

ENDSIGHT.NET

End User Cybersecurity Training

VERSION 6.2

Jan. 13th, 2025

endsight

1144 Jordan Lane, Napa, CA 94559 | www.endsight.net | info@endsight.net | (833) 363-7444



JASON CLAUSE
HOST

Director of Marketing @ Endsight
[linkedin.com/in/jasonclause](https://www.linkedin.com/in/jasonclause)



STEPHEN HICKS
PRESENTER

Security Practice Manager @ Endsight
<https://www.linkedin.com/in/shicks/>



Our purpose: Help others thrive

Our values:



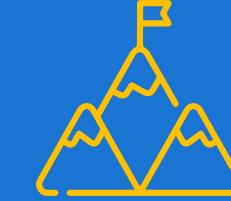
Respect &
Connect



Servant's
Heart



Value
Value



Progress Over
Comfort

Exciting News: Some proud moments



MSP 501
Channel Futures™ 2025

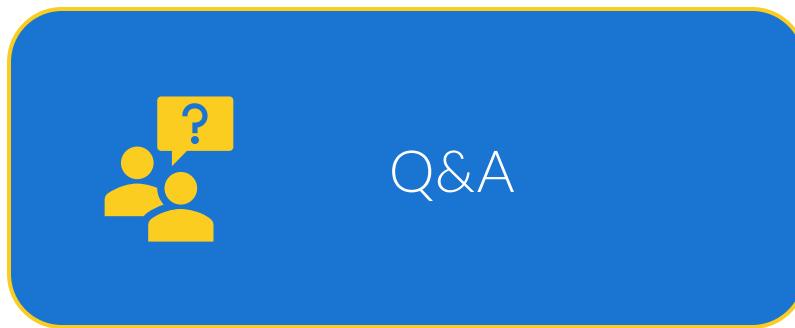


Right of Boom 2025: Capture the Flag
2nd Place



SAN DIEGO BUSINESS JOURNAL
2025 TOP
TECHNOLOGY SOLUTION PROVIDERS

Agenda



For CLMs & California Lawyers



Eligible for 1 credit hour of CLE (State of California) and the CLM program



During sign-up, you were asked to select “Yes” if either applied to you



We have currently identified 0 registrants eligible for credit

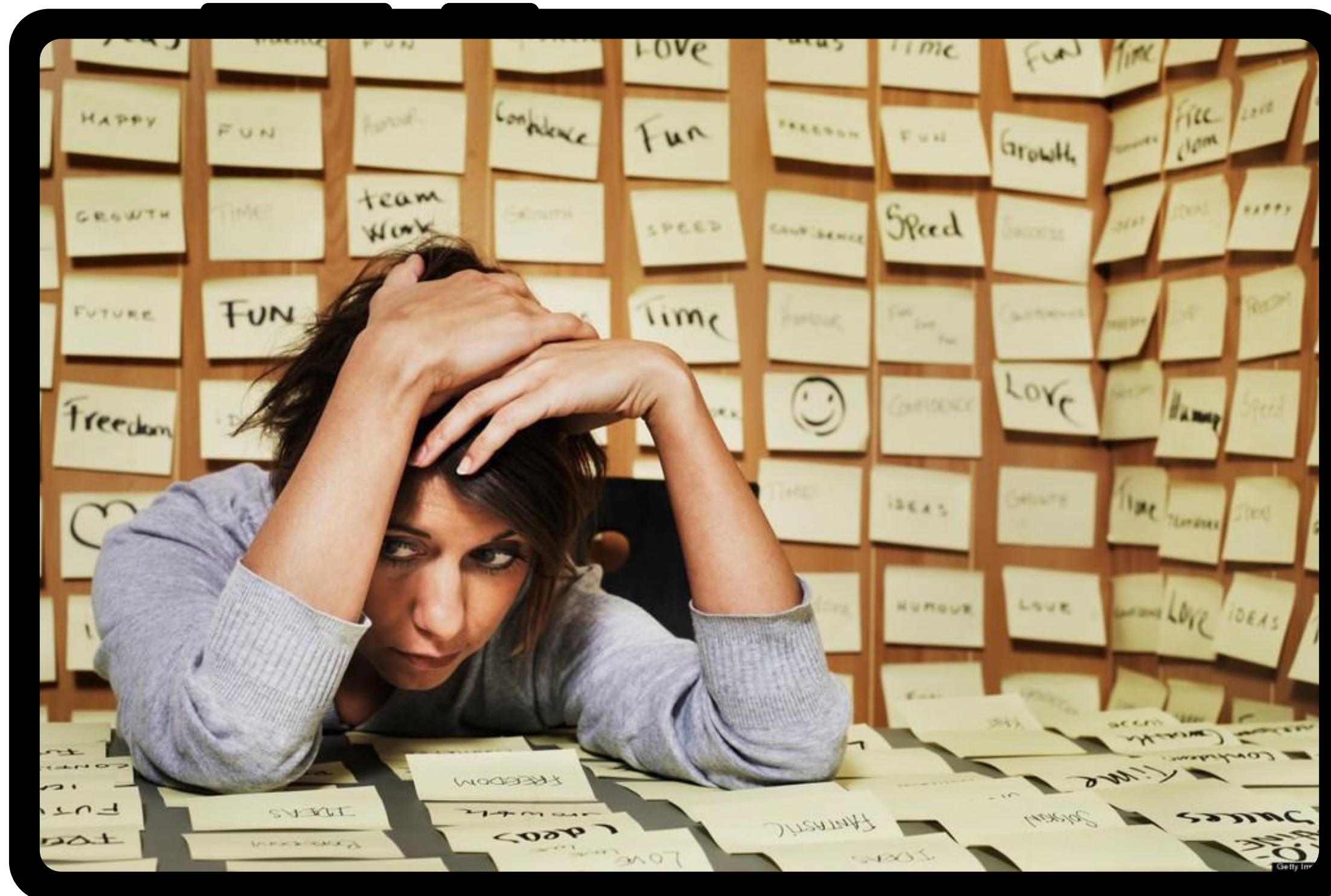


To confirm your eligibility, please contact Aaron at akreps@endsight.net to ensure credit is received

Currently Eligible for Credit



Why are you here?



CYBER SECURITY MARKET FORECAST

Rising attack incidents and cyber regulation are key forces behind the global cybersecurity market. By 2026, it is predicted to reach \$270 billion—an 86% leap from 2018.



Source: Australian Cyber Security Growth Network, 2019
USD B per annum, 2018 • latest actual data (constant exchange rates)

ANYONE CAN BE A VICTIM OF CYBER CRIME.

Even businesses and entire governments. As the world becomes ever more connected and reliant on technology, it opens the door for online hackers to exploit critical security flaws in our systems.

To combat this growing threat, our cybersecurity capabilities must match—and better yet, surpass—the sophistication of cybercriminals.

DIGITAL WORLD / 93

Lifecycle of an Attack

From Phish to \$2.5M Ransomware Attack



Layered Cyber Security

(People, Process, Technology)



SECURITY



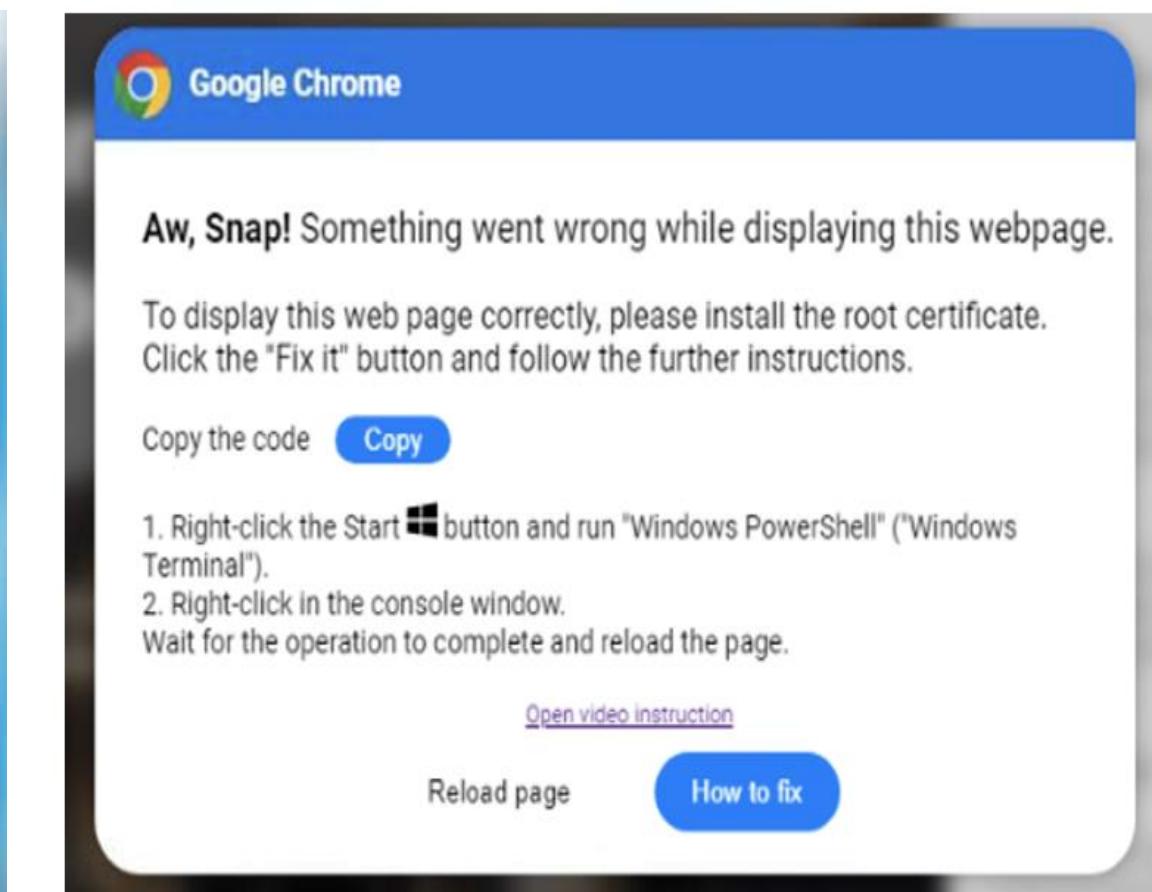
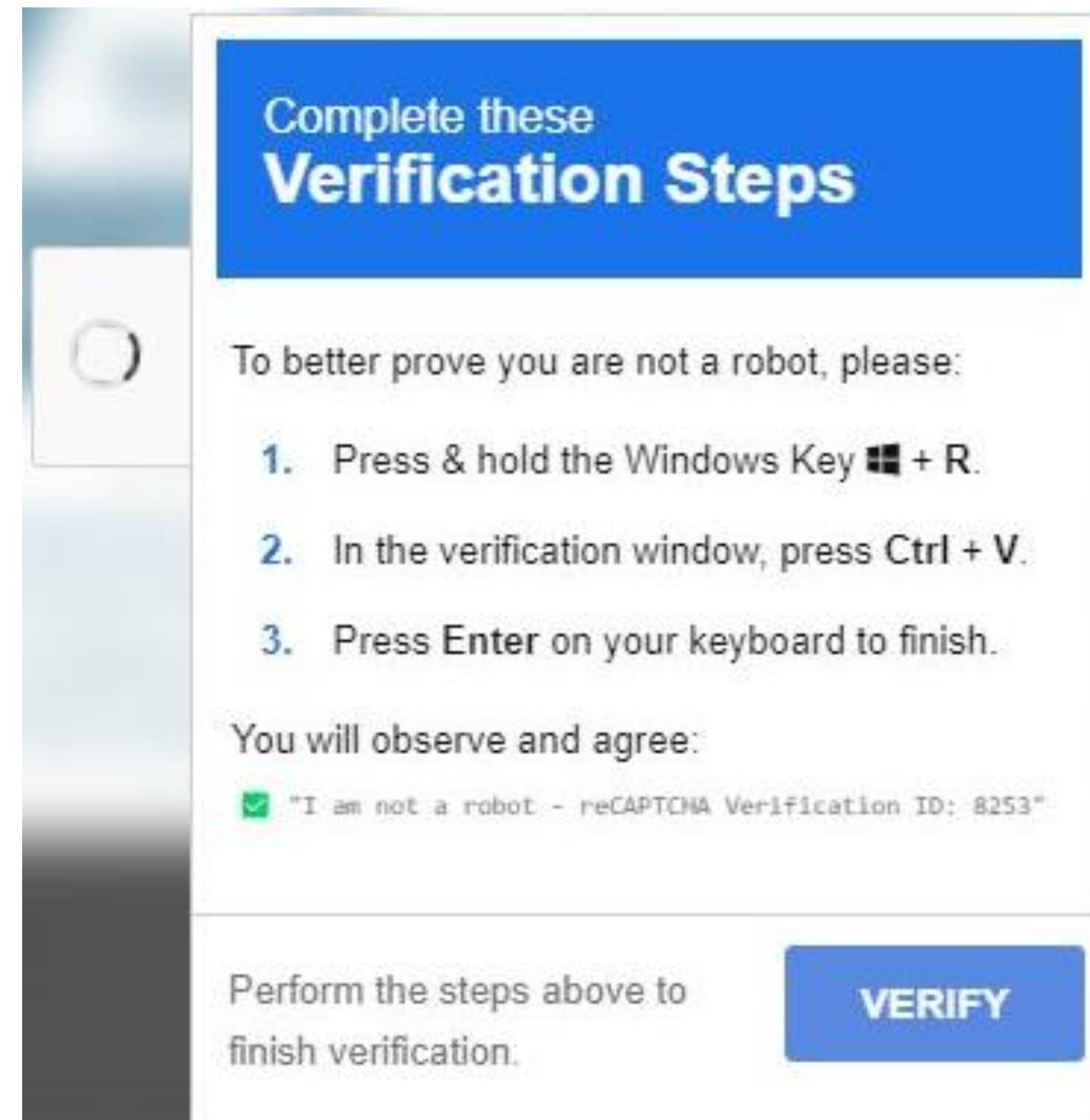
Stephen Hicks

Security Practice Manager

Endsight

Fake CAPTCHAs

What is
a fake
CAPTCHA?



2025 ↑

Delete Archive Report Reply Reply all Forward Zoom Read / Unread Categorize Flag / Unflag Print ...

Quarantine<noreply@urbanhome.co.jp> Reply Reply all Forward ...
Thu 1/30/2025 9:03 AM

! High importance

Some content in this message has been blocked because the sender isn't in your Safe senders list. [Trust sender](#) [Show blocked content](#)

You forwarded this message on Thu 1/30/2025 12:10 PM

You don't often get email from noreply@urbanhome.co.jp. [Learn why this is important](#)

CAUTION: This email originated from outside your organization. Exercise caution when opening attachments or clicking links; especially from unknown senders.



Review These Messages

2 messages are being held for you to review as of **January 30, 2025 at 08:58:13 AM (UTC)**.

Review them within **30 days of the received date** by going to the [Quarantine page](#) in the Security Center.

Prevented spam messages

Sender: [REDACTED]

Subject: Office 365 Password Authentication Record Change

Date: January 30, 2025 at 08:58:13 AM

[Review Message](#) [Delete](#)

Sender: [REDACTED]

Subject: Payroll Recordkeeping Requirements And Changes

Date: January 30, 2025 at 08:58:13 AM

[Review Message](#) [Delete](#)

© 2024 Microsoft Corporation. All rights reserved.
[Privacy Statement](#)
[Acceptable Use Policy](#)

Reply Forward

Fundamentals Overview

Dictionary

Search for a word



sus·pi·cion

/səˈspiSHən/

noun

1. a feeling or thought that something is possible, likely, or true.
"she had a sneaking **suspicion** that he was laughing at her"

Similar:

intuition

feeling

impression

inkling

surmise

guess



2. cautious distrust.

"her activities were regarded with suspicion by the headmistress"

Similar:

misgiving

doubt

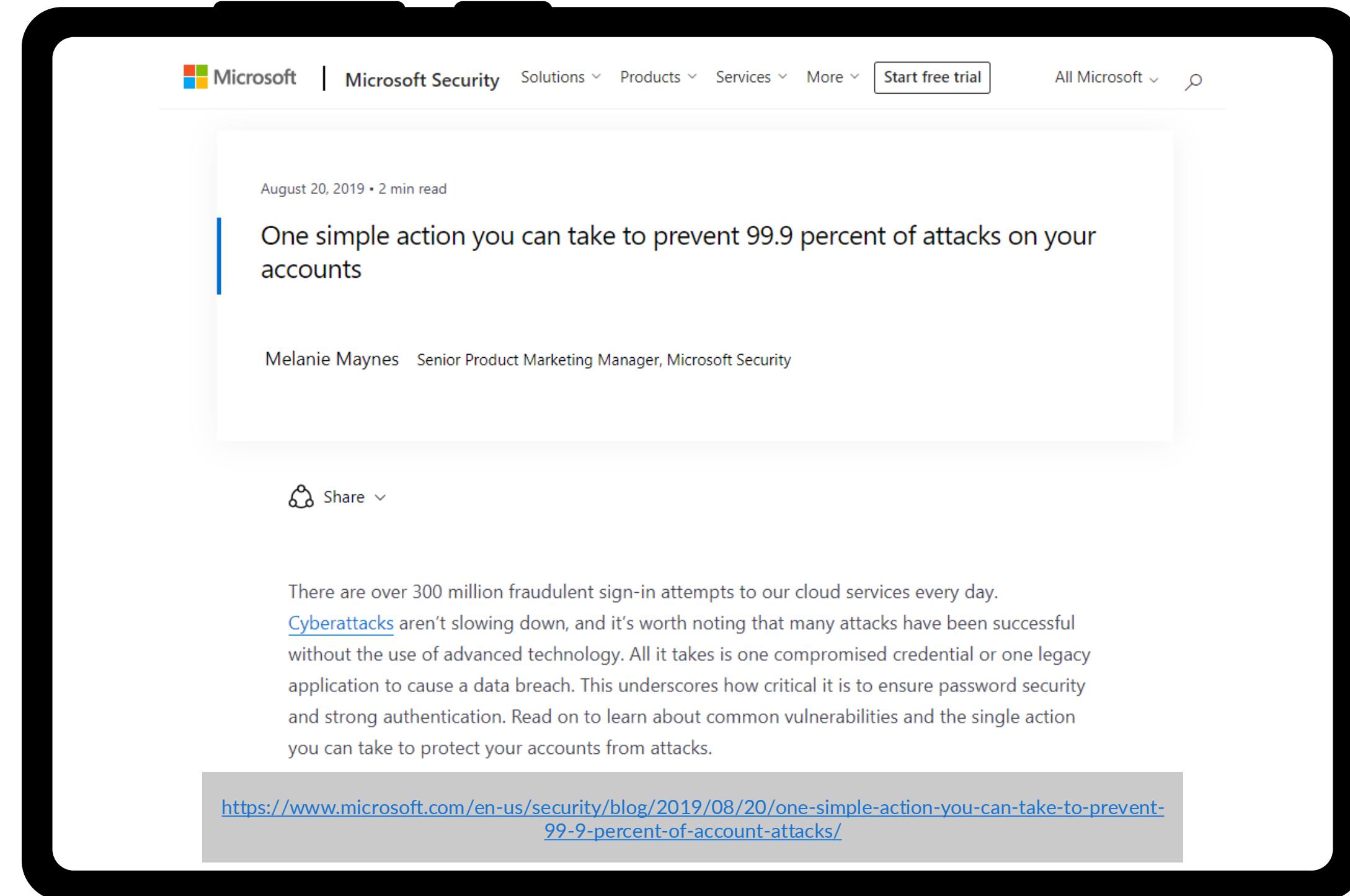
qualm

wariness

chariness

reservation





Microsoft | Microsoft Security Solutions Products Services More Start free trial All Microsoft

August 20, 2019 • 2 min read

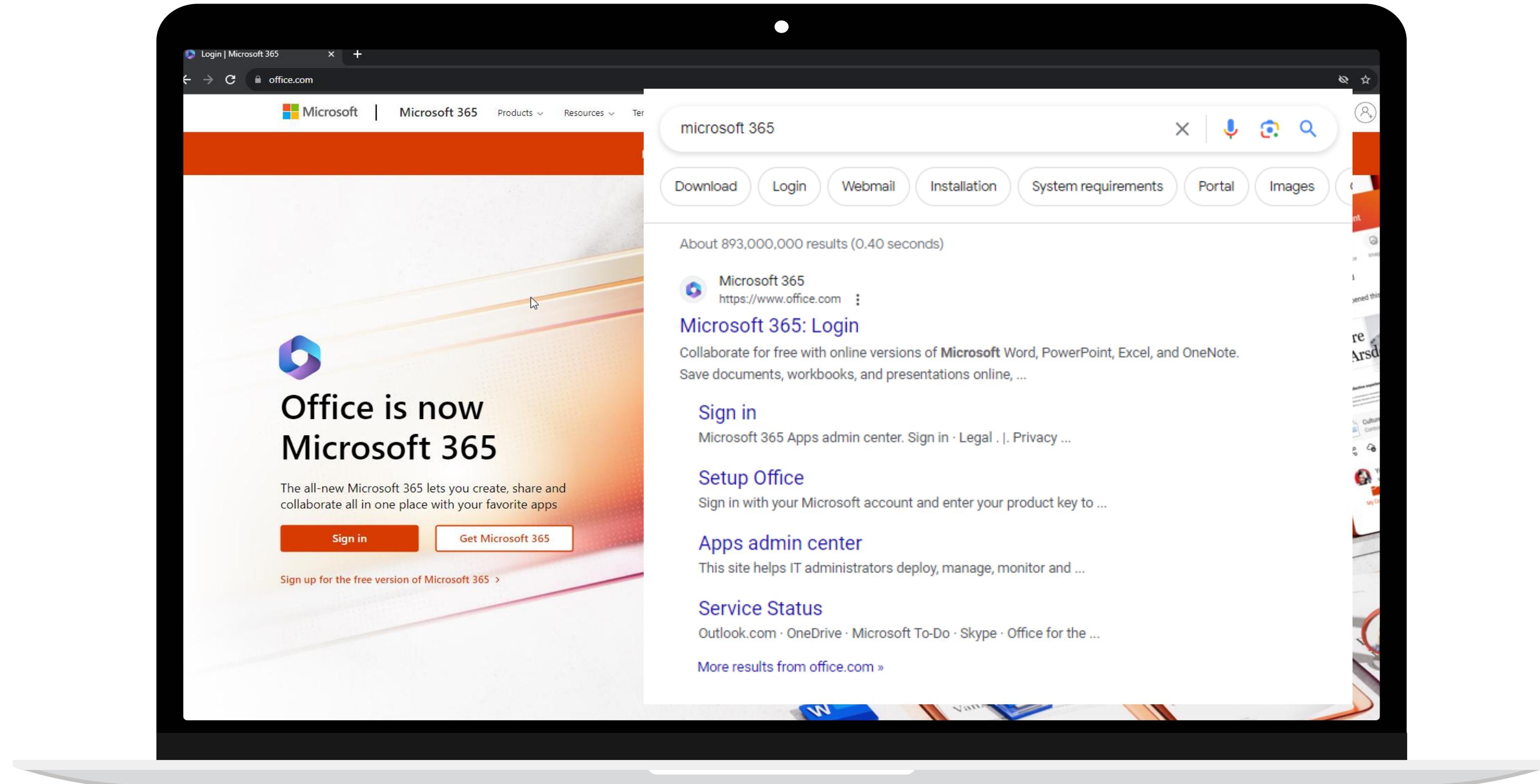
One simple action you can take to prevent 99.9 percent of attacks on your accounts

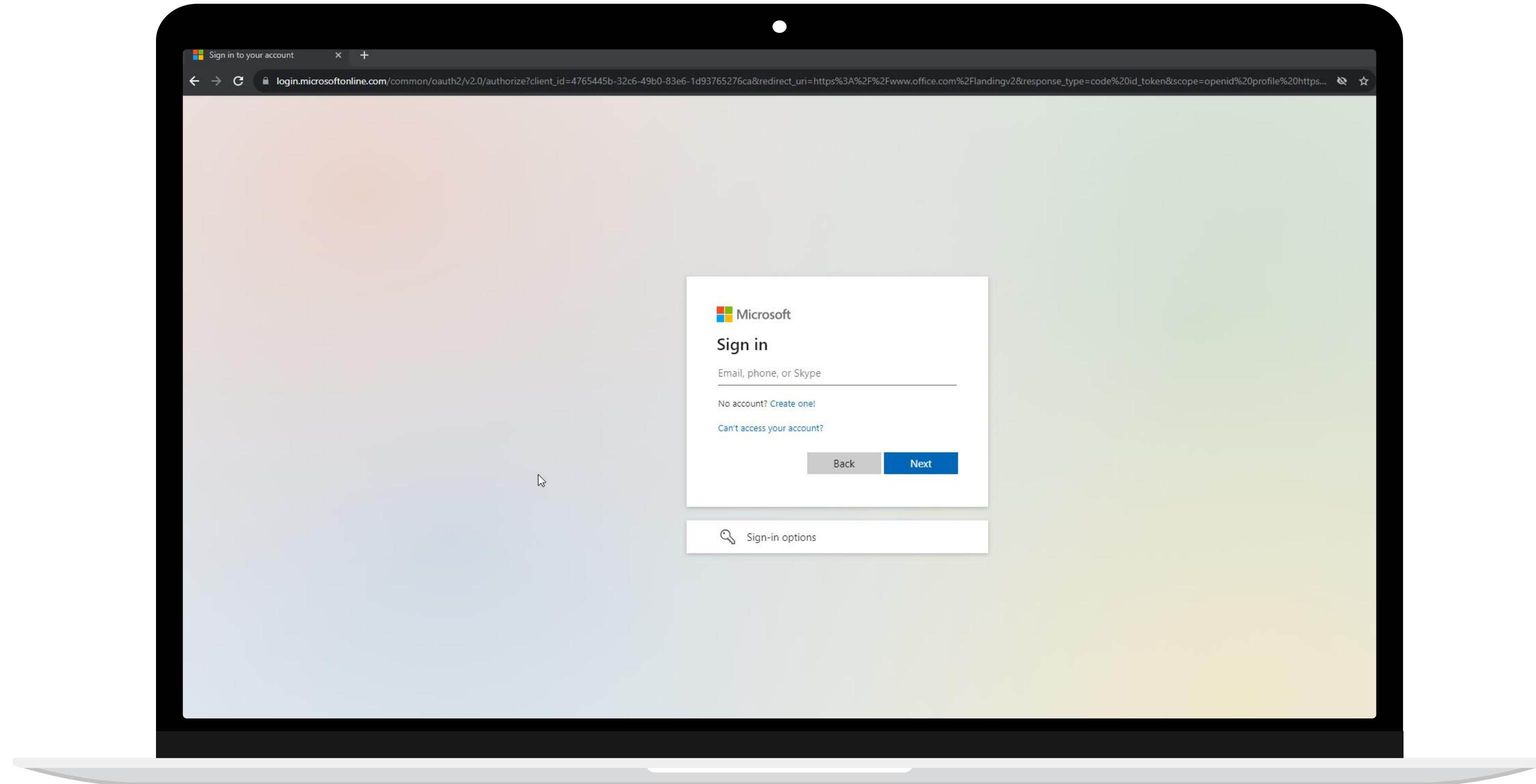
Melanie Maynes Senior Product Marketing Manager, Microsoft Security

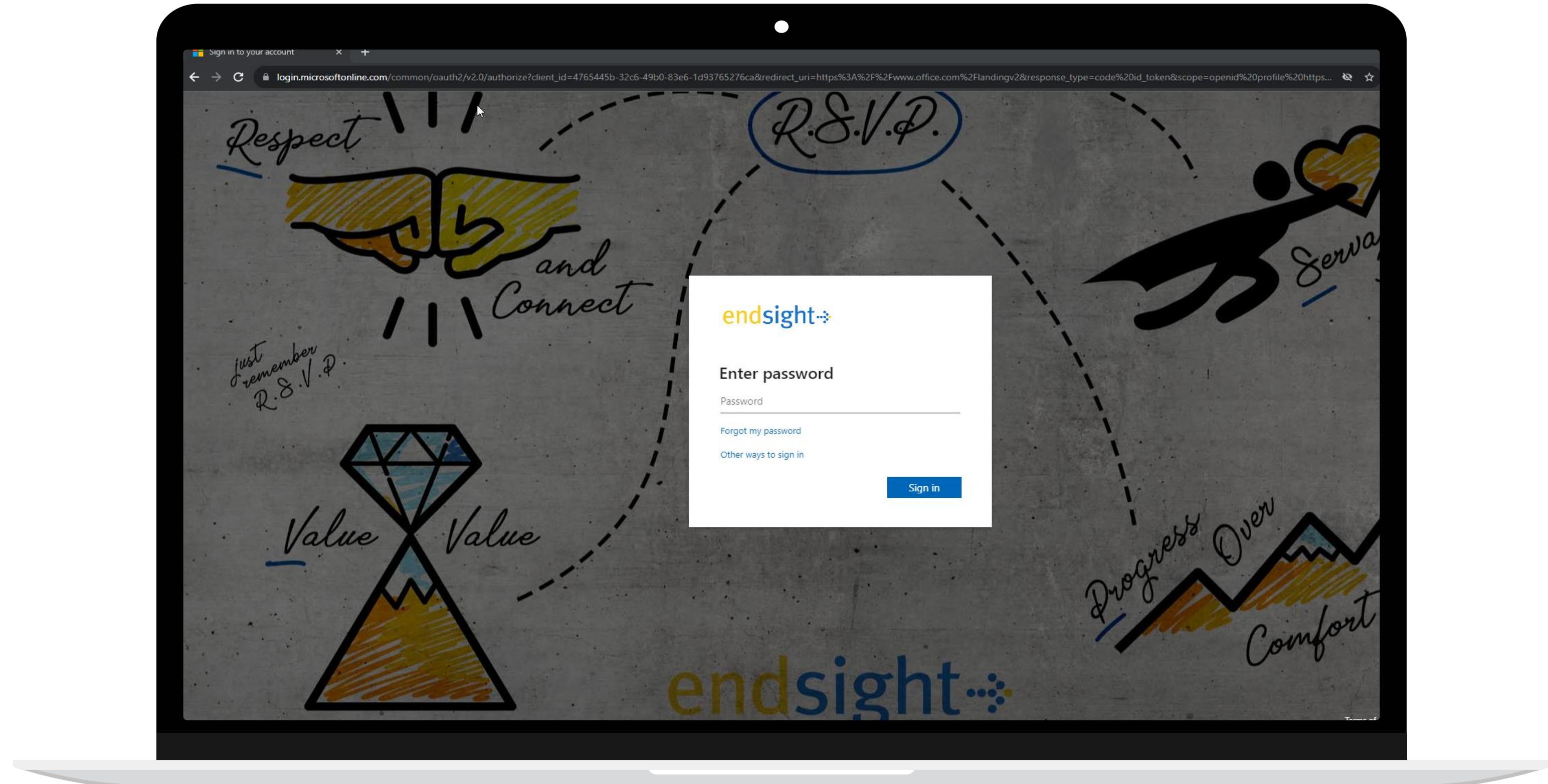
Share

There are over 300 million fraudulent sign-in attempts to our cloud services every day. [Cyberattacks](#) aren't slowing down, and it's worth noting that many attacks have been successful without the use of advanced technology. All it takes is one compromised credential or one legacy application to cause a data breach. This underscores how critical it is to ensure password security and strong authentication. Read on to learn about common vulnerabilities and the single action you can take to protect your accounts from attacks.

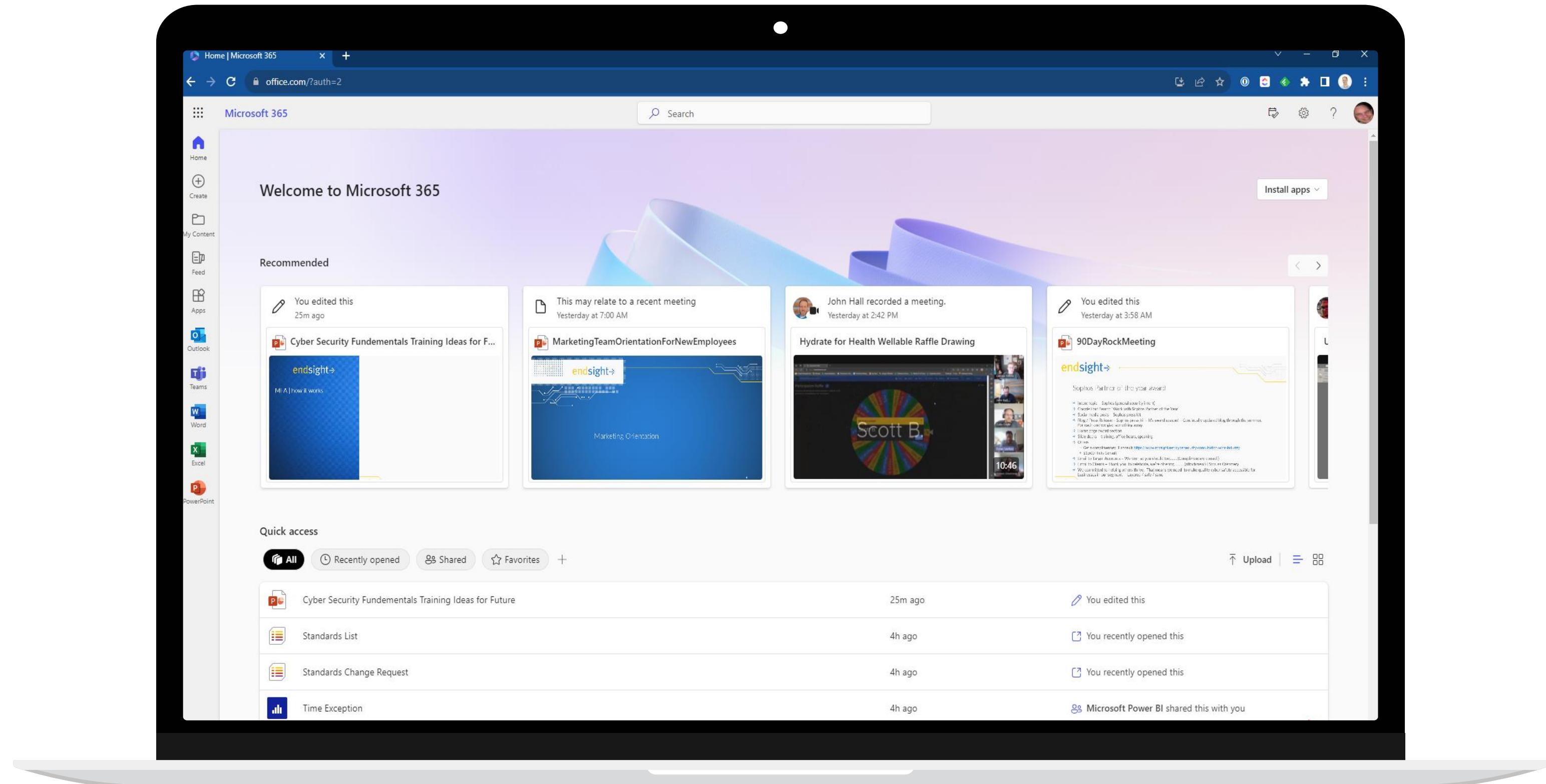
<https://www.microsoft.com/en-us/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/>





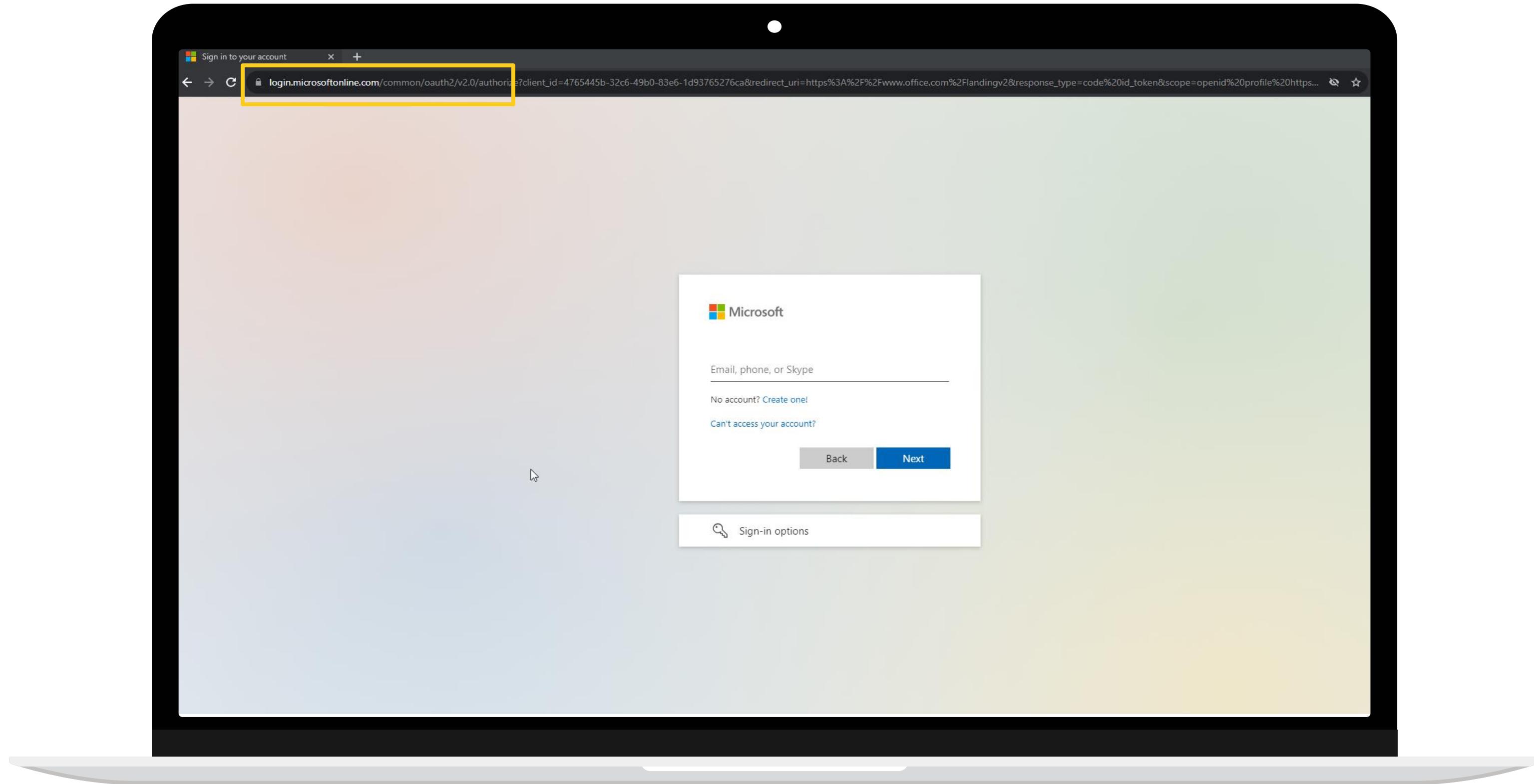






MFA Bypass

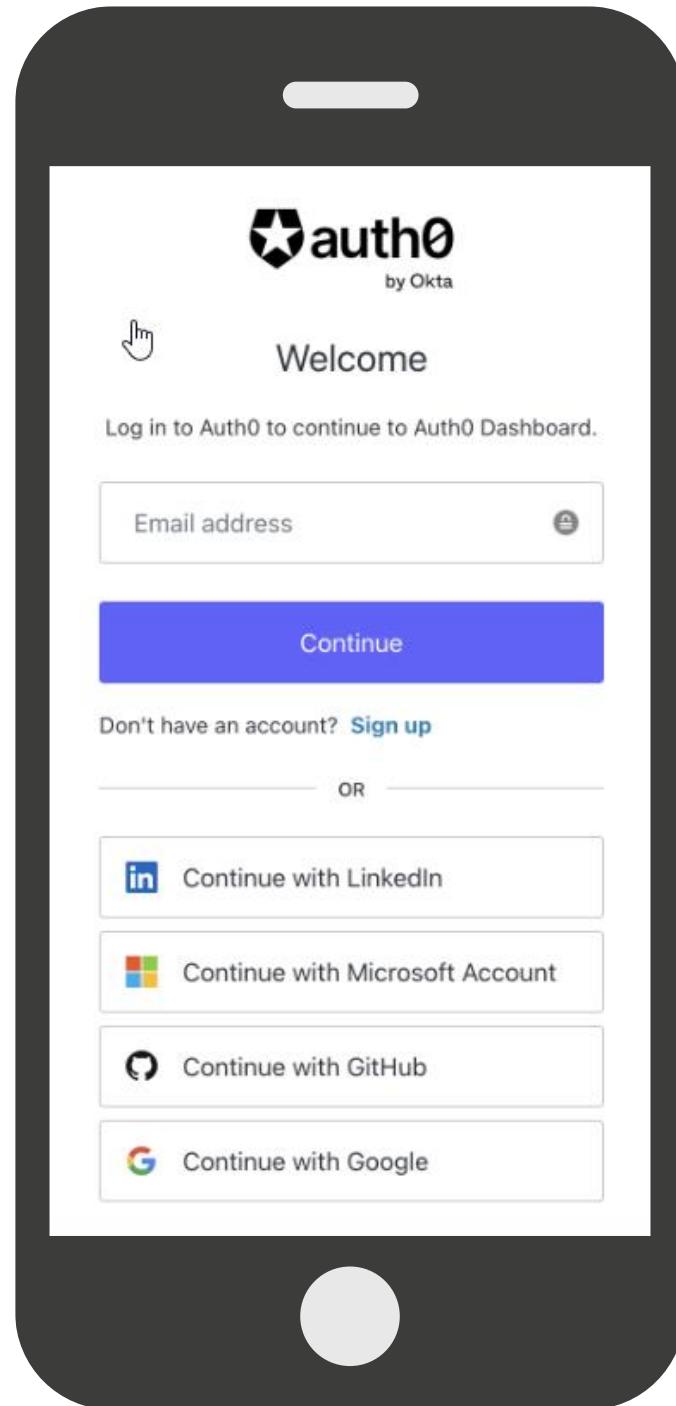




Use multi-channel verification



Identity management



01

Less access to personal information

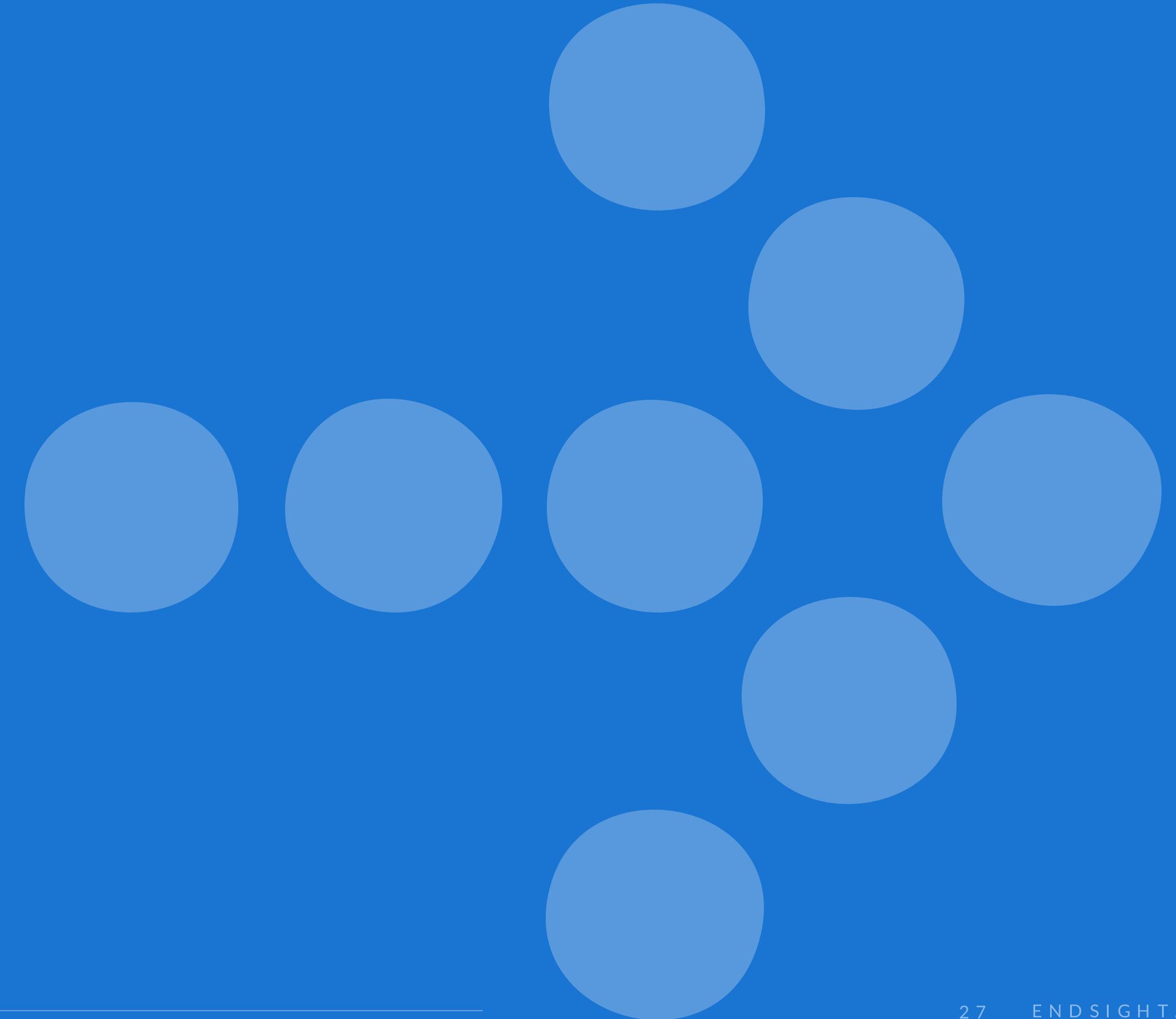
02

Be careful how much permission/access you allow

Tapping isn't just easy.....

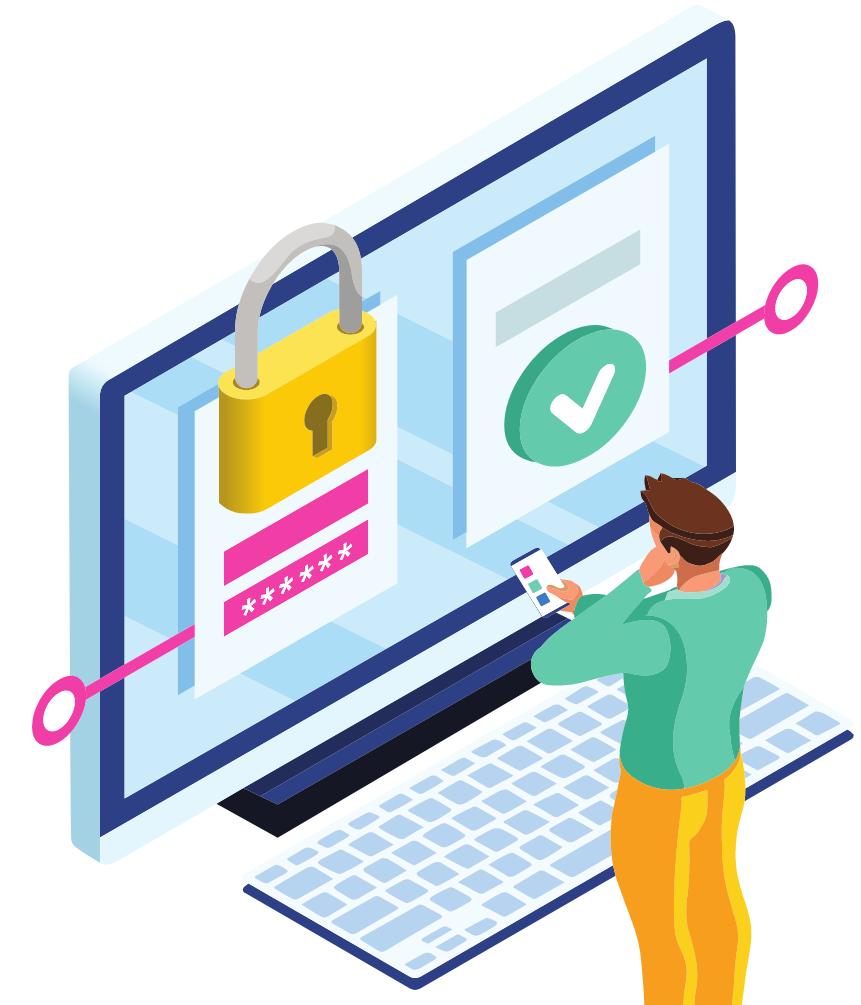


Cybersecurity Hygiene



NETWORKS

- 01 Make sure you have a good password on your home network
- 02 Change that password once a year
- 03 If you don't live here, you don't get the Wi-Fi password
- 04 Don't forget about your smart devices!!!



01

Good passwords are long

02

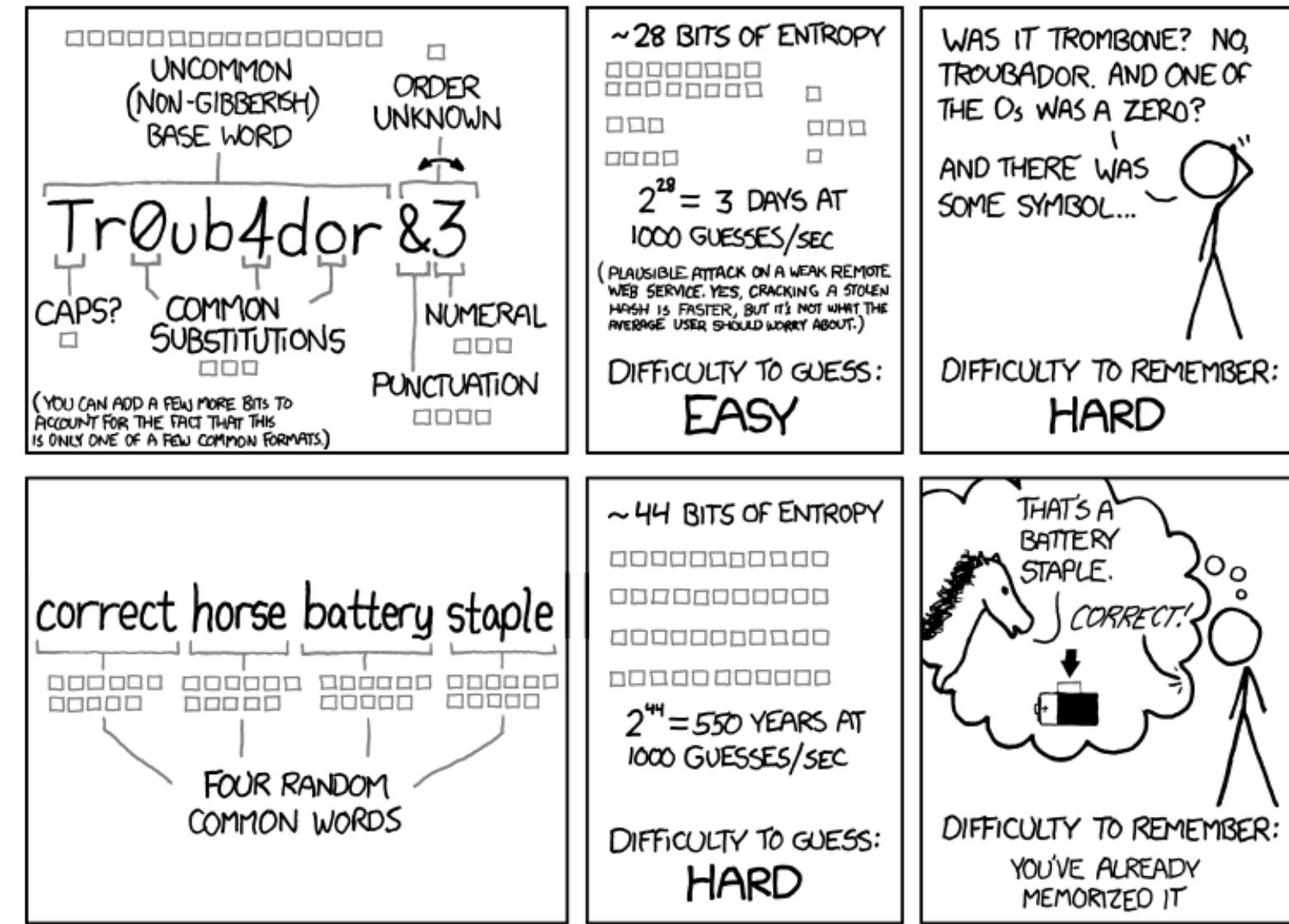
Good passwords are random

03

Humans are bad at randomness

04

Password generators matter



THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

WORKSTATIONS

- 01 If you leave it, LOCK it!
- 02 Never share your password with anyone!
- 03 Use your work devices for work, your home devices for home
- 04 Continue to leave your computers on at night

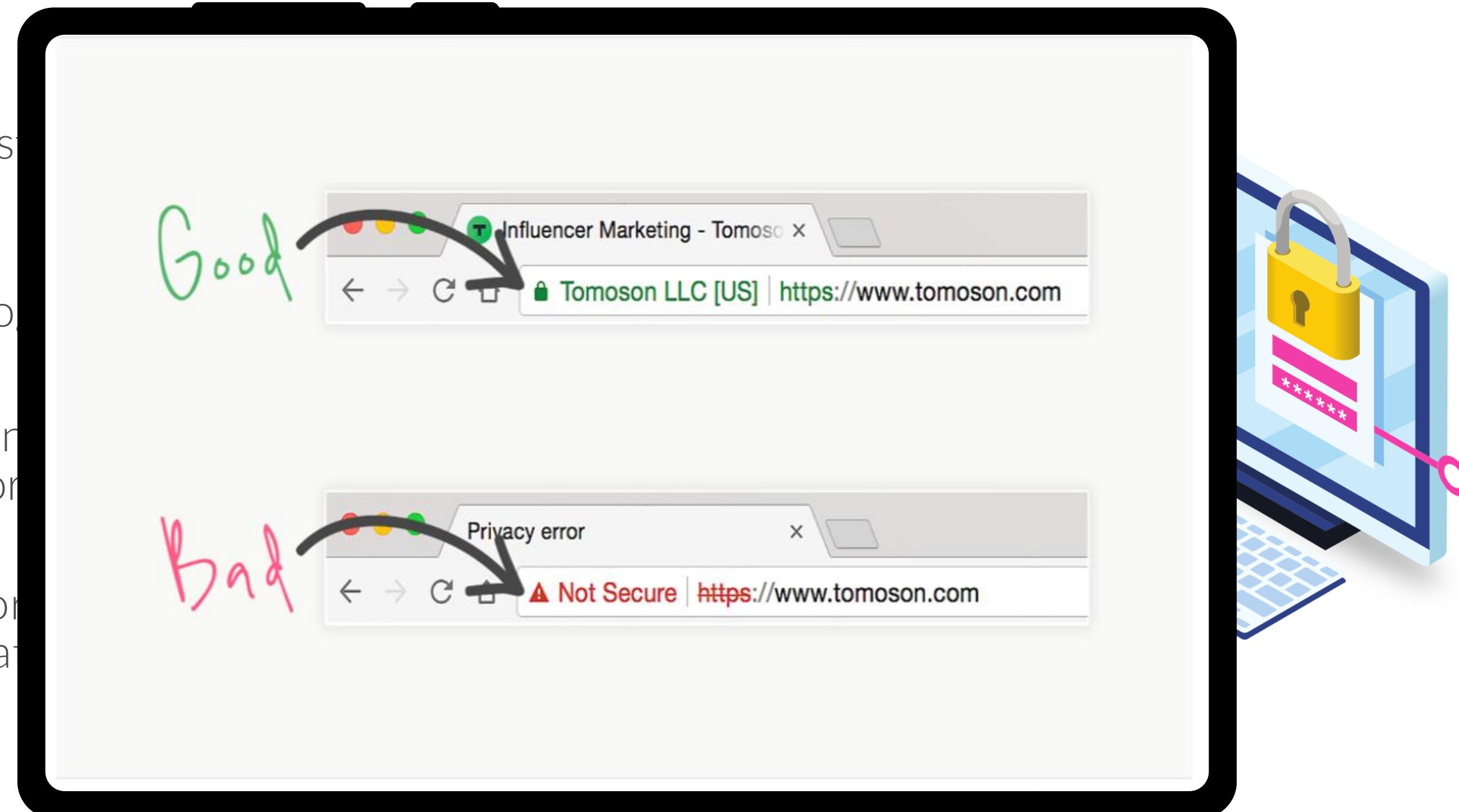


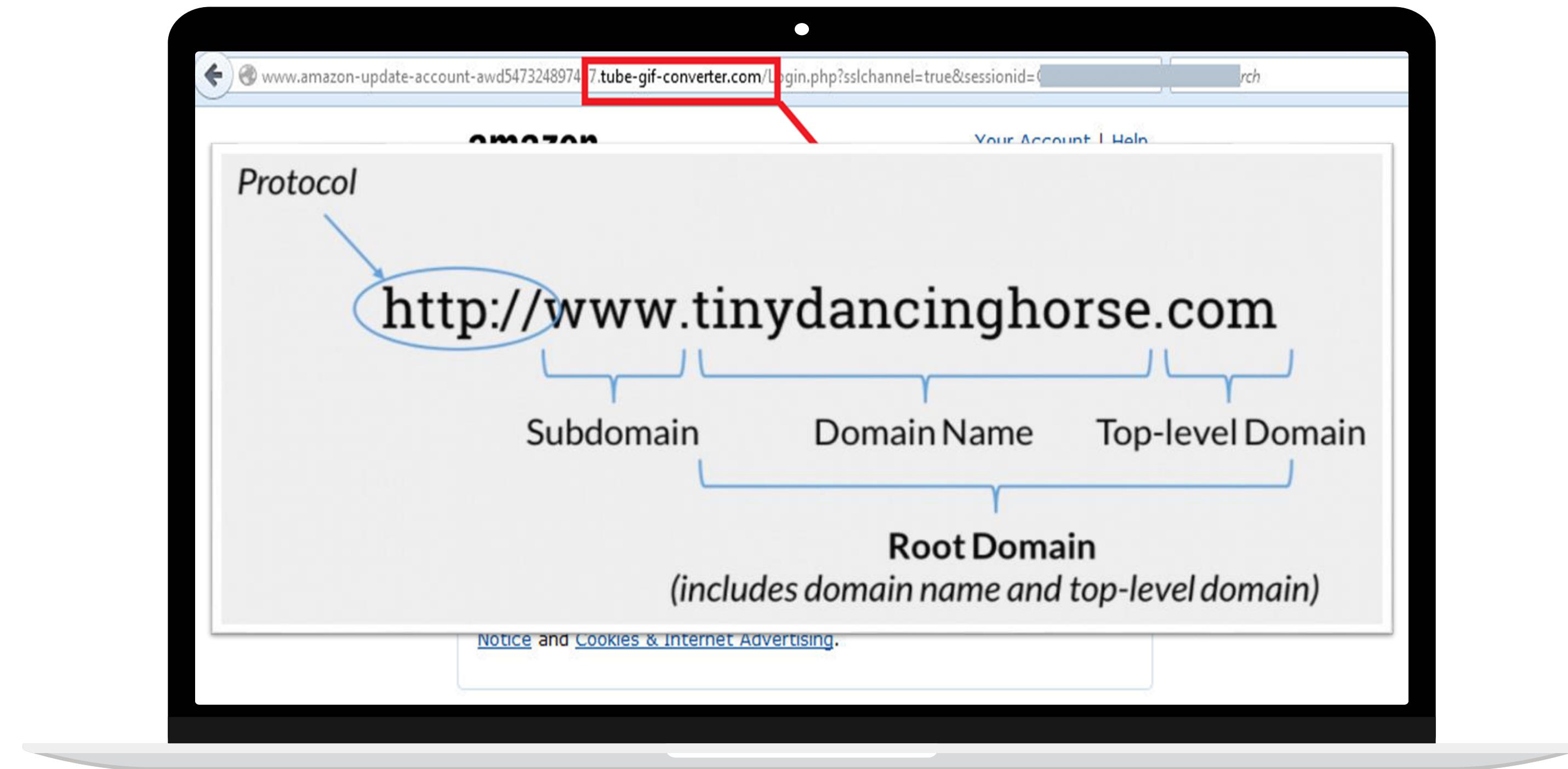
Do you know your acceptable use policy?

Every company should have one and
you should understand it.

WILD, WILD WEB

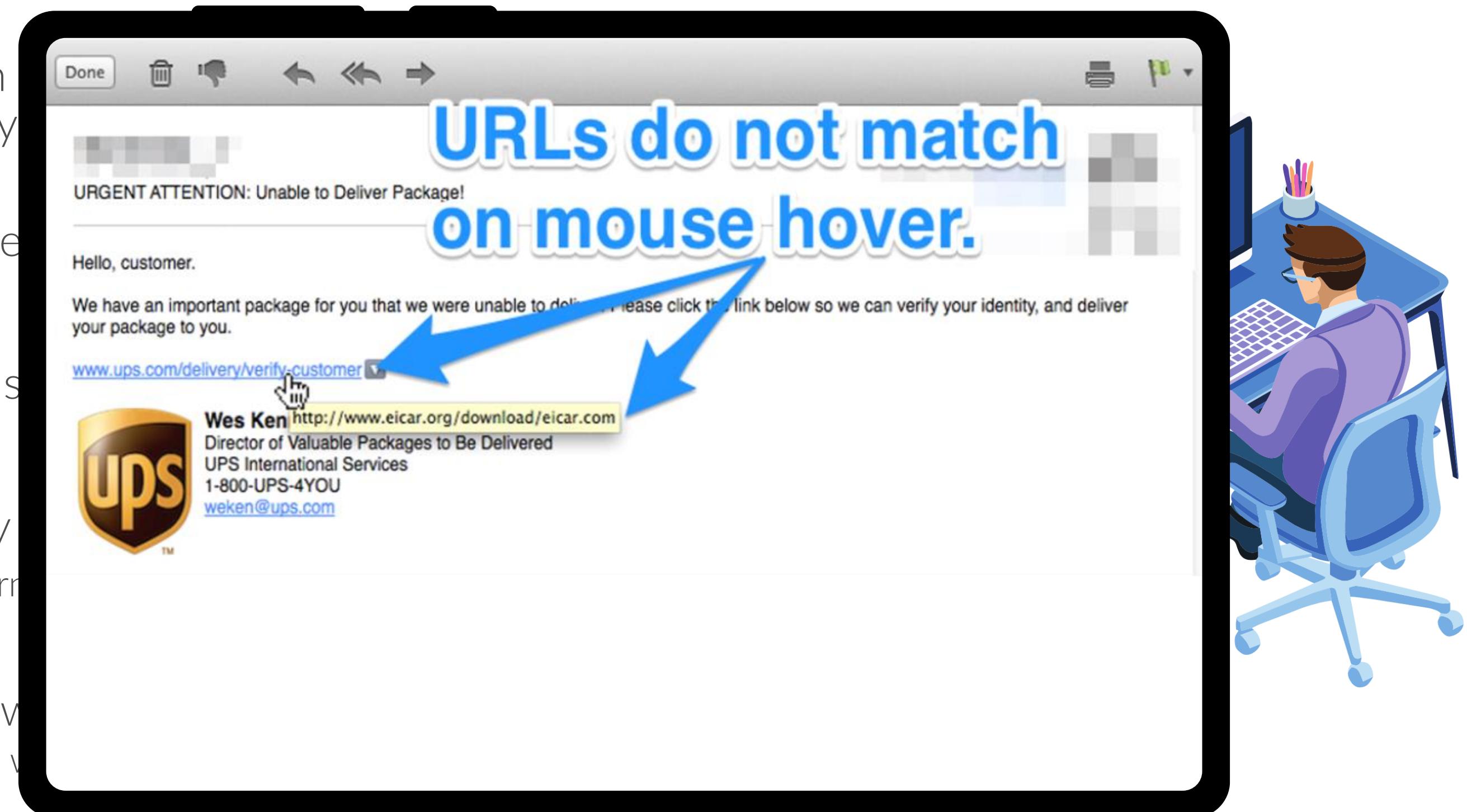
- 01 Only install apps from the official app store
- 02 If you log in, make sure the URL starts with https://
- 03 Trust only sites with a green padlock in the address bar
- 04 Look for information on the company's website

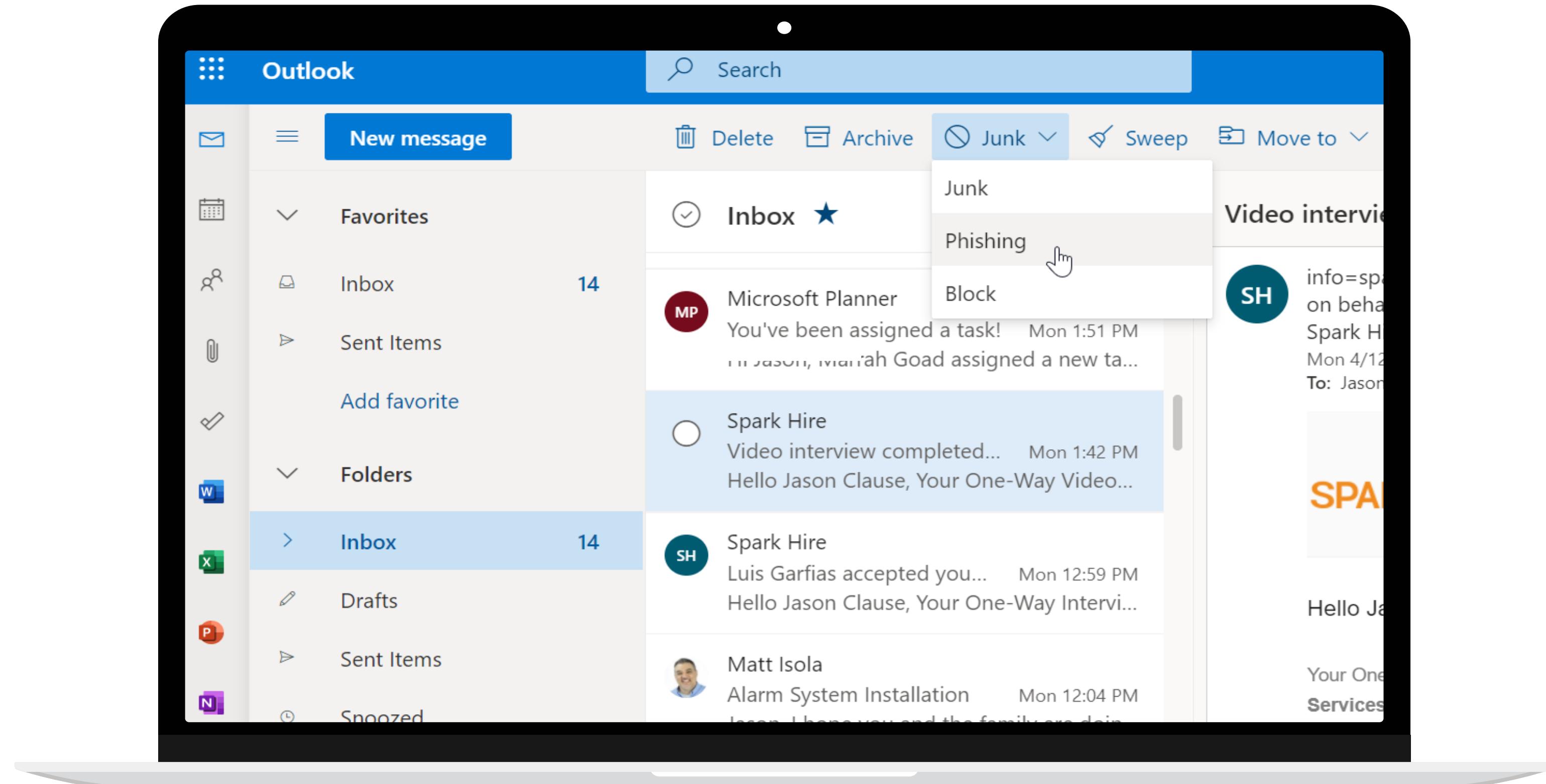


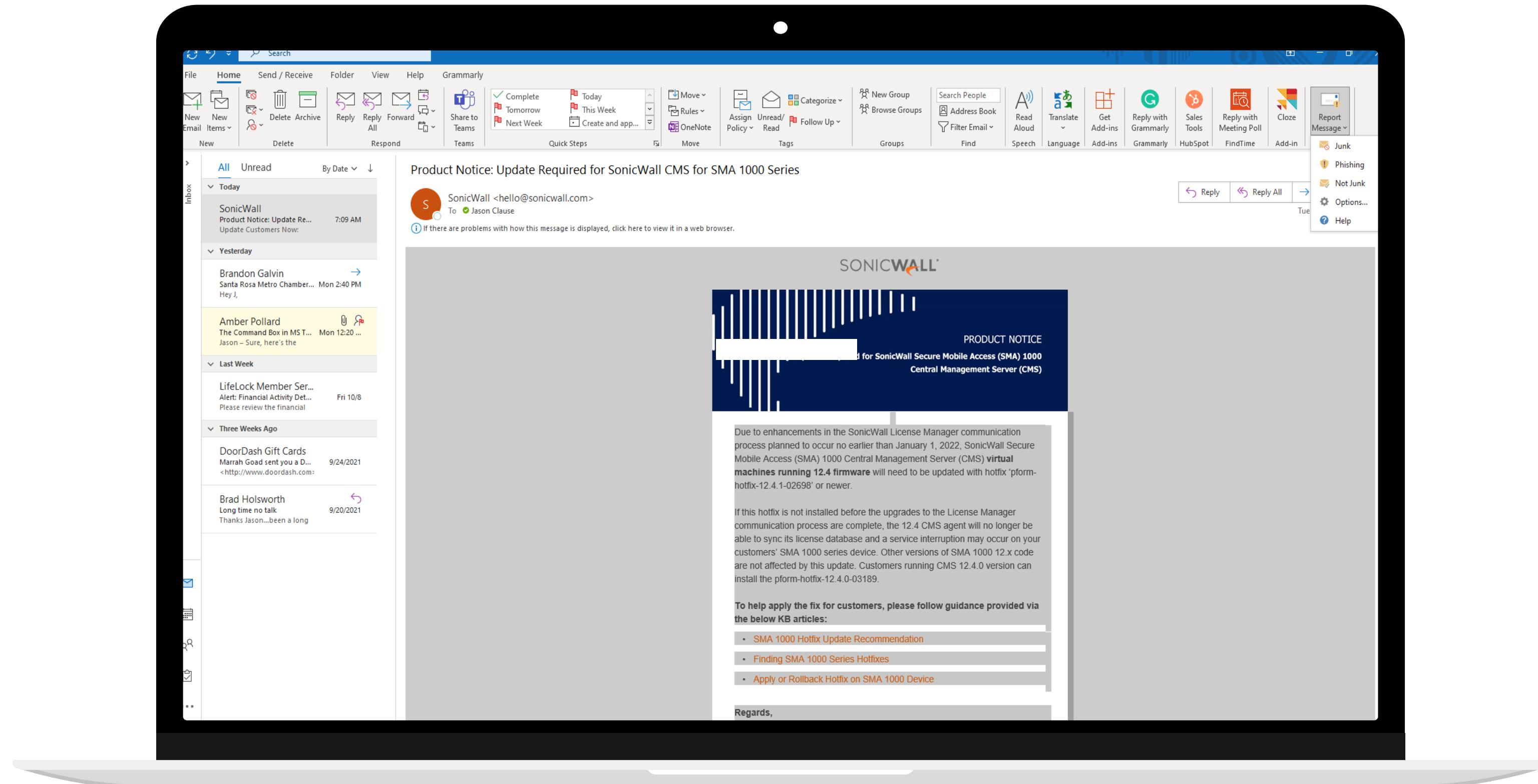


EVIL EMAIL

- 01 Don't open certain they
- 02 If you suspect
- 03 Check the s
- 04 Read every
bob.smith@grr
- 05 Do not forward
(hover over it v)







Email Encryption

01

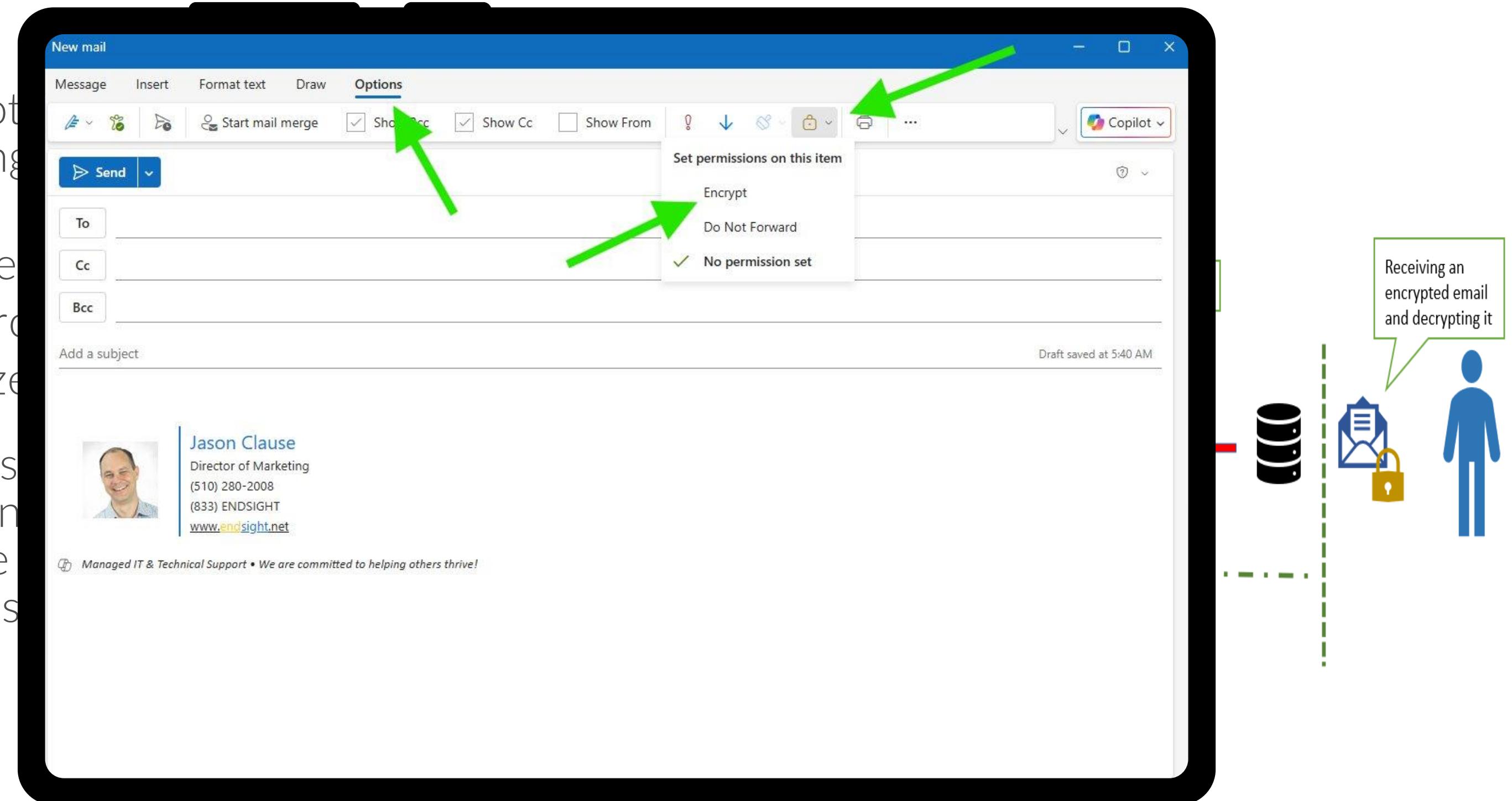
Email is not transmitting

02

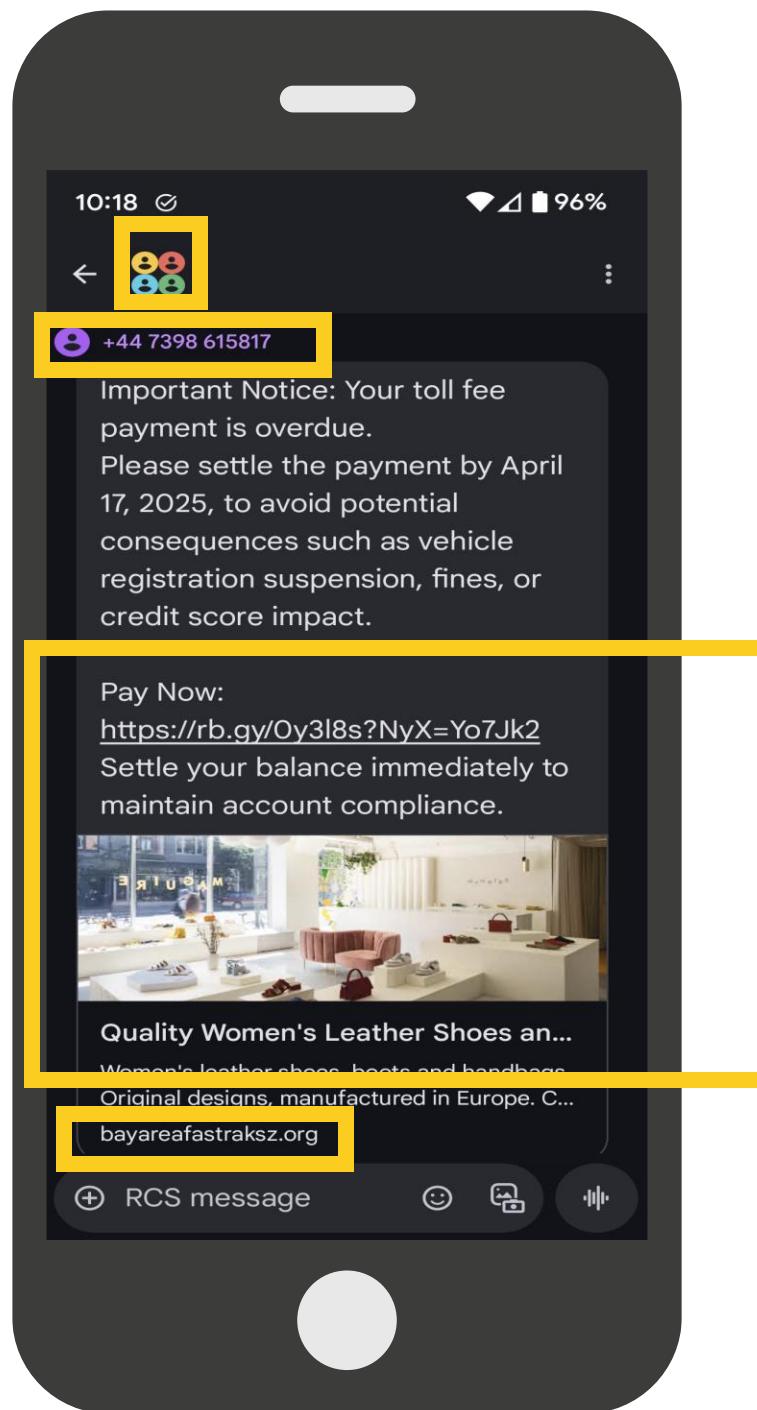
Protects sensitive information from being intercepted by unauthorized users

03

Businesses and sensitive institutions in healthcare, finance, and other industries



Look Closely



What's wrong with
this text message?

PERSONAL HABITS (I.T. life hacks)

- 01 Always use a lock screen/password on your smartphone
- 02 Only give out personal or sensitive data on phone calls you've initiated
- 03 Invest in Identity Theft protection of some kind
- 04 Invest in a password manager











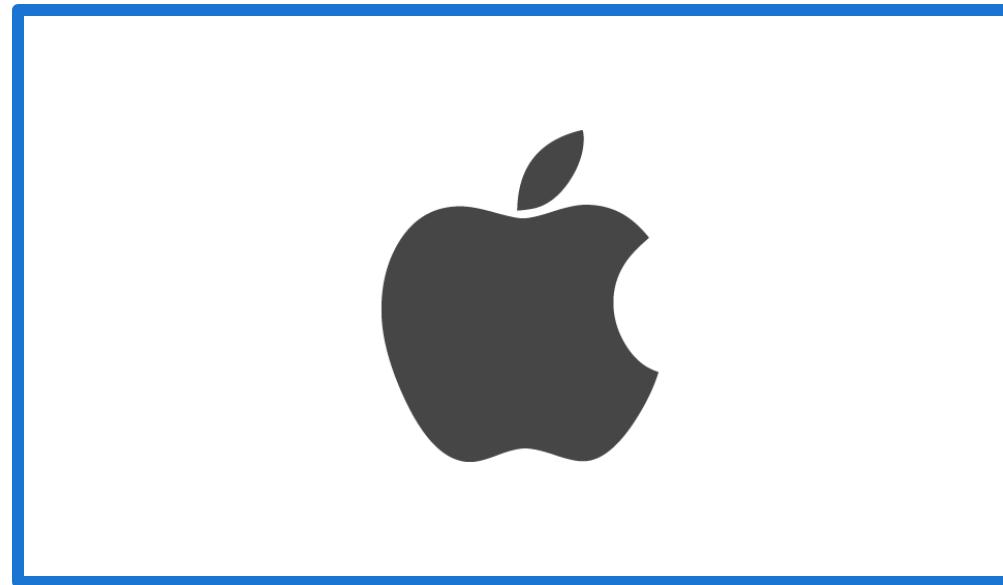
???



Everyone and everything online is a stranger.

Always be suspicious of strangers!

What do these brands have in common?



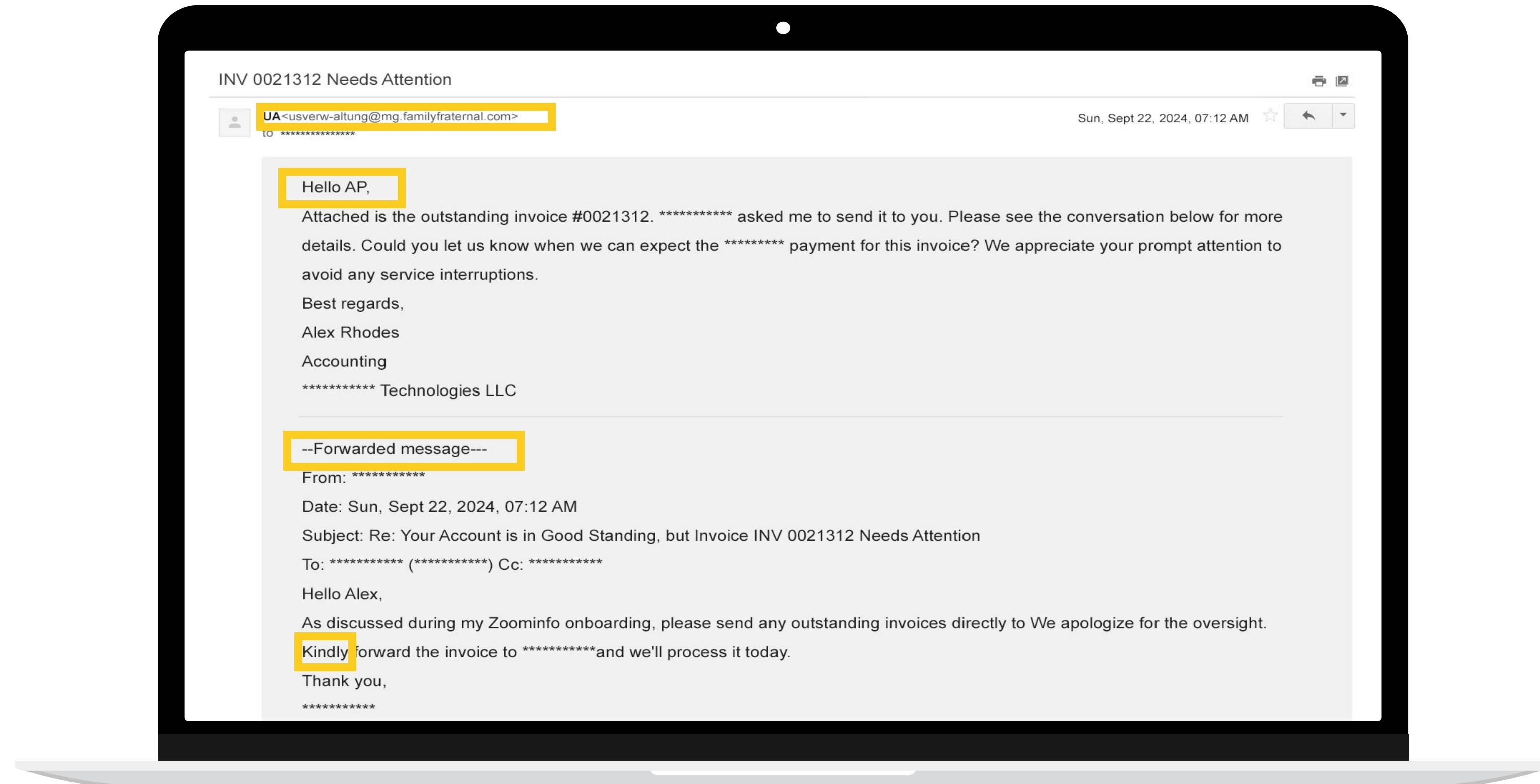
3 Most Spoofed Brands in Phishing Attacks

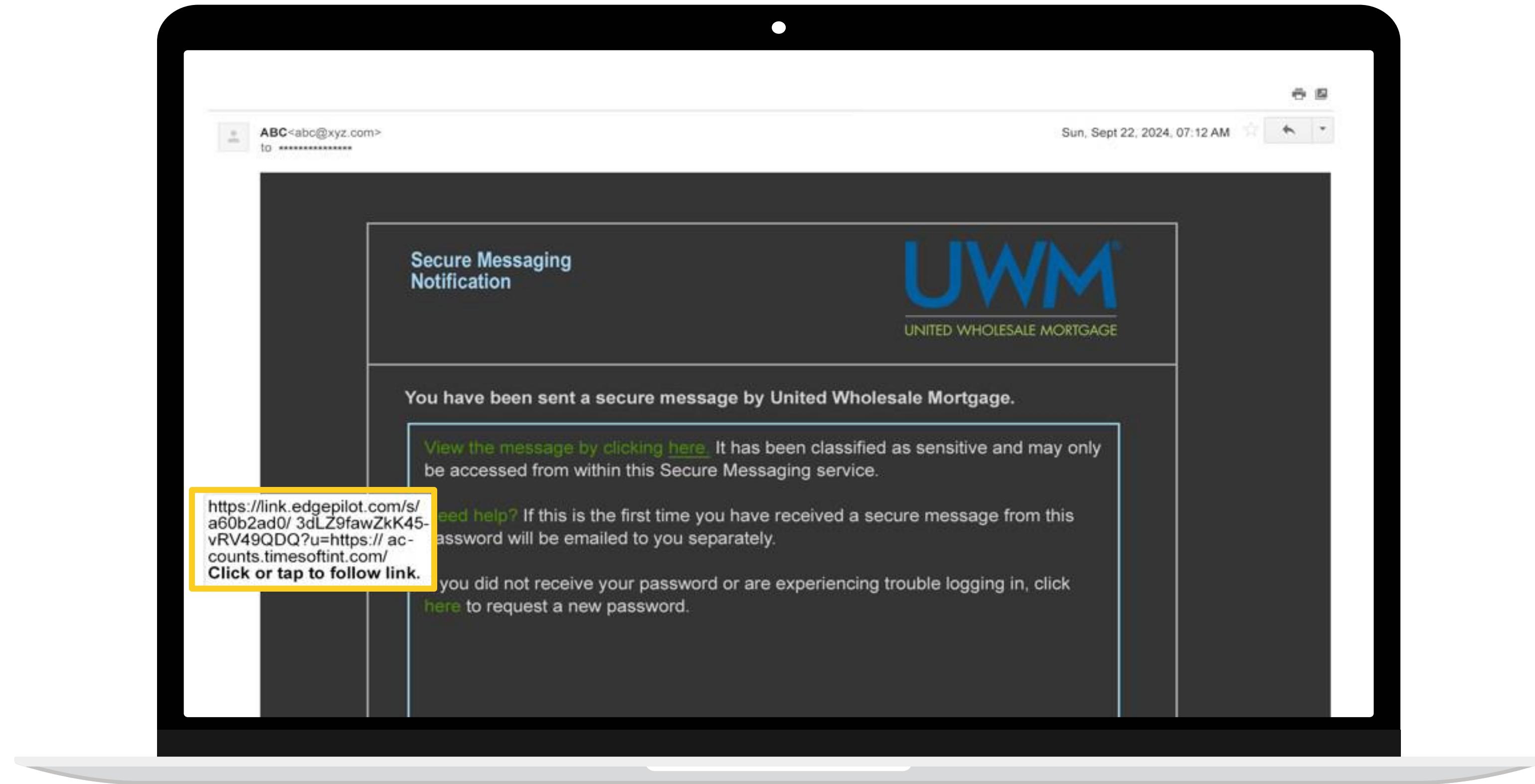
Things That Will Never Happen

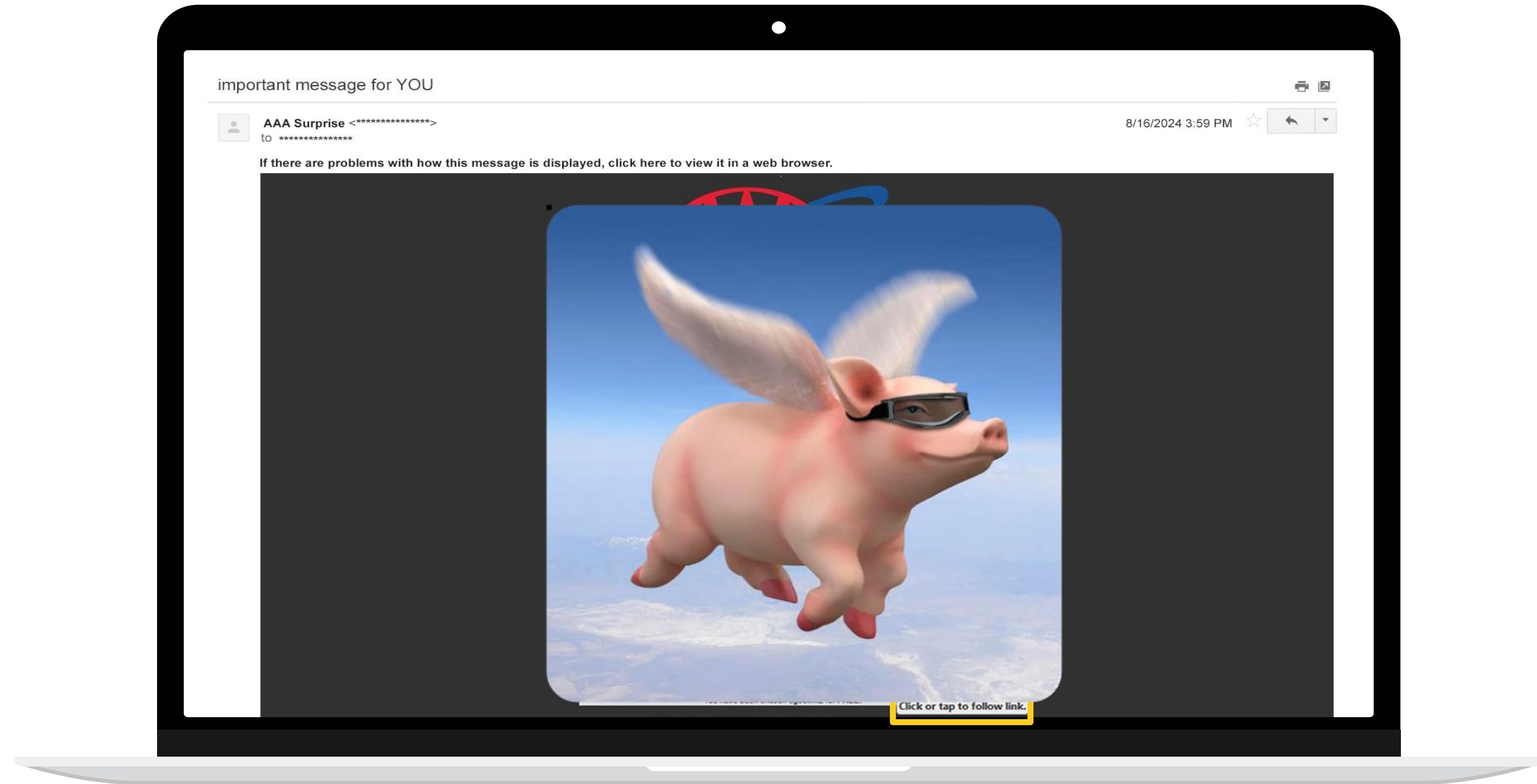
- Amazon is refusing to do business if you don't 'update your account'.
- Microsoft calling to help with your computer (yes, this call really happened)
- I'm not getting arrested in Thailand (yes, this call really happened)
- You didn't win a prize
- Nobody lost a puppy
- We haven't changed the parking rules
- Nobody needs your gift cards!

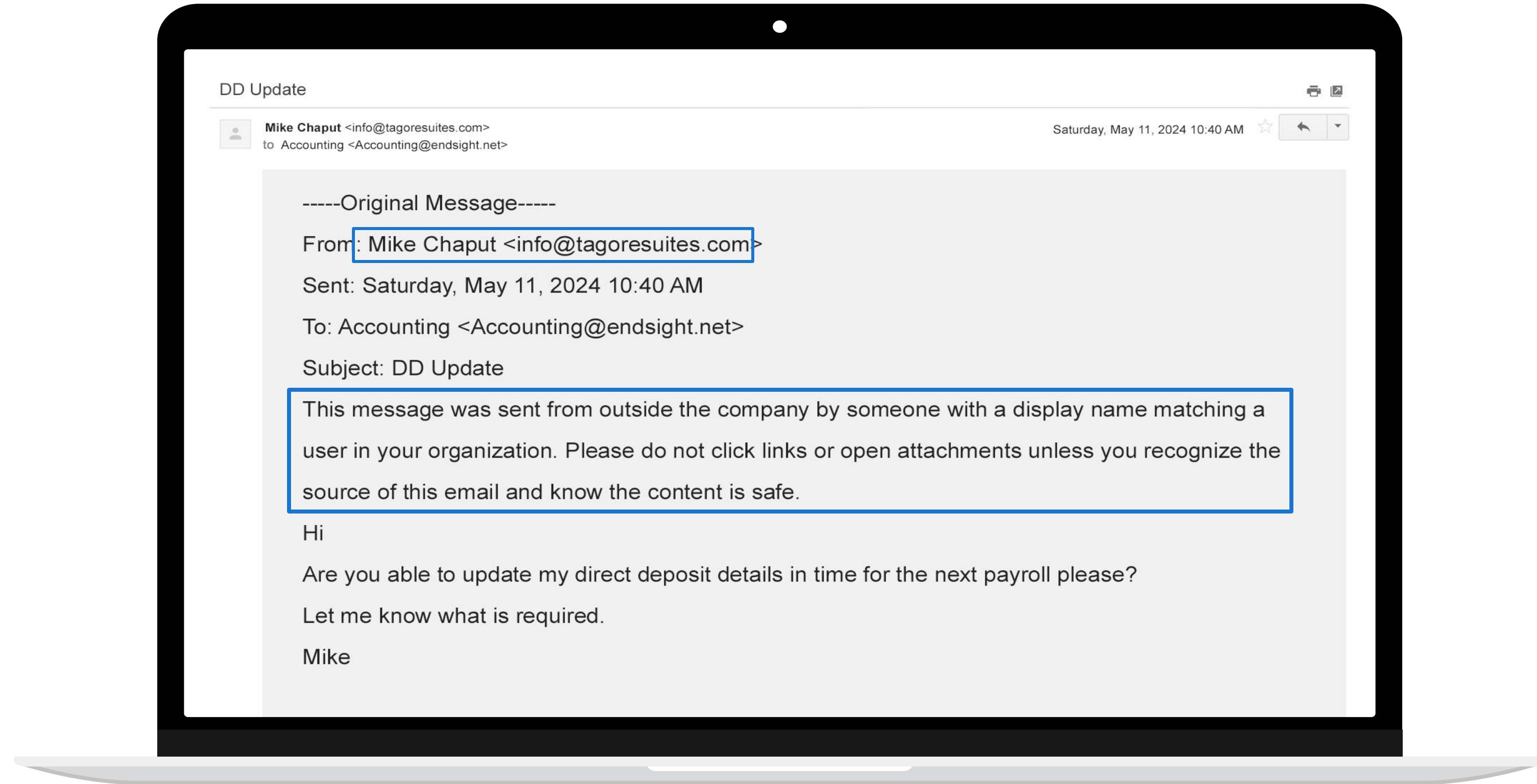


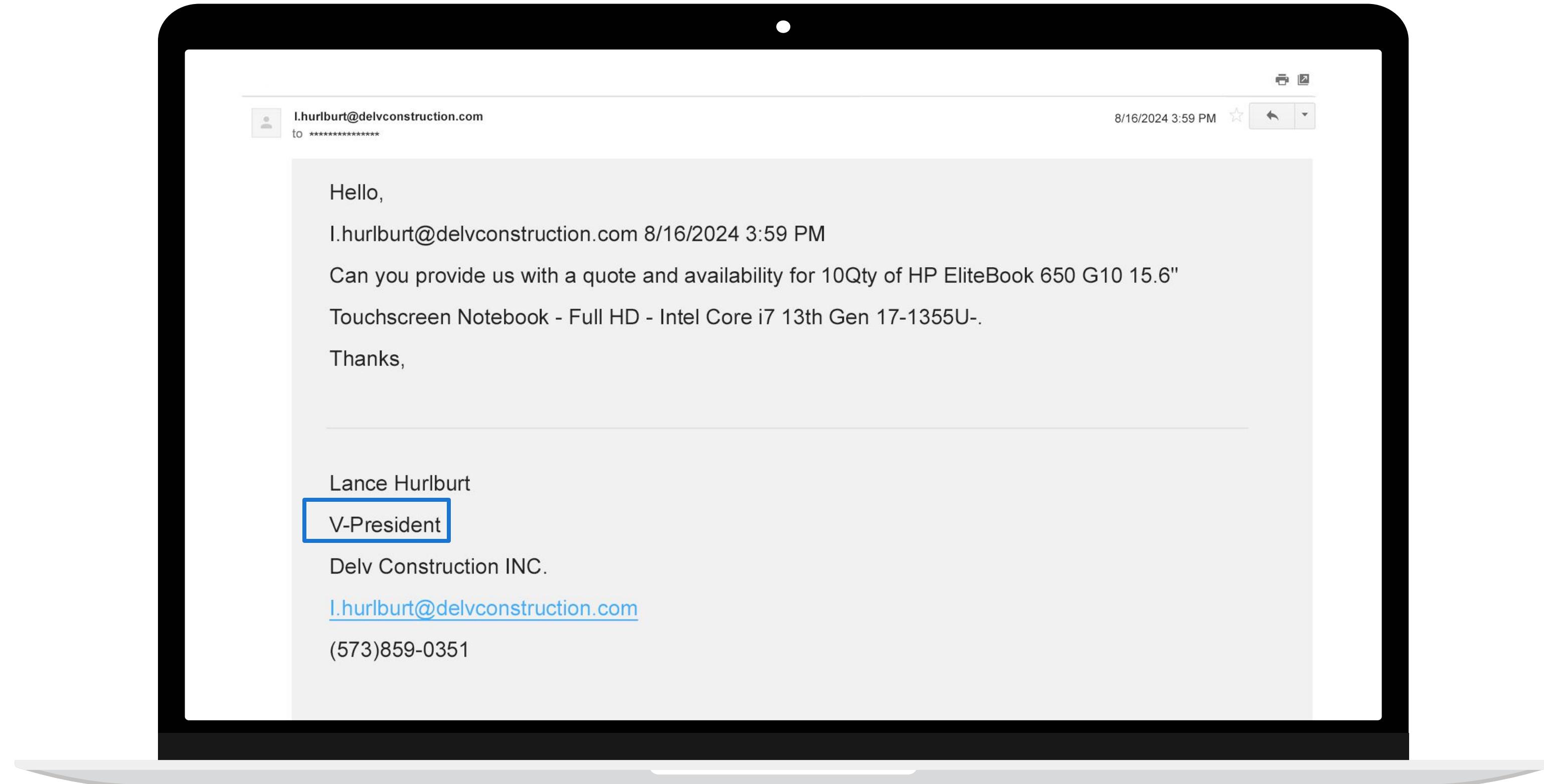
Phishing Examples

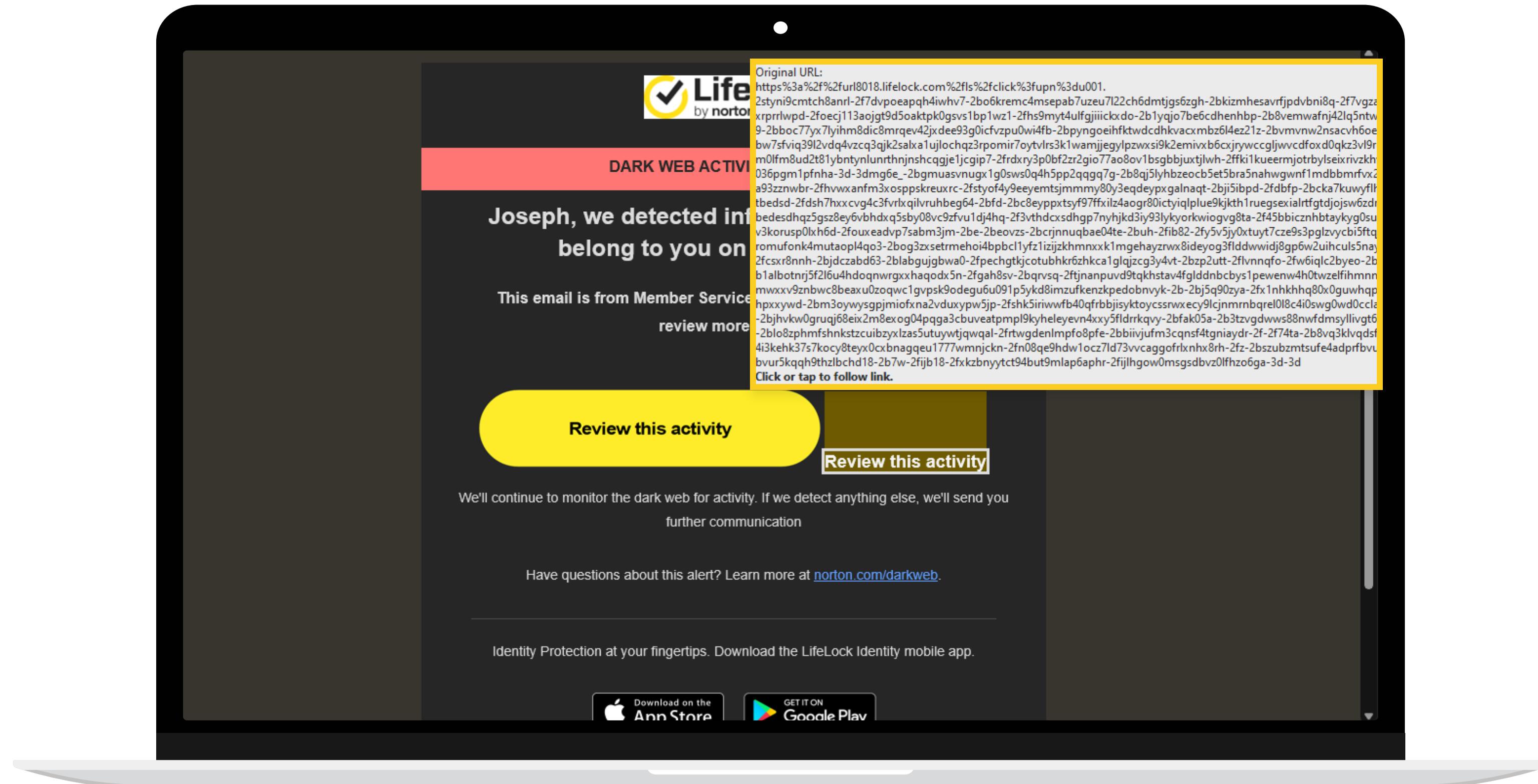




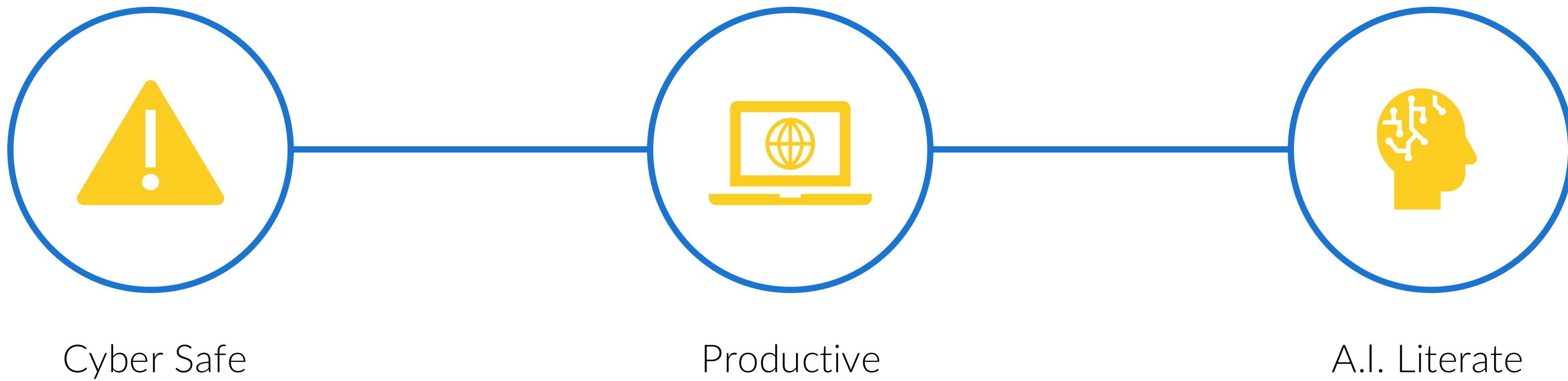






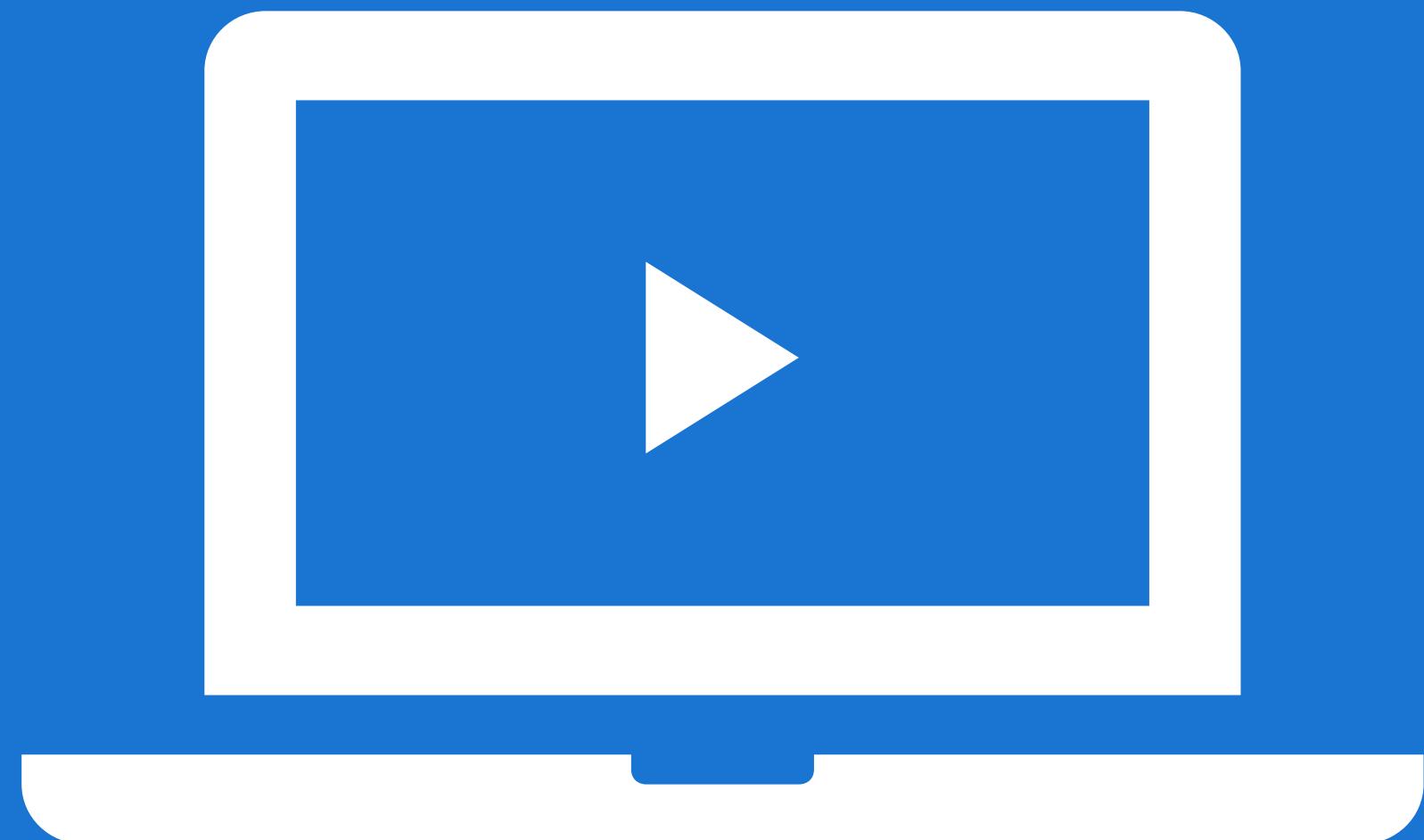


A Weekly Habit To Keep You Off the Breach List



365 Tip of The Week

1 Cyber Security Habit | 1 Microsoft 365 Tip | 1 A.I. Tip
Every Week.



www.endsight.net/365

Ethics and Compliance

Attacks on Lawyers are at an all time high

- In the first 5 months of 2023, 21 Law Firms reported breaches to state attorneys.
 - In all of 2022 there were 28
 - This was only Law Firms that reported it.
- The American Bar Association's 2023 Cybersecurity TechReport revealed that 29% of law firms experienced a cybersecurity vulnerability.
 - Note: A cybersecurity vulnerability is not the same as a breach. This also includes smaller incidents, like a stolen work laptop.
- The legal sector is the fourth most targeted sector by cybercriminals.



Attacks on Lawyers are at an all time high

- In 2025, seven California law firms reported data breaches to the California Attorney General.
 - This reflects only law firms that publicly reported incidents.
- A 2025 survey reported by Law.com found that 20% of U.S. law firms were targeted by cyberattacks in the past year.
- The legal sector consistently ranks among the top ten most targeted industries by cybercriminals.



Why are Lawyers Prime Targets for Hackers?

- Access to confidential client data.
 - Gateway to valuable targets
- Wealth of negotiation and litigation information.
- Smaller firms/businesses are believed to have a lack of advanced cybersecurity.
- Law Firms can't risk their reputation.
 - Gives hackers leverage to negotiate with the firm to prevent a leak.
- Lawyers are extremely busy and focused on legal work.
 - The busier you are the more likely you are to speed through things making it easier for hackers to trick you.



Notable Legal Breaches

Grubman Shire Meiselas & Sacks
around 70 employees



- Entertainment Law Firm (with A-Listers as clients) that experienced a ransomware attack.
- Hackers demanded \$42 million; the firm did not pay it.

Hastings, Cohan & Walsh, LLP
around 10 employees



- Real-estate law firm in Connecticut. One of their clients received a fraudulent email from them asking for a \$600,000 wire transfer.
- Alleged that hackers breached the firm's email system.

Bryan Cave Leighton Paisner
around 1,200 employees



- Law firm used by major conglomerate Mondelez that experienced a data breach.



Hackers don't care
about you.

They only care about money.

Ethical Considerations

- Duty of client confidentiality.
- Inform clients of risk.
 - The communication and software platforms you use can be vulnerable.
 - Clear billing directions, your clients might get an email that looks like it's coming from you but isn't.
- Collect only necessary data.
- Have a written, tested incident response plan



California Rules of Professional Conduct

- Lawyers must take reasonable measures to safeguard confidential client information when using technology to transmit or store it. [Duty of Confidentiality \(Rule 1.6; Business & Professions Code § 6068\(e\)\)](#).
- Lawyers must take steps to secure devices and systems containing confidential client data, conduct inquiries after a breach, and notify affected clients if their interests may be harmed. [Data Breaches & Notification \(Formal Opinion No. 2020-203\)](#)
- Lawyers are not technologists. If they do not understand, they are required to communicate with an expert. [Ethical Duties in Handling of Discovery of Electronically Stored Information \(Formal Opinion No. 2015-193\)](#)
- For remote practice, attorneys must implement security measures such as:
[Duties When Working Remotely \(Formal Opinion 20-004\)](#)
 - Two-factor authentication
 - Strong passwords and auto-logoff
 - Secure storage and disposal of physical and electronic files
 - Limiting access from other household users and disabling listening devices at home unless needed
- They should also counsel clients to take similar precautions when communicating remotely.
[Duties When Working Remotely \(Formal Opinion 20-004\)](#)



California Rules of Professional Conduct (Links)

These QR codes provide
direct access to the
source materials
referenced on the
previous slide.



Rule 1.6



2020-203

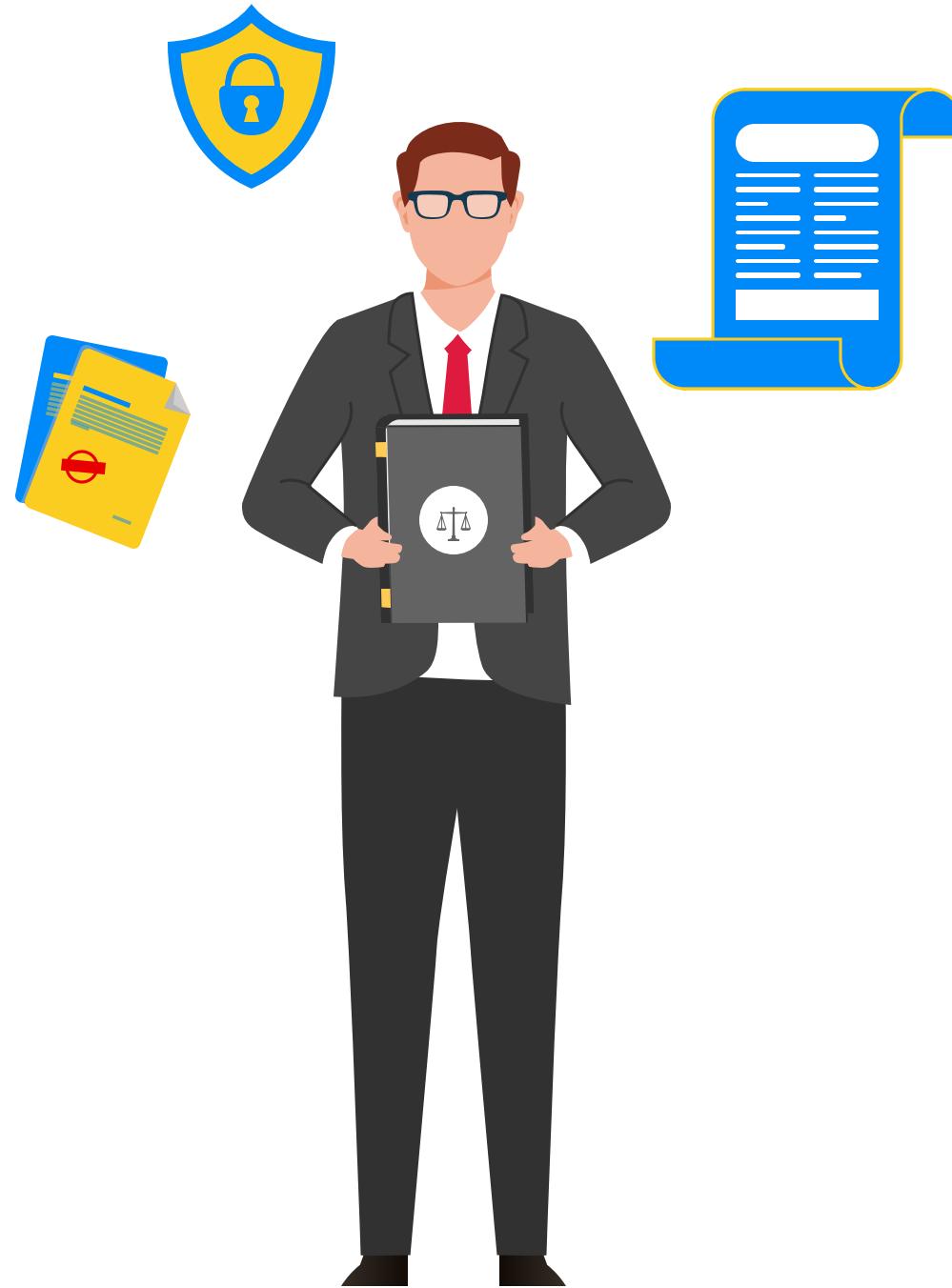


2015-193



20-004

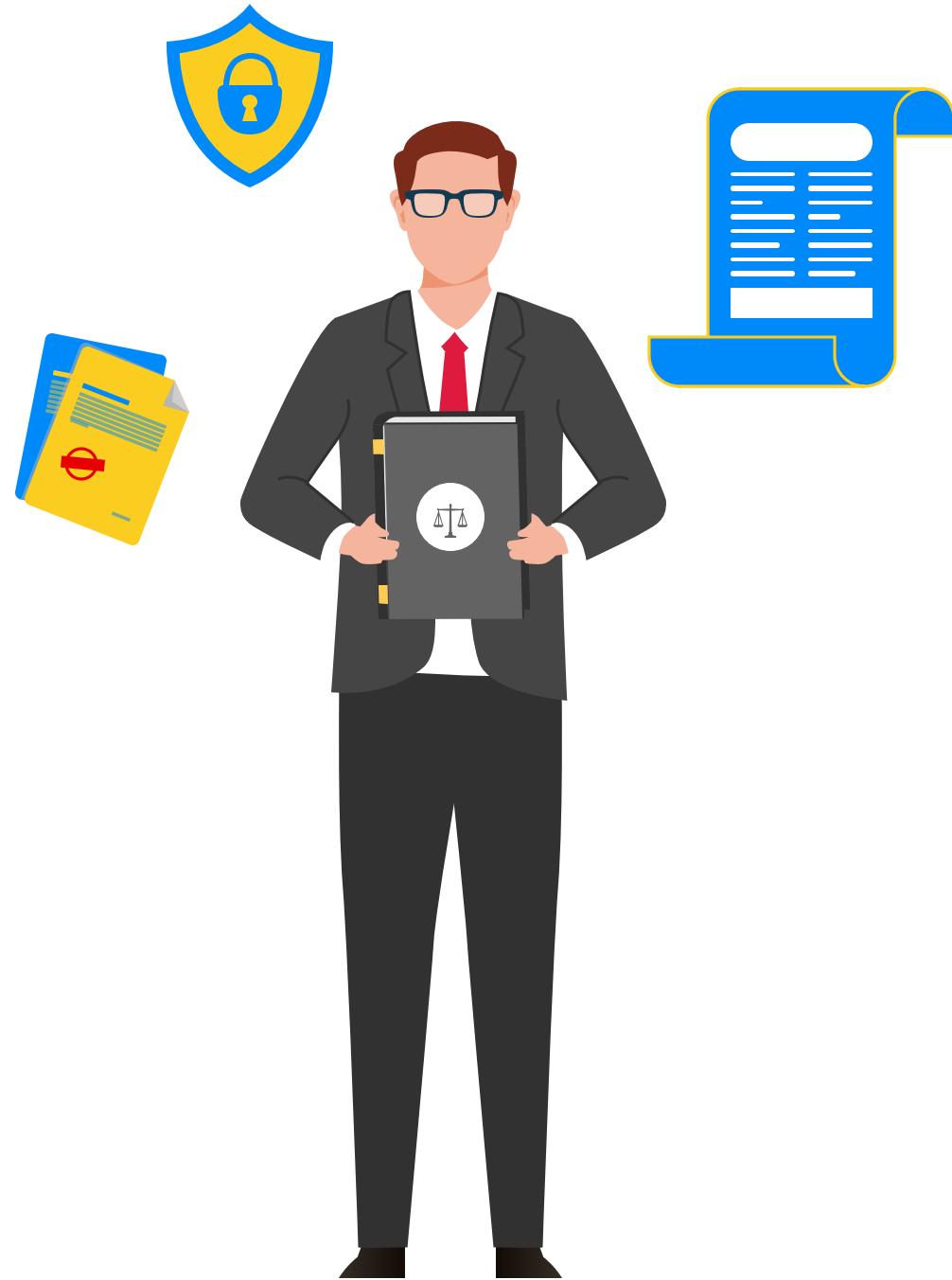
Formal Opinion 477R



- Provides guidance for lawyers on their ethical obligations to protect client confidentiality when using electronic communication. It is a revision of a previous opinion to address the evolving cybersecurity landscape.

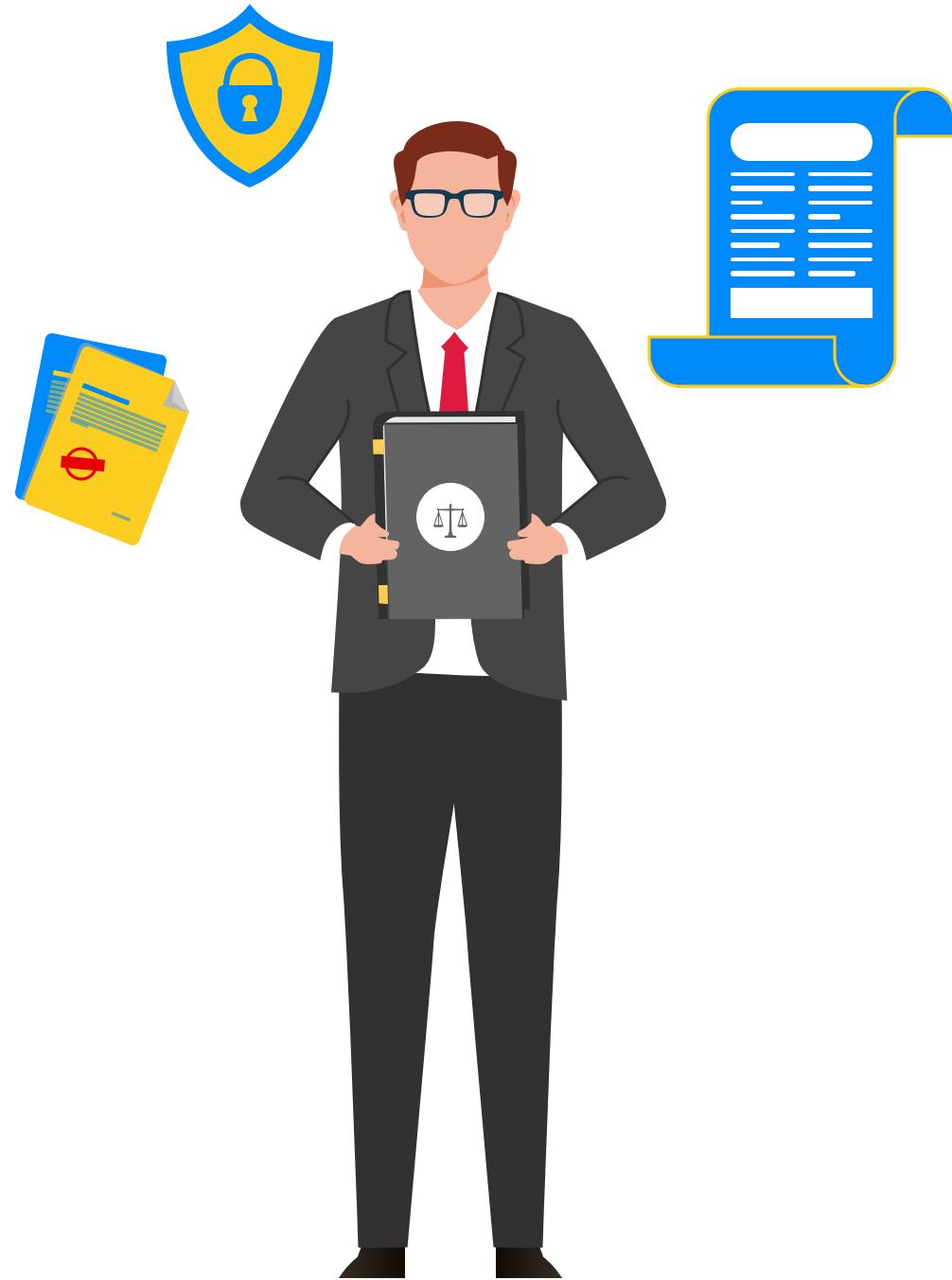
*Link available in the Resources section on the recording page.

Formal Opinion 477R Takeaways (Part 1)



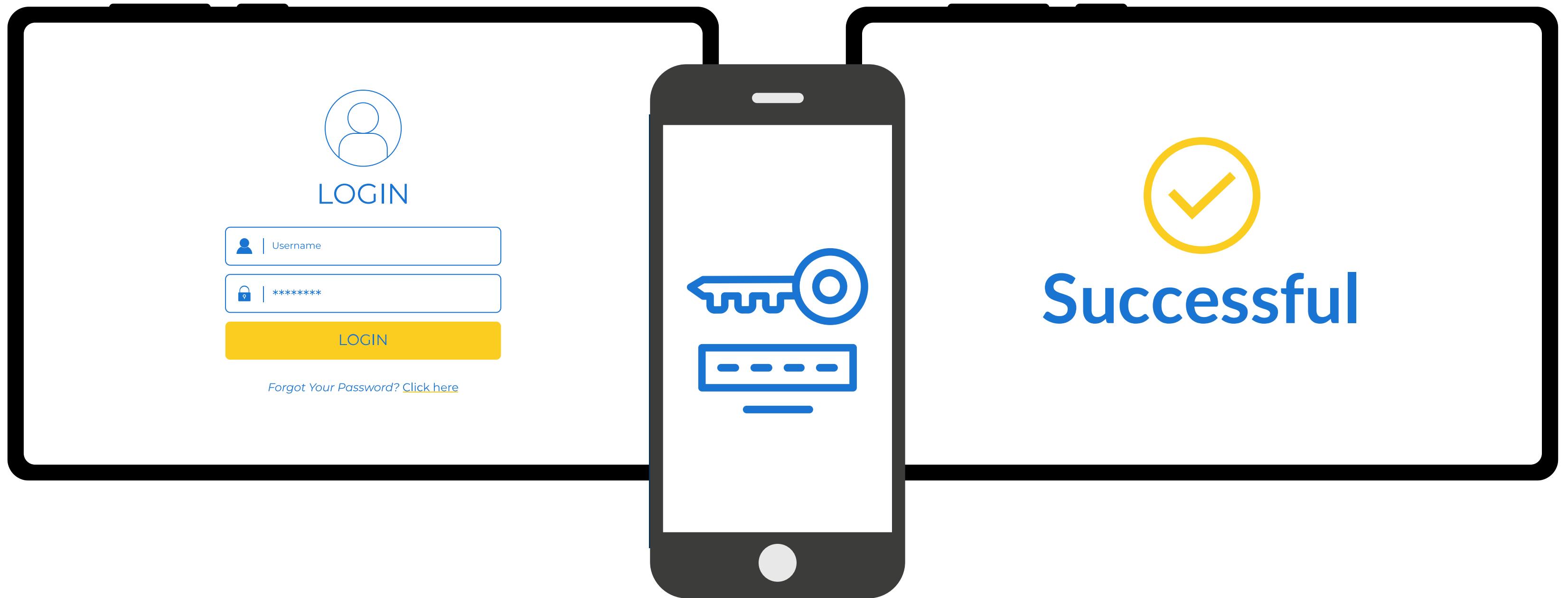
- Duty to Safeguard Client Information.
 - Lawyers have an ethical obligation under Model Rule 1.6 to take reasonable steps to prevent unauthorized access to client information, including in electronic communications.
- Reasonable Efforts Standard.
 - The opinion emphasizes that what constitutes "reasonable efforts" depends on several factors.
- Risk Assessment.
 - Lawyers are advised to conduct a risk assessment to determine the appropriate level of protection for client communications. This includes considering the type of technology used, potential risks, and mitigation strategies.

Formal Opinion 477R Takeaways (Part 2)



- Enhanced Security Measures
 - When dealing with highly sensitive information, lawyers may need to implement enhanced security measures.
- Client Communication and Consent
 - Lawyers should discuss confidentiality risks with clients and obtain consent when using less secure communication methods, particularly when sensitive information is involved.
- Third-Party Service Providers
 - If a lawyer uses third-party services, such as cloud storage, they must ensure these providers adhere to strong security protocols to protect client information.
- Continuous Monitoring
 - The opinion encourages lawyers to stay informed about evolving cybersecurity threats and regularly update their practices to address new risks.

Recap & Resources



Dictionary

Search for a word



sus·pi·cion

/səˈspiSHən/

noun

1. a feeling or thought that something is possible, likely, or true.
"she had a sneaking **suspicion** that he was laughing at her"

Similar:

intuition

feeling

impression

inkling

surmise

guess



2. cautious distrust.

"her activities were regarded with suspicion by the headmistress"

Similar:

misgiving

doubt

qualm

wariness

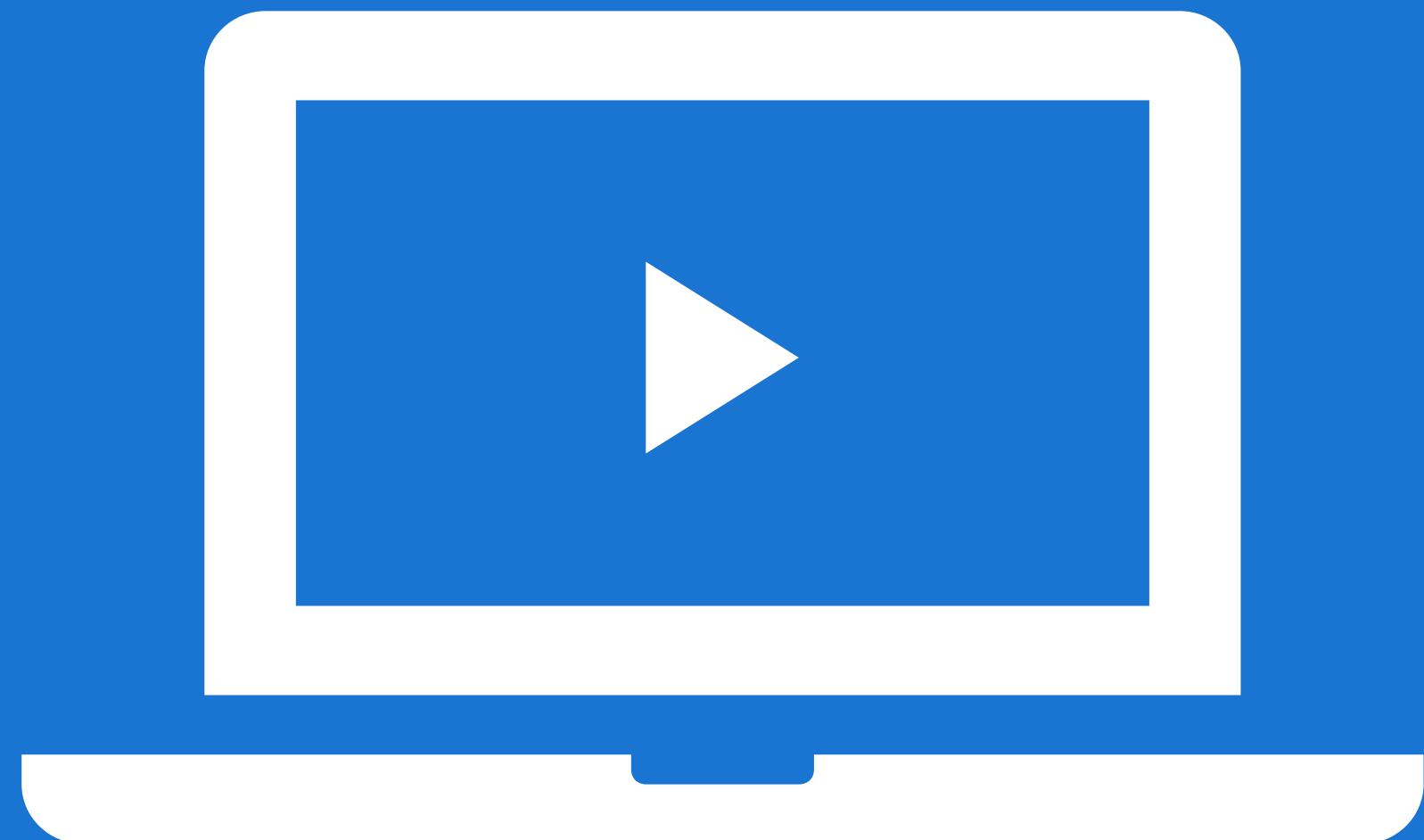
chariness

reservation



365 Tip of The Week

1 Cyber Security Habit | 1 Microsoft 365 Tip | 1 A.I. Tip
Every Week.



www.endsight.net/365

Thank you!

endsight 