.com

AGL Solid Waste Disposal Authority

**AGL Solid Waste Disposal Authority** · Contact Us. Search: Go! Toggle navigation. Home · Residential Services · Commercial Services Toggle menu. Commercial ...

<- Real site

Pay My Bill Online

A-G-L customers can now pay their bill online 24/7 with a credit card ...

Contact Us

Phone: 256-354-5803.

Payment Options

Cash, Check or Credit Card Payments · Payment options ...

Landfill

Landfill · Landfill:1177 Landfill Road · A-G-L operates its own ...

Roll-Off Containers

We offer Roll-Off containers in 10, 20, 30, & 40 cubic yard sizes ...

More results from aglsolidwaste.com »

Doxo
https://www.doxo.com › info › agl-solid-waste-disposal-...

Agl Solid Waste Disposal Authority | Pay Your Bill Online

Pay your **Agl Solid Waste Disposal Authority** bill online with doxo, Pay with a credit card, debit card, or direct from your bank account. doxo is the simple, ...

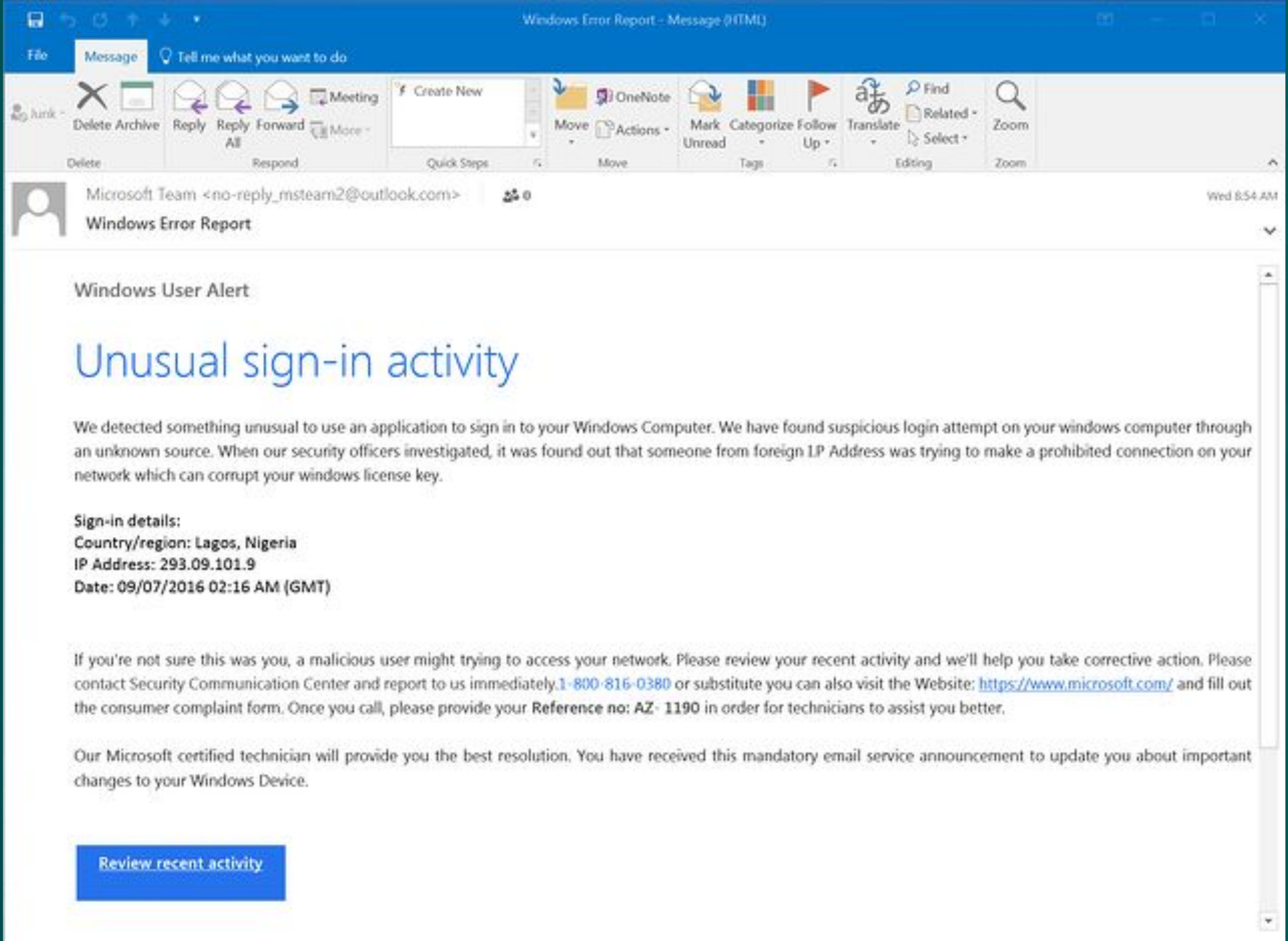
<- Scam site

# 3. Make sure DMARC is enabled to keep others from sending mail as you

D-huh?

*(MXToolbox.com free check)*

# 4. Be ready for Phishing



Microsoft Team <no-reply_msteam2@outlook.com>

Wed 8:54 AM

Windows Error Report

Windows User Alert

## Unusual sign-in activity

We detected something unusual to use an application to sign in to your Windows Computer. We have found suspicious login attempt on your windows computer through an unknown source. When our security officers investigated, it was found out that someone from foreign I.P Address was trying to make a prohibited connection on your network which can corrupt your windows license key.

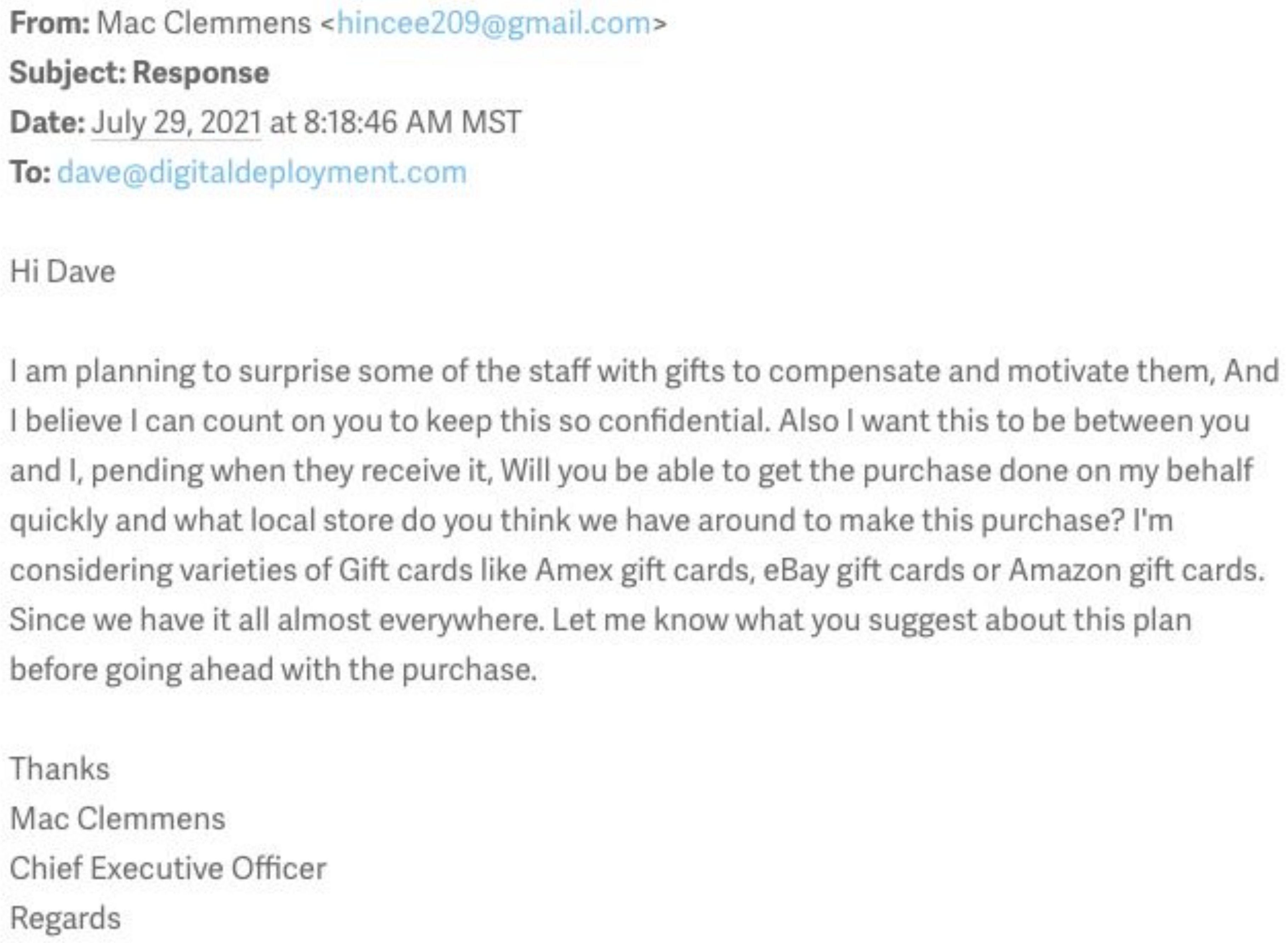
**Sign-in details:**
**Country/region: Lagos, Nigeria**
**IP Address: 293.09.101.9**
**Date: 09/07/2016 02:16 AM (GMT)**

If you're not sure this was you, a malicious user might trying to access your network. Please review your recent activity and we'll help you take corrective action. Please contact Security Communication Center and report to us immediately.1-800-816-0380 or substitute you can also visit the Website: https://www.microsoft.com/ and fill out the consumer complaint form. Once you call, please provide your **Reference no: AZ- 1190** in order for technicians to assist you better.

Our Microsoft certified technician will provide you the best resolution. You have received this mandatory email service announcement to update you about important changes to your Windows Device.

Review recent activity

# Phishing Example



**From:** Mac Clemmens <hincee209@gmail.com>

**Subject: Response**

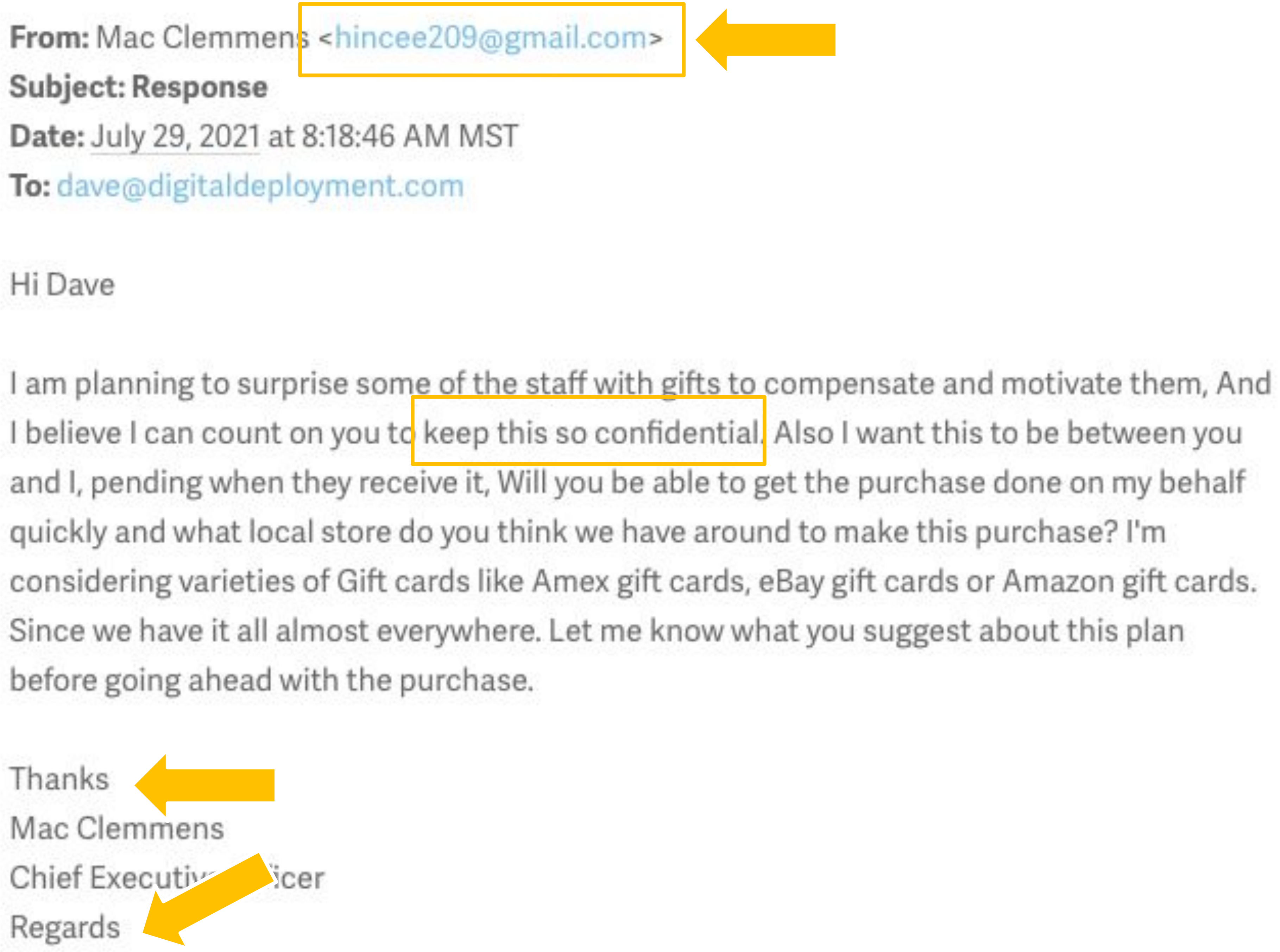
**Date:** July 29, 2021 at 8:18:46 AM MST

**To:** dave@digitaldeployment.com

Hi Dave

I am planning to surprise some of the staff with gifts to compensate and motivate them, And I believe I can count on you to keep this so confidential. Also I want this to be between you and I, pending when they receive it, Will you be able to get the purchase done on my behalf quickly and what local store do you think we have around to make this purchase? I'm considering varieties of Gift cards like Amex gift cards, eBay gift cards or Amazon gift cards. Since we have it all almost everywhere. Let me know what you suggest about this plan before going ahead with the purchase.

Thanks
Mac Clemmens
Chief Executive Officer
Regards



**From:** Mac Clemmens <hincee209@gmail.com>

**Subject: Response**

**Date:** July 29, 2021 at 8:18:46 AM MST

**To:** dave@digitaldeployment.com

Hi Dave

I am planning to surprise some of the staff with gifts to compensate and motivate them, And I believe I can count on you to keep this so confidential. Also I want this to be between you and I, pending when they receive it, Will you be able to get the purchase done on my behalf quickly and what local store do you think we have around to make this purchase? I'm considering varieties of Gift cards like Amex gift cards, eBay gift cards or Amazon gift cards. Since we have it all almost everywhere. Let me know what you suggest about this plan before going ahead with the purchase.

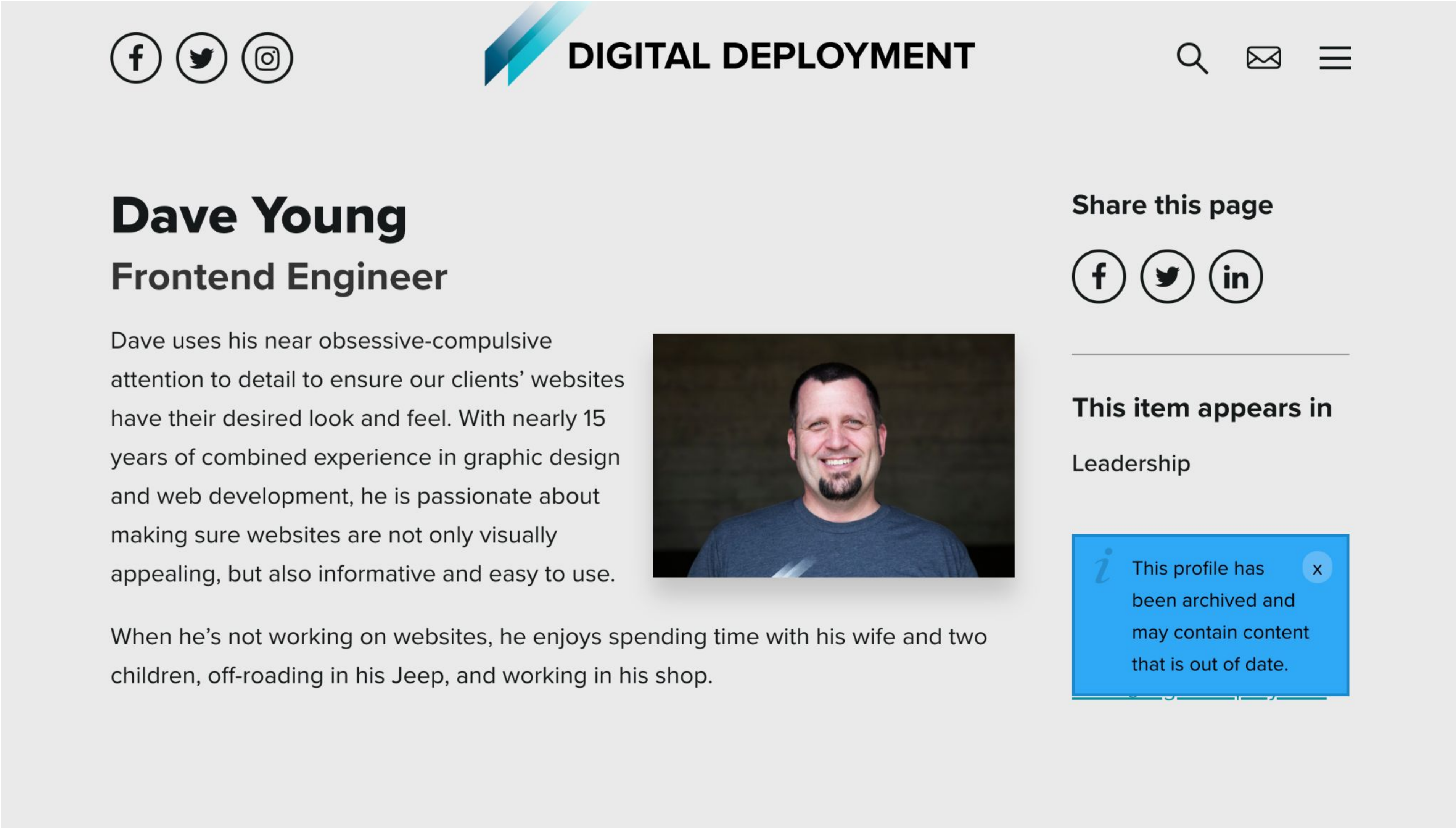
Thanks

Mac Clemmens

Chief Executive Officer

Regards

# AI has made it even worse



# Dave Young

## Frontend Engineer

Dave uses his near obsessive-compulsive attention to detail to ensure our clients' websites have their desired look and feel. With nearly 15 years of combined experience in graphic design and web development, he is passionate about making sure websites are not only visually appealing, but also informative and easy to use.

When he's not working on websites, he enjoys spending time with his wife and two children, off-roading in his Jeep, and working in his shop.

Share this page
This item appears in
Leadership
This profile has been archived and may contain content that is out of date.
x

"Help me rewrite this email to sound like these blog posts written by Mac Clemmens."

"Personalize the message based on information in Dave's biography on the website"

Hey Dave,

Given your exceptional attention to detail, which has always been evident in ensuring our clients' websites look impeccable, I wanted to reach out. With your 15 years of experience, I know you understand the importance of both aesthetic appeal and user-friendliness.

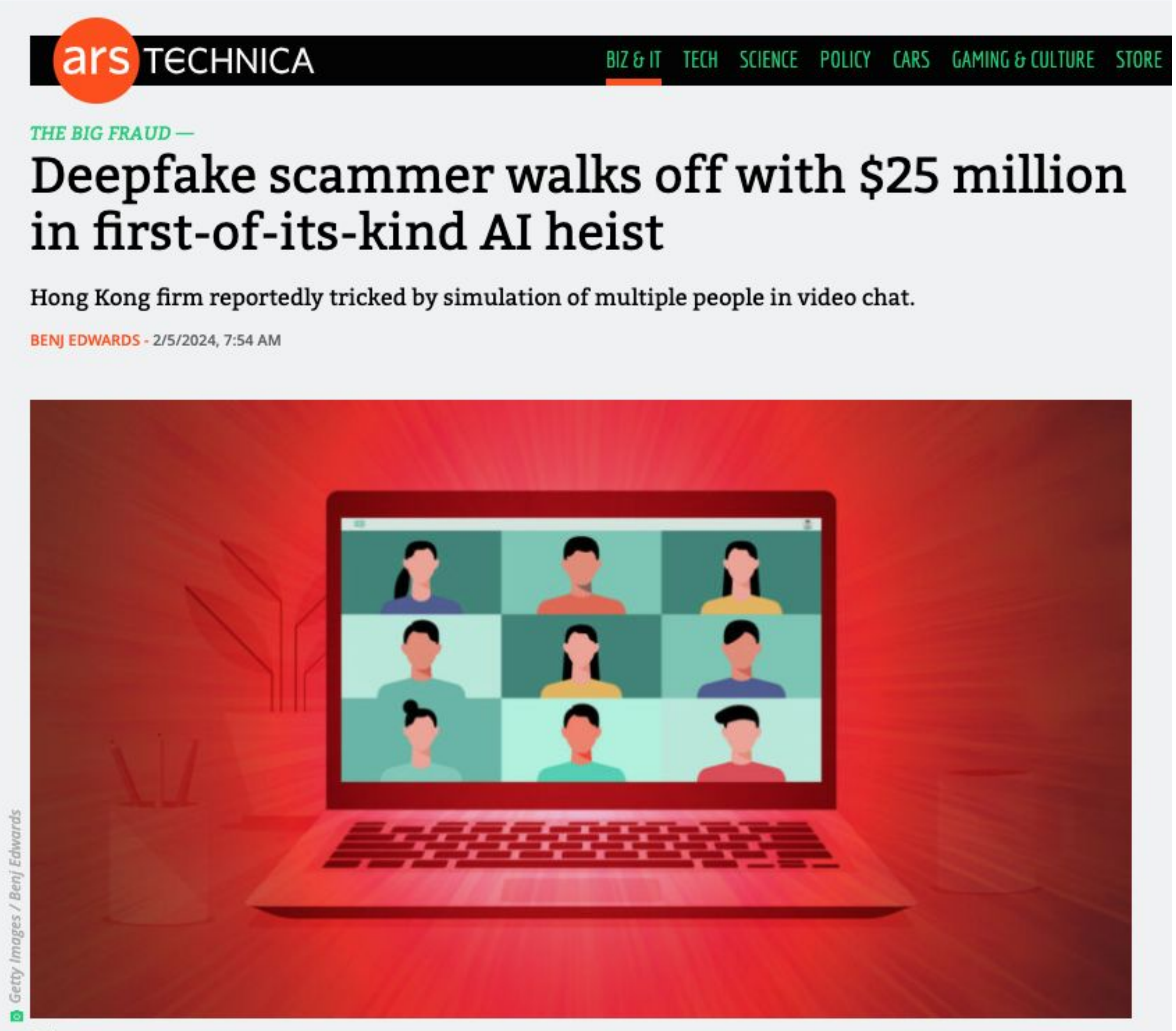
I'm thinking of rewarding our staff with surprise gifts as a token of appreciation and motivation. I trust you'll keep this information under wraps. I'd like this to remain between us until the gifts are handed out. Could you help with the purchase soon? Knowing your keen eye for detail, do you have any recommendations for local stores to buy these gift cards? I'm considering options like Amex, eBay, or Amazon.

When you're not busy tinkering in your shop or off-roading in your Jeep, I'd love to get your feedback. Looking forward to your insights before we move forward with this idea.

Best regards,
Mac Clemmens

**This might be far more difficult to spot!**

**Dave has to think even more critically.**



*THE BIG FRAUD —*

# Deepfake scammer walks off with $25 million in first-of-its-kind AI heist

Hong Kong firm reportedly tricked by simulation of multiple people in video chat.

BENJ EDWARDS - 2/5/2024, 7:54 AM

Getty Images / Benj Edwards

In February of 2024, a report from the South China Morning Post revealed a significant financial loss suffered by a multinational company's Hong Kong office, amounting to HK$200 million (US$25.6 million), due to a sophisticated scam involving deepfake technology.

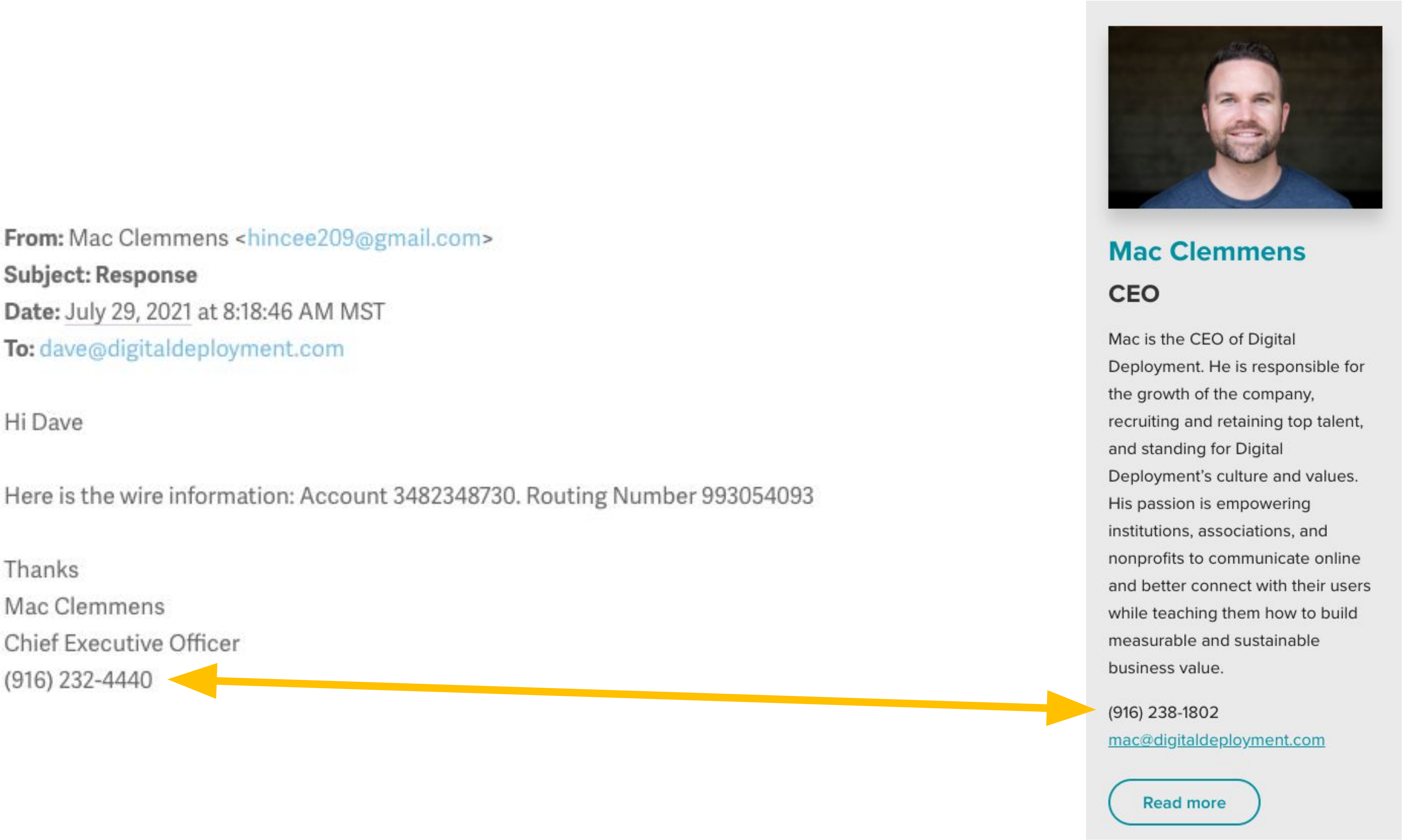
The scam featured a digitally recreated version of the company's chief financial officer, along with other employees, who appeared in a video conference call instructing an employee to transfer funds.

# Phishing Strategies

1. Need to test your staff from time to time
2. *Breach Secure Now* or *Bullphish ID* are good companies to use

# 5. Call when confirming wire transfers and payments

*(and how to know which phone numbers to use)*



**From:** Mac Clemmens <hincee209@gmail.com>
**Subject: Response**
**Date:** July 29, 2021 at 8:18:46 AM MST
**To:** dave@digitaldeployment.com

Hi Dave

Here is the wire information: Account 3482348730. Routing Number 993054093

Thanks
Mac Clemmens
Chief Executive Officer
(916) 232-4440

## Mac Clemmens

### CEO

Mac is the CEO of Digital Deployment. He is responsible for the growth of the company, recruiting and retaining top talent, and standing for Digital Deployment's culture and values. His passion is empowering institutions, associations, and nonprofits to communicate online and better connect with their users while teaching them how to build measurable and sustainable business value.

(916) 238-1802
mac@digitaldeployment.com

# How to be safe with wire transfers

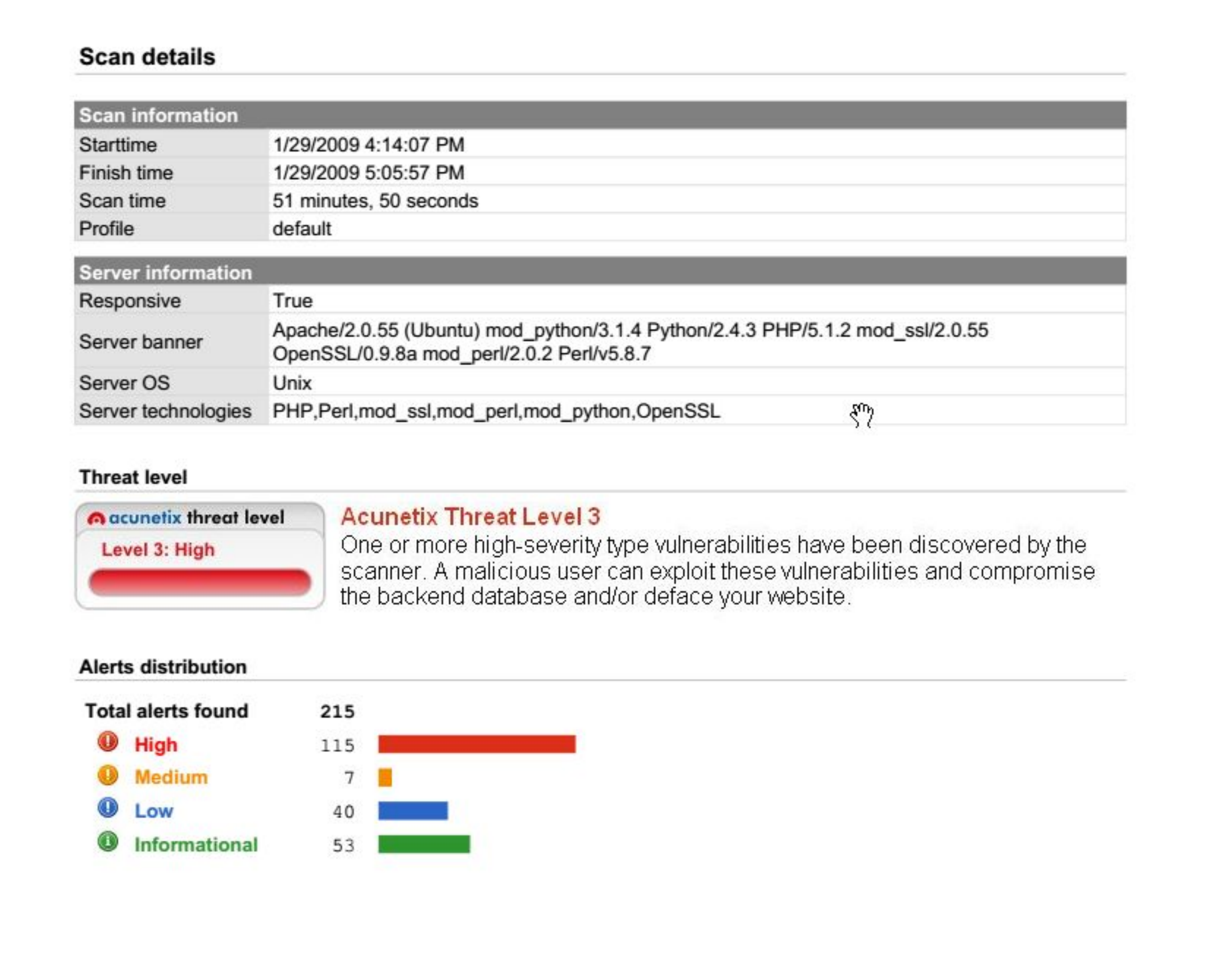
1. Always call YOUR number (in *your* contacts) to the vendor to verify, not the number on the request

2. You can use tools like iMessage Contact Key Verification (if on iPhone) to be sure you know you are text messaging the right person

3. Any new vendor OR updated change requires a 2-person control (one other person to sign off on the process)
   - One initiates
   - One approves

# 6. Conduct Network Security Testing

AKA "Pen Testing"



## Scan details

| Scan information | |
|---|---|
| Starttime | 1/29/2009 4:14:07 PM |
| Finish time | 1/29/2009 5:05:57 PM |
| Scan time | 51 minutes, 50 seconds |
| Profile | default |

| Server information | |
|---|---|
| Responsive | True |
| Server banner | Apache/2.0.55 (Ubuntu) mod_python/3.1.4 Python/2.4.3 PHP/5.1.2 mod_ssl/2.0.55 OpenSSL/0.9.8a mod_perl/2.0.2 Perl/v5.8.7 |
| Server OS | Unix |
| Server technologies | PHP,Perl,mod_ssl,mod_perl,mod_python,OpenSSL |

### Threat level

acunetix threat level

Level 3: High

**Acunetix Threat Level 3**

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

### Alerts distribution

| Total alerts found | 215 |
|---|---|
| High | 115 |
| Medium | 7 |
| Low | 40 |
| Informational | 53 |

# Network Security Testing Strategies

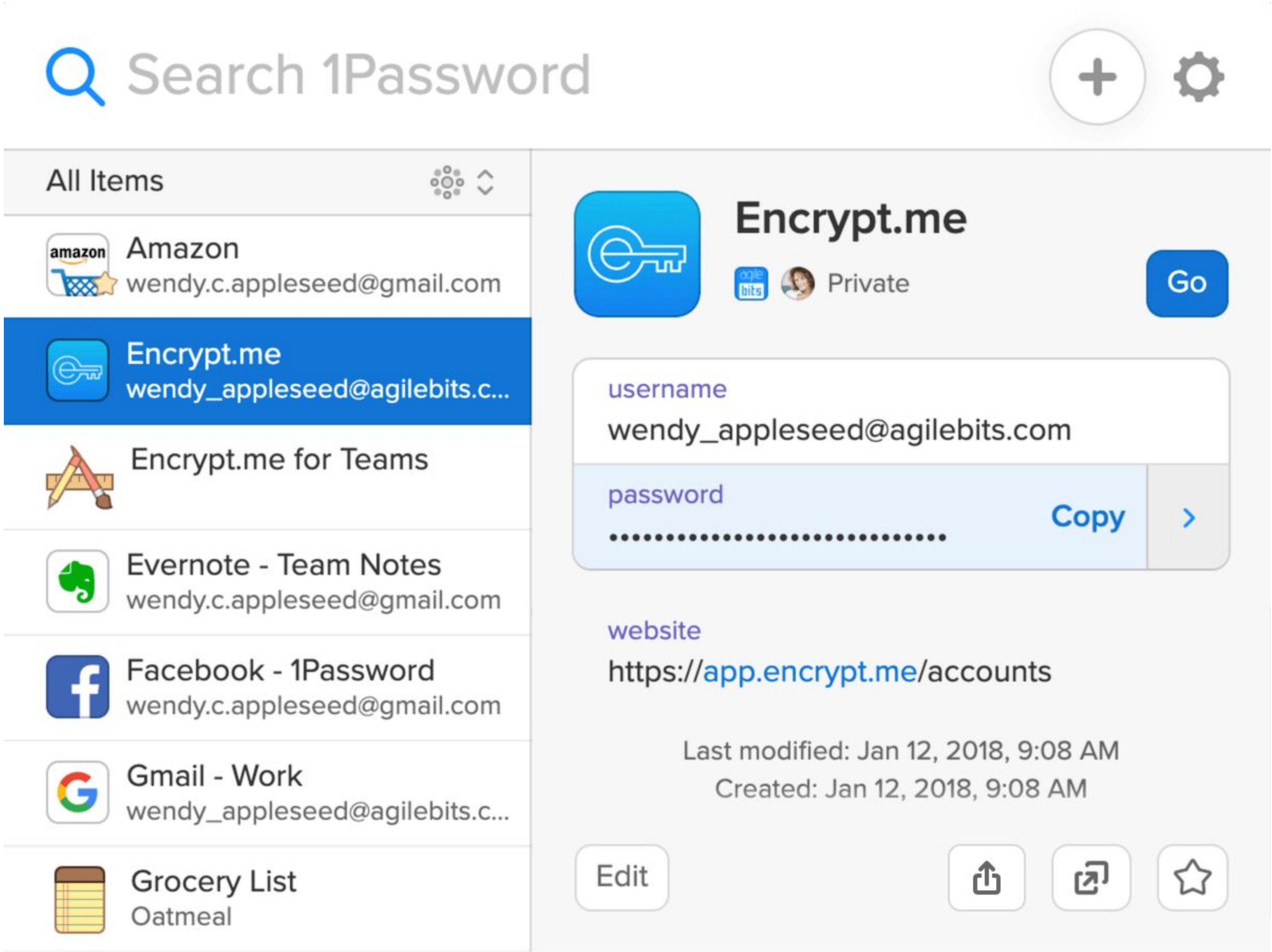
- Use an outside consultant
- Internal Network Scan: 5K-50K (especially if you have SCADA devices)
- Website Security Scan: 1K-5K depending on platform
- Like an audit

# 7. Password protect all devices

- Consider mobile device management (MDM) to enforce this and recover/wipe lost devices

# 8. Consider a password manager

- 1Password
- Bitwarden (for teams)
- LastPass



Amazon
wendy.c.appleseed@gmail.com

Encrypt.me
wendy_appleseed@agilebits.c...

Encrypt.me for Teams

Evernote - Team Notes
wendy.c.appleseed@gmail.com

Facebook - 1Password
wendy.c.appleseed@gmail.com

Gmail - Work
wendy_appleseed@agilebits.c...

Grocery List
Oatmeal

Encrypt.me

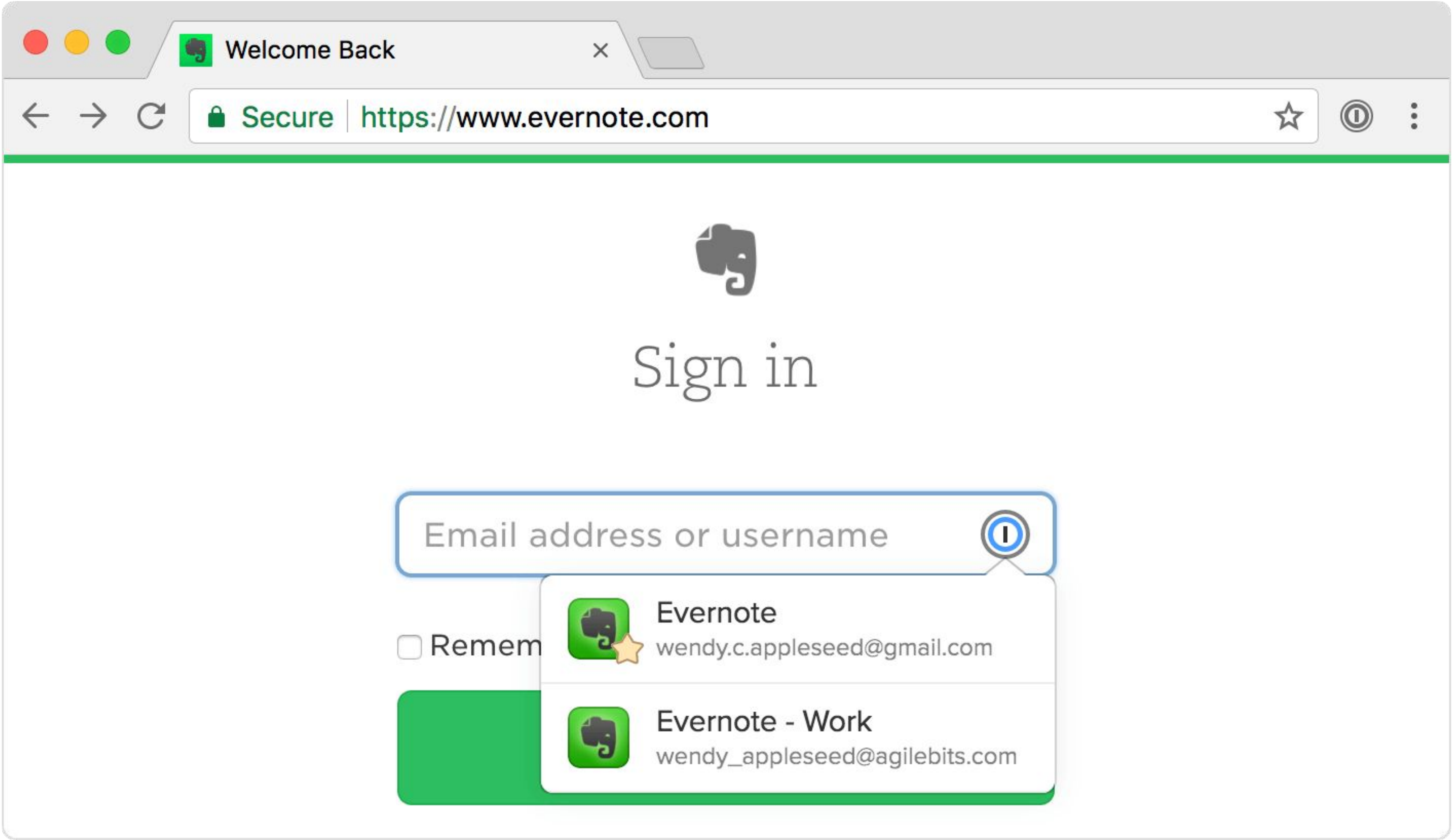
Private

username
wendy_appleseed@agilebits.com

password
••••••••••••••••••••••••••••••

website
https://app.encrypt.me/accounts

Last modified: Jan 12, 2018, 9:08 AM
Created: Jan 12, 2018, 9:08 AM


Welcome Back
Secure
https://www.evernote.com
Sign in
Email address or username
Remem
Evernote
wendy.c.appleseed@gmail.com
Evernote - Work
wendy_appleseed@agilebits.com

# Password Manager Benefits:

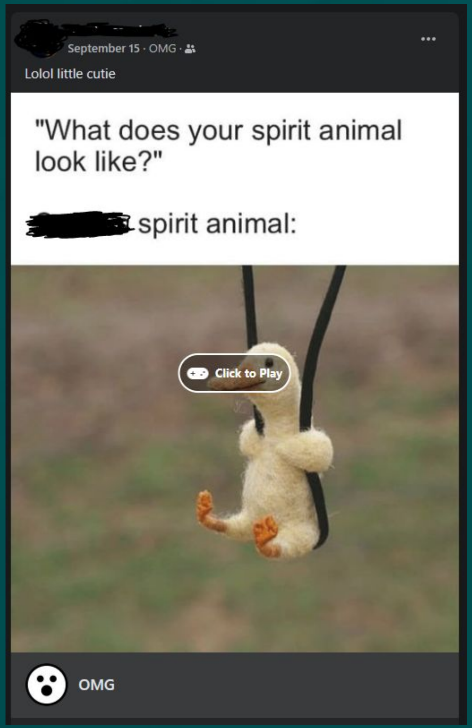
1. Encourages the use of unique passwords for every login

2. Helps ease staff transition problems (the #1 cause of lockout)

3. Defends against fraudulent lookalike sites from stealing credentials

4. You get an accurate list of systems!

# 9. Be careful what you share online (companies can aggregate data)



[redacted]

September 15 · OMG ·

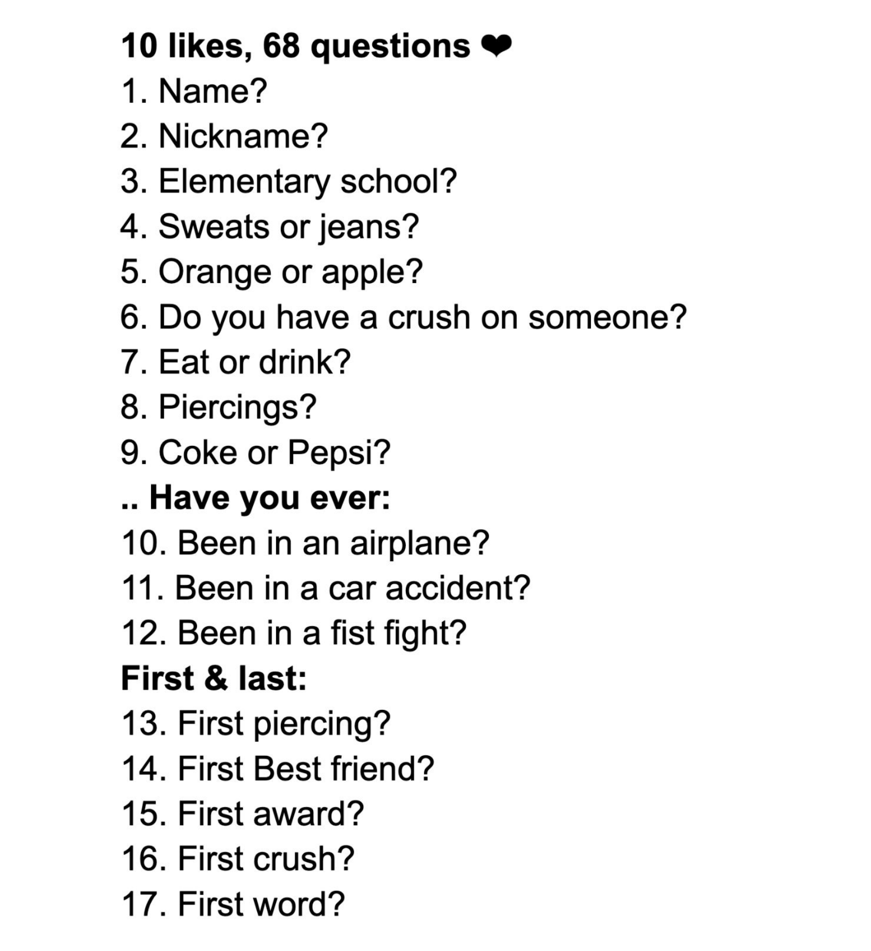
Lolol little cutie

"What does your spirit animal look like?"

[redacted] spirit animal:

The “games” you play and ask you to share to your feed may ask for permissions you’re not expecting

# These have been making the rounds



**10 likes, 68 questions ❤**
1. Name?
2. Nickname?
3. Elementary school?
4. Sweats or jeans?
5. Orange or apple?
6. Do you have a crush on someone?
7. Eat or drink?
8. Piercings?
9. Coke or Pepsi?

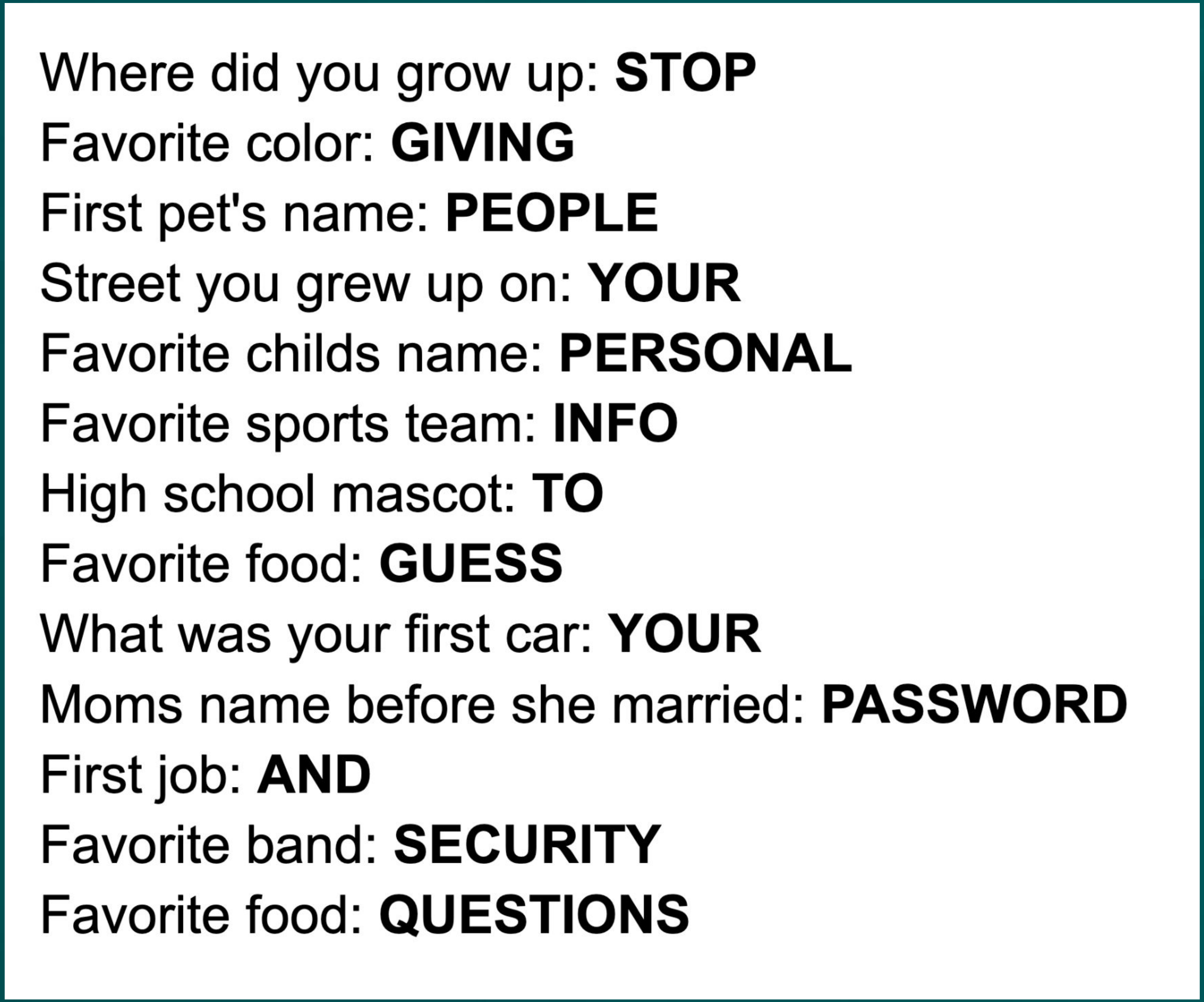
**.. Have you ever:**

10. Been in an airplane?
11. Been in a car accident?
12. Been in a fist fight?

**First & last:**

13. First piercing?
14. First Best friend?
15. First award?
16. First crush?
17. First word?

The Best Way to Answer???



Where did you grow up: **STOP**

Favorite color: **GIVING**

First pet's name: **PEOPLE**

Street you grew up on: **YOUR**

Favorite childs name: **PERSONAL**

Favorite sports team: **INFO**

High school mascot: **TO**

Favorite food: **GUESS**

What was your first car: **YOUR**

Moms name before she married: **PASSWORD**

First job: **AND**

Favorite band: **SECURITY**

Favorite food: **QUESTIONS**

# 10. Keep learning

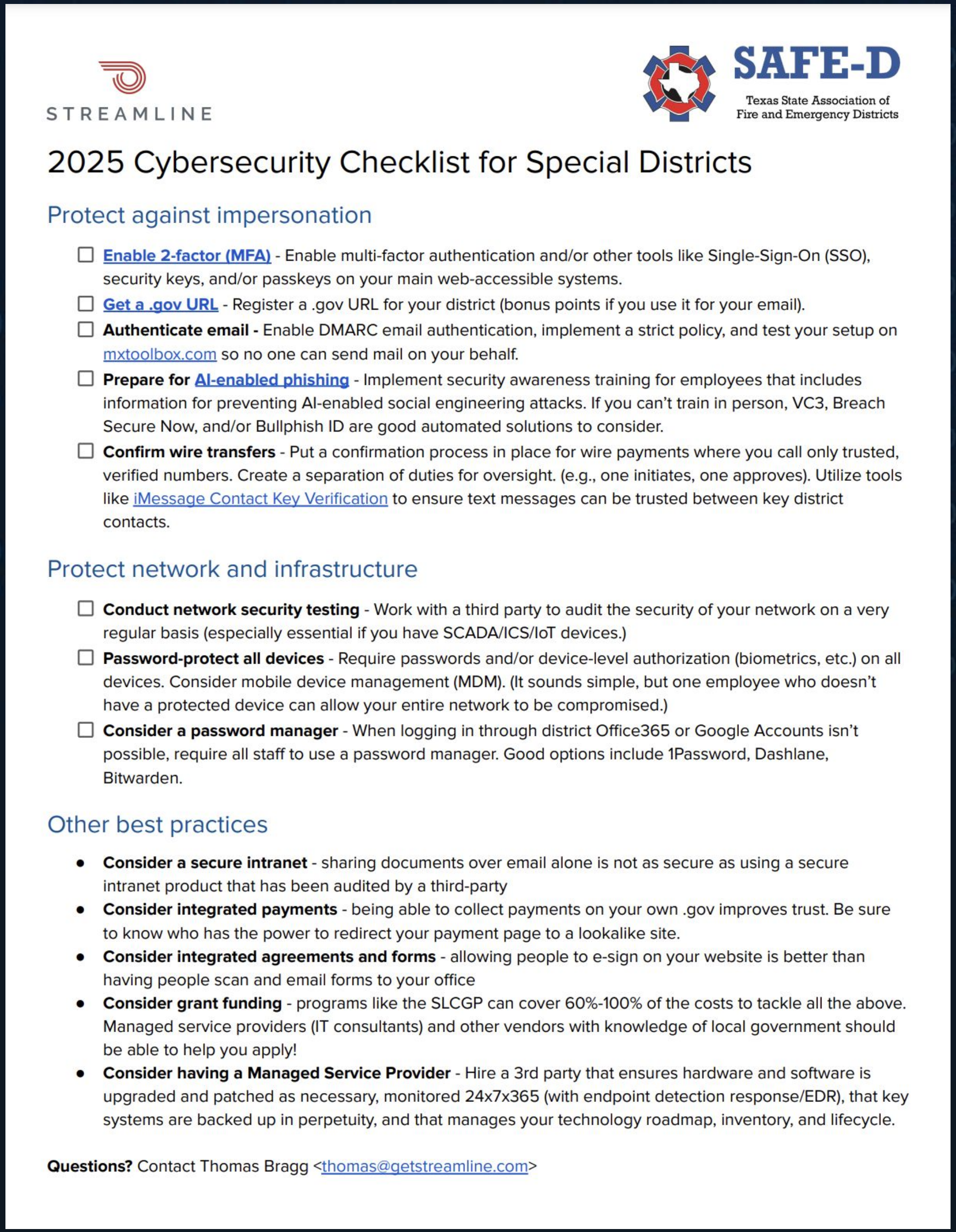
*What you're doing today is a perfect example of how to spot AI-powered cyber threats!*

# Get the checklist:

**tinyurl.com/TXSafeD**

**Questions?**

Tom Bragg
thomas@getstreamline.com



STREAMLINE

SAFE-D
Texas State Association of
Fire and Emergency Districts

## 2025 Cybersecurity Checklist for Special Districts

### Protect against impersonation

- ☐ **Enable 2-factor (MFA)** - Enable multi-factor authentication and/or other tools like Single-Sign-On (SSO), security keys, and/or passkeys on your main web-accessible systems.
- ☐ **Get a .gov URL** - Register a .gov URL for your district (bonus points if you use it for your email).
- ☐ **Authenticate email -** Enable DMARC email authentication, implement a strict policy, and test your setup on mxtoolbox.com so no one can send mail on your behalf.
- ☐ **Prepare for AI-enabled phishing** - Implement security awareness training for employees that includes information for preventing AI-enabled social engineering attacks. If you can't train in person, VC3, Breach Secure Now, and/or Bullphish ID are good automated solutions to consider.
- ☐ **Confirm wire transfers** - Put a confirmation process in place for wire payments where you call only trusted, verified numbers. Create a separation of duties for oversight. (e.g., one initiates, one approves). Utilize tools like iMessage Contact Key Verification to ensure text messages can be trusted between key district contacts.

### Protect network and infrastructure

- ☐ **Conduct network security testing** - Work with a third party to audit the security of your network on a very regular basis (especially essential if you have SCADA/ICS/IoT devices.)
- ☐ **Password-protect all devices** - Require passwords and/or device-level authorization (biometrics, etc.) on all devices. Consider mobile device management (MDM). (It sounds simple, but one employee who doesn't have a protected device can allow your entire network to be compromised.)
- ☐ **Consider a password manager** - When logging in through district Office365 or Google Accounts isn't possible, require all staff to use a password manager. Good options include 1Password, Dashlane, Bitwarden.

### Other best practices

- **Consider a secure intranet** - sharing documents over email alone is not as secure as using a secure intranet product that has been audited by a third-party
- **Consider integrated payments** - being able to collect payments on your own .gov improves trust. Be sure to know who has the power to redirect your payment page to a lookalike site.
- **Consider integrated agreements and forms** - allowing people to e-sign on your website is better than having people scan and email forms to your office
- **Consider grant funding** - programs like the SLCGP can cover 60%-100% of the costs to tackle all the above. Managed service providers (IT consultants) and other vendors with knowledge of local government should be able to help you apply!
- **Consider having a Managed Service Provider** - Hire a 3rd party that ensures hardware and software is upgraded and patched as necessary, monitored 24x7x365 (with endpoint detection response/EDR), that key systems are backed up in perpetuity, and that manages your technology roadmap, inventory, and lifecycle.

**Questions?** Contact Thomas Bragg <thomas@getstreamline.com>