OSB Professional Liability Fund presents

How Law Firms Get Hacked (And What You Can Do About It)

Tuesday, April 9th, 2024
2:00 pm – 3:00 pm

MCLE ID 108831
1 Practical Skills Credit

Speakers: Sherri Davidoff
Founder and Chief Executive Officer
LMG Security

Sean Hoar
Partner - Cybersecurity & Data Privacy Chair
Constangy, Brooks, Smith & Prophete LLP

OSB Professional Liability Fund

CLE Materials

- Speakers’ Biographies
- PowerPoint Slides
- Additional Resources

Speaker Biographies

Sherri Davidoff

Sherri Davidoff is the CEO of LMG Security and the author of three books, including “Ransomware and Cyber Extortion” and “Data Breaches: Crisis and Opportunity.” As a recognized expert in cybersecurity, she has been called a “security badass” by the New York Times. Sherri has been featured as the protagonist in the book, *Breaking and Entering: The Extraordinary Story of a Hacker Called “Alien.”* She is a GIAC-certified forensic examiner (GCFA) and penetration tester (GPEN) and received her degree in Computer Science and Electrical Engineering from MIT.

Sean Hoar

Sean Hoar is the Chair of the Cybersecurity & Data Privacy Team at Constangy, Brooks, Smith & Prophete LLP. He is a former cyber attorney for the U.S. Dept. of Justice and received multiple honors for his work with the FBI and Secret Service in prosecuting cybercrime. He now manages a 70-member national team that manage responses to over 2,000 data breeches a year, and has been named by the Cybersecurity Docket as one of the best and brightest data breach response lawyers in the United States. He is a certified Global Information Security Professional (GISP), a Certified Information Systems Security Professional (CISSP), and a Certified Information Privacy Professional for U.S. law (CIPP/US).

How Attorneys Get Hacked

(And What You Can Do About It)

Sean Hoar
Chair & Partner

Sherri Davidoff
CEO

CONSTANGY BROOKS, SMITH & PROPHETE LLP

LMG SECURITY

1

Today's Speakers

Sherri Davidoff

Founder & CEO, LMG Security

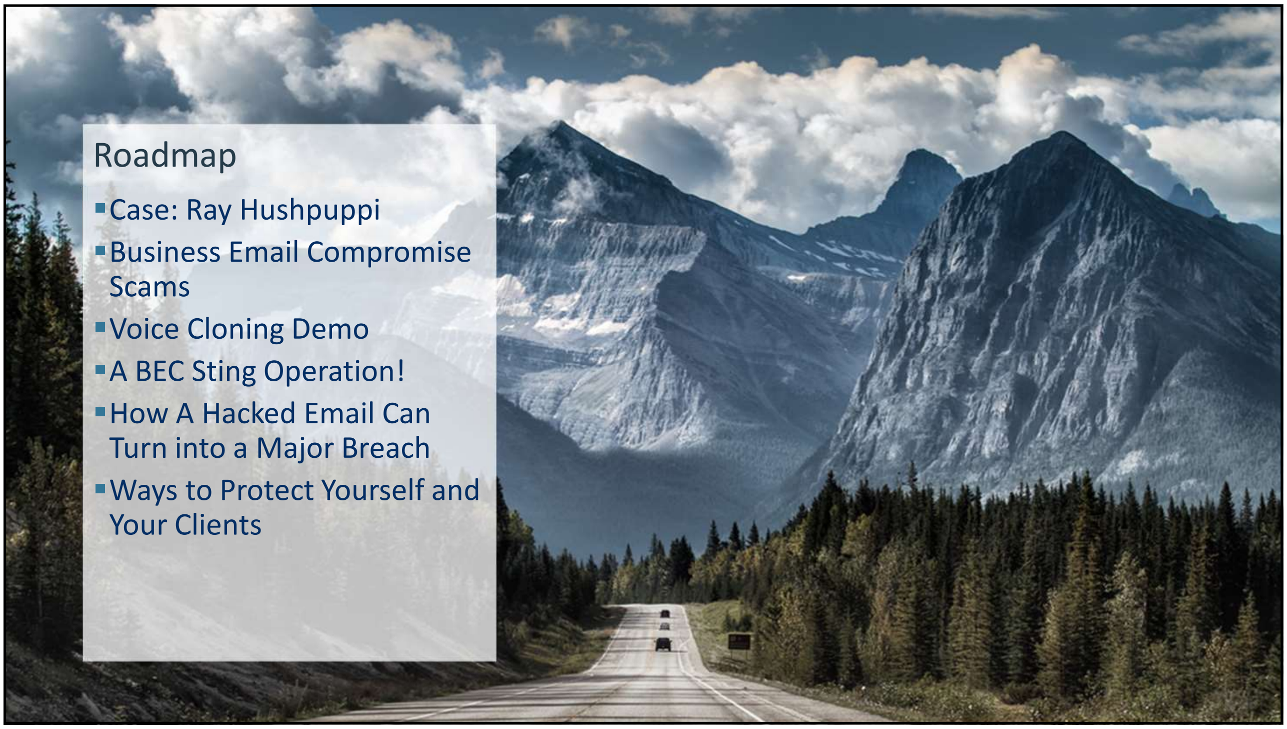
MIT EE/CS, GCFA, GPEN

Sean Hoar

Partner & Chair, Cybersecurity & Data Privacy Team

Constangy, Brooks, Smith & Prophete, LLP

2

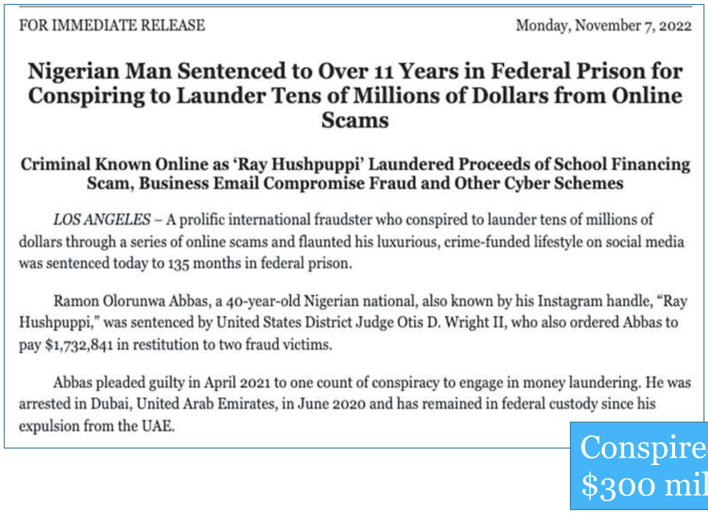


Roadmap

- Case: Ray Hushpuppi
- Business Email Compromise Scams
- Voice Cloning Demo
- A BEC Sting Operation!
- How A Hacked Email Can Turn into a Major Breach
- Ways to Protect Yourself and Your Clients

3

Ray Hushpuppi Sentenced!



FOR IMMEDIATE RELEASE Monday, November 7, 2022

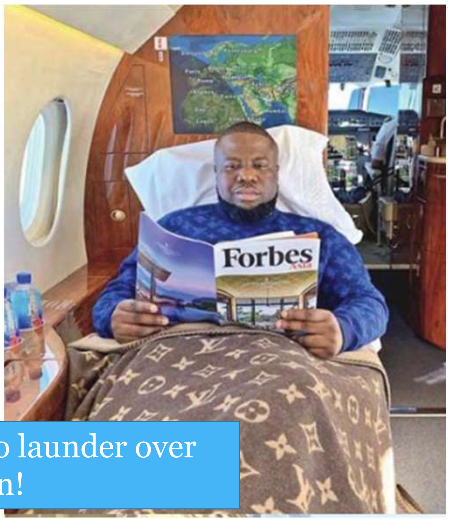
Nigerian Man Sentenced to Over 11 Years in Federal Prison for Conspiring to Launder Tens of Millions of Dollars from Online Scams

Criminal Known Online as 'Ray Hushpuppi' Laundered Proceeds of School Financing Scam, Business Email Compromise Fraud and Other Cyber Schemes

LOS ANGELES – A prolific international fraudster who conspired to launder tens of millions of dollars through a series of online scams and flaunted his luxurious, crime-funded lifestyle on social media was sentenced today to 135 months in federal prison.

Ramon Olorunwa Abbas, a 40-year-old Nigerian national, also known by his Instagram handle, "Ray Hushpuppi," was sentenced by United States District Judge Otis D. Wright II, who also ordered Abbas to pay $1,732,841 in restitution to two fraud victims.

Abbas pleaded guilty in April 2021 to one count of conspiracy to engage in money laundering. He was arrested in Dubai, United Arab Emirates, in June 2020 and has remained in federal custody since his expulsion from the UAE.



Conspired to launder over $300 million!

4

Case Study: Hushpuppi Scams a NY Law Firm

- Victim 1: NY Law Firm
- Transferred $922,857 to an account controlled by the criminals
- Represented a client who was refinancing a property w. Citizens Bank
- Paralegal sent verification email to a scam address that looked like Citizens Bank
- Law firm policy – must be sent to firm "by fax and followed-up by a phone call"

"Ramon Abbas, a.k.a. 'Hushpuppi,' targeted both American and international victims, becoming one of the most prolific money launderers in the world," said Don Alway, the Assistant Director in Charge of the FBI's Los Angeles Field Office.

5

Case Study: Hushpuppi Scams a Law Firm

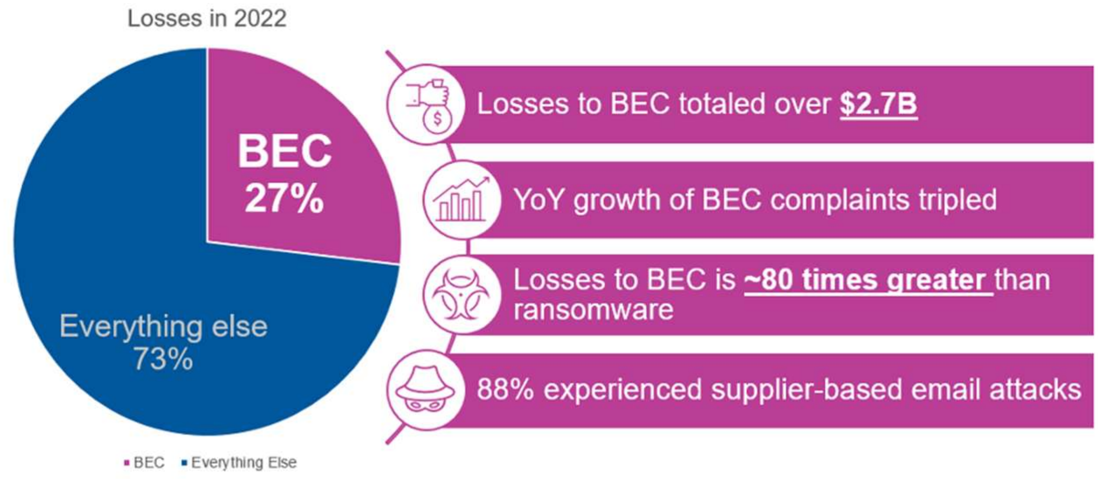
- Paralegal follows the process!
  - Receives a fax in response w/ fraudulent wire instructions
  - Calls the number on the fax to verify (oops!)
- Wire transfer - $922,857
- Not discovered until much later
- No funds recovered

6

Model Rules of Professional Conduct

- ABA Formal Opinion 483
  - Issued October 17, 2018
  - **Duty of confidentiality (Oregon RPC 1.6)**
  - **Duty of competence** to develop an understanding of relevant technology **(RPC 1.1)**
  - **Obligation to monitor digital infrastructure** on which confidential client information resides
  - **Obligation to act reasonably and promptly** to contain and mitigate the adverse effects of the breach
  - **Obligation to conduct reasonable assessment** of what occurred
  - **Obligation to provide notice** of data breach
    - Current clients
    - Former clients

Business Email Compromise is on the Rise



Losses to BEC totaled over **$2.7B**

YoY growth of BEC complaints tripled

Losses to BEC is **~80 times greater** than ransomware

88% experienced supplier-based email attacks

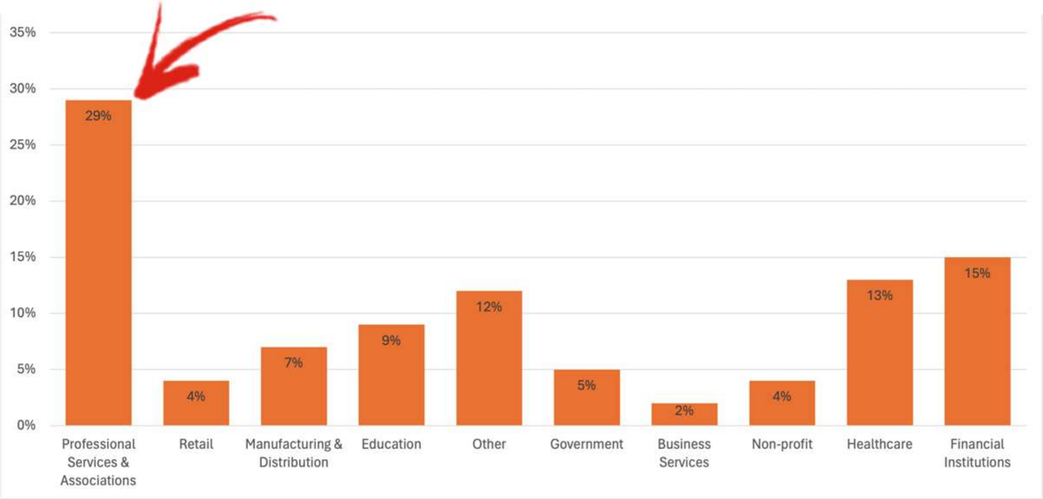
Image: https://www.proofpoint.com/us/blog/email-and-cloud-threats/fbis-ic3-report-financial-losses-email-fraud-increased-nearly-50-just

What is Business Email Compromise?

- Criminals steal money
- Typically leverage hacked email accounts
- Monitor communications
- Look for scam opportunities
- Send a carefully crafted spoofed or hacked email to trick recipients into transferring funds

9

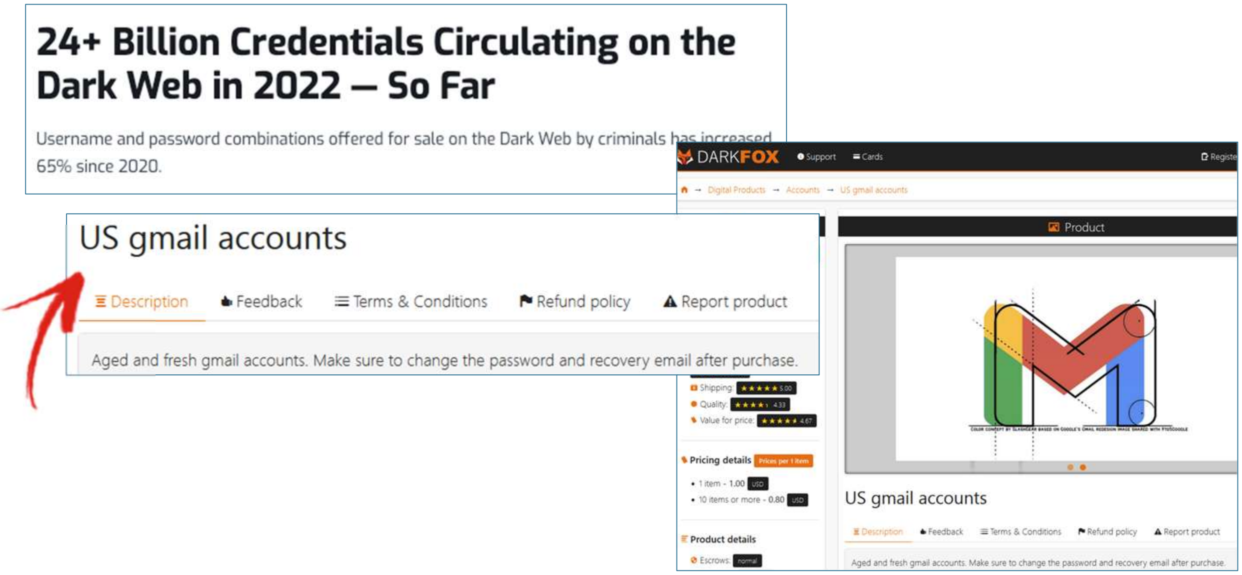
Attorneys Are Targeted



Business Email Compromise Incidents, 2023 – Beazley Insurance
https://www.beazley.com/en-US/cyber-services-snapshot/2024-cyber-risk-predictions/latest-trends/

10

It’s Easy to Break Into Email Accounts



24+ Billion Credentials Circulating on the Dark Web in 2022 – So Far

Username and password combinations offered for sale on the Dark Web by criminals has increased 65% since 2020.

DARKFOX · Support · Cards · Registe

Digital Products → Accounts → US gmail accounts

Product

US gmail accounts

≣ Description · Feedback · ≡ Terms & Conditions · ⚑ Refund policy · ⚠ Report product

Aged and fresh gmail accounts. Make sure to change the password and recovery email after purchase.

Shipping: ★★★★★ 5.00

Quality: ★★★★ 4.33

Value for price: ★★★★★ 4.67

Pricing details · Prices per 1 item

- 1 item - 1.00 USD
- 10 items or more - 0.80 USD

Product details

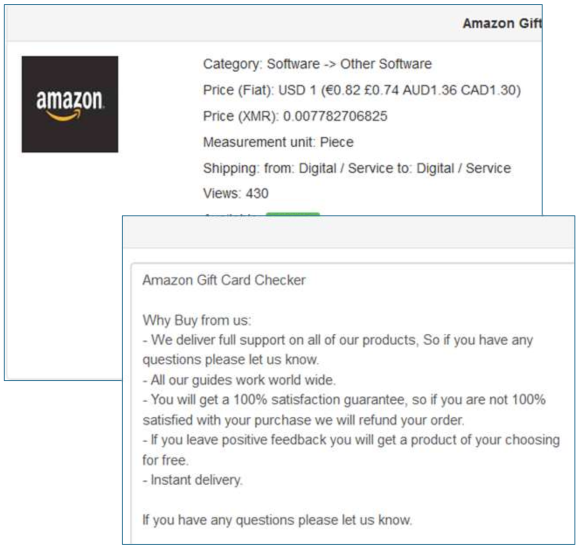
Escrows: normal

How Hackers Monetize Your Email Account

Hackers can:

- **Reset your passwords** for other accounts
  - Ecommerce, Banking, Social media & more
- **Send malicious emails to your contacts**
  - Get more victims!
- **Sell your password on the dark web**
- **Steal data from your email**
  - Financial details (tax info, etc.)
  - Personal info (SSNs, birthdays, etc.)

But the big payoff is….



Amazon Gift

Category: Software -> Other Software

Price (Fiat): USD 1 (€0.82 £0.74 AUD1.36 CAD1.30)

Price (XMR): 0.007782706825

Measurement unit: Piece

Shipping: from: Digital / Service to: Digital / Service

Views: 430

Amazon Gift Card Checker

Why Buy from us:
- We deliver full support on all of our products, So if you have any questions please let us know.
- All our guides work world wide.
- You will get a 100% satisfaction guarantee, so if you are not 100% satisfied with your purchase we will refund your order.
- If you leave positive feedback you will get a product of your choosing for free.
- Instant delivery.

If you have any questions please let us know.

The Big $$ Comes from BEC Scams

1. Executive fraud
2. Upcoming real estate transaction
3. Payroll redirect
4. Vendor payment (i.e. invoice fraud)
5. Billing fraud
6. Attorney impersonation

Example: BEC Lure

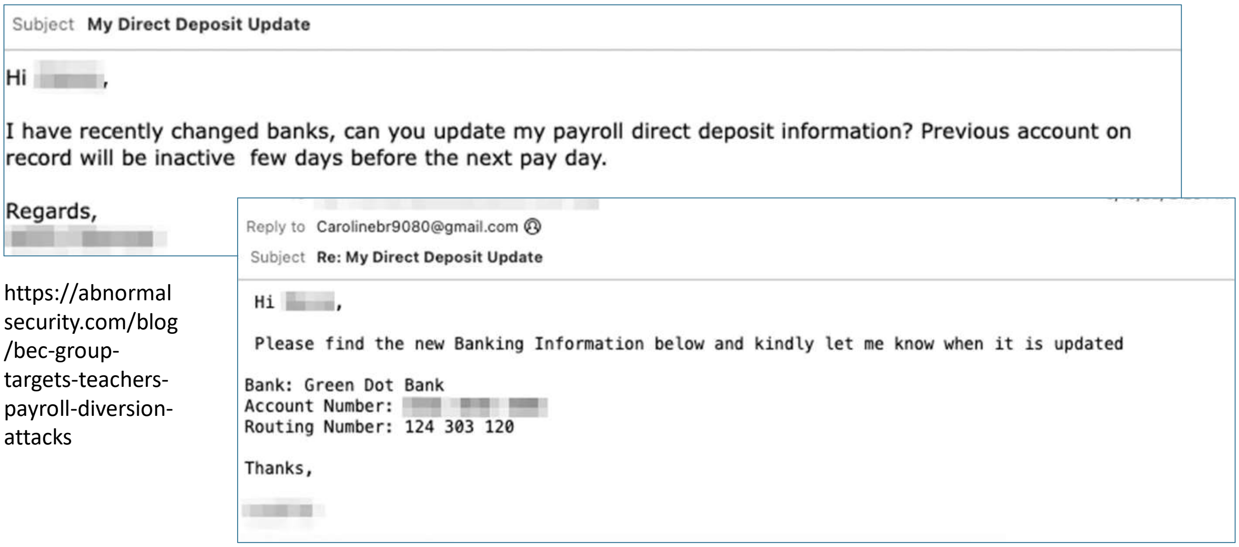
From: Sherri Davidoff <myipadmailcoo.net@gmail.com>
Subject: urgent task
Date: November 8, 2022 at 12:17:48 PM CST
To: XXXXXX@lmgsecurity.com

Hi Sam,

Do you have some free moment? I'll need you to get something done for me real quick.

Sent from my mobile device

Payroll Redirect



Subject My Direct Deposit Update

Hi [redacted],

I have recently changed banks, can you update my payroll direct deposit information? Previous account on record will be inactive few days before the next pay day.

Regards,
[redacted]

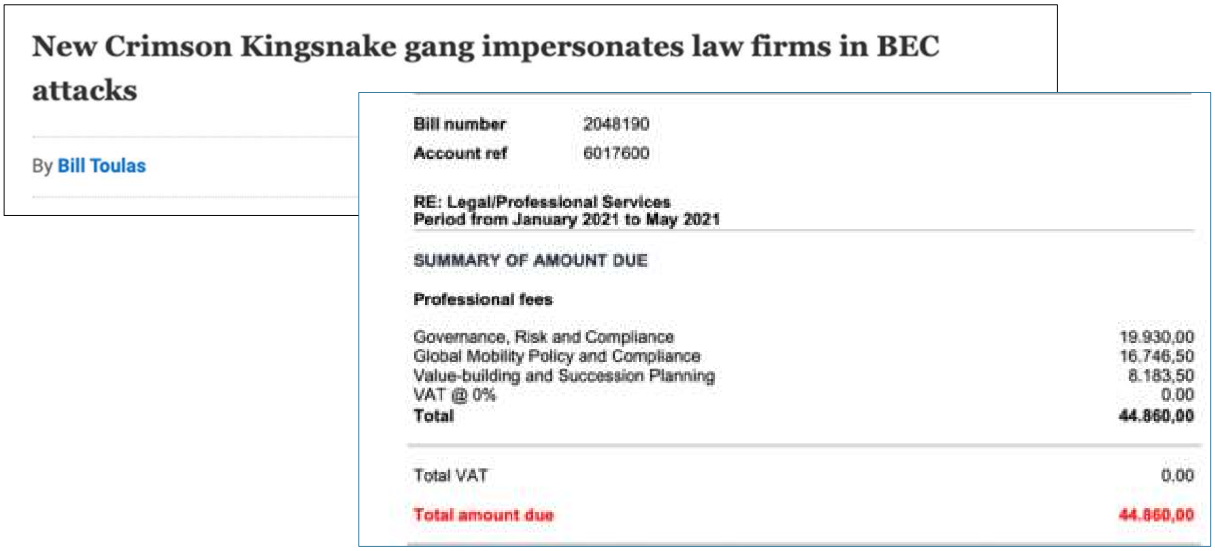
Reply to Carolinebr9080@gmail.com

Subject Re: My Direct Deposit Update

```
Hi [redacted],

Please find the new Banking Information below and kindly let me know when it is updated

Bank: Green Dot Bank
Account Number: [redacted]
Routing Number: 124 303 120

Thanks,

[redacted]
```

https://abnormalsecurity.com/blog/bec-group-targets-teachers-payroll-diversion-attacks

Trend: Impersonating Attorneys



New Crimson Kingsnake gang impersonates law firms in BEC attacks

By Bill Toulas

Bill number	2048190
Account ref	6017600

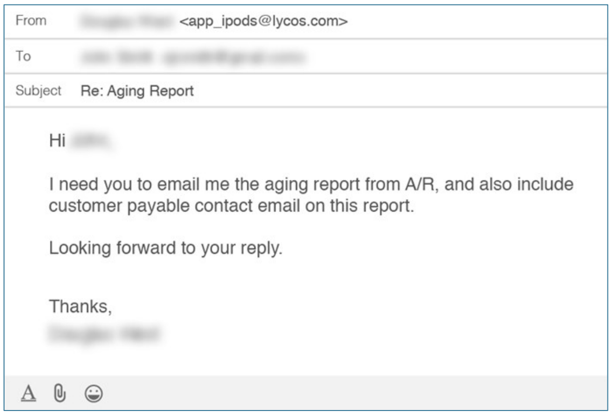
RE: Legal/Professional Services
Period from January 2021 to May 2021

SUMMARY OF AMOUNT DUE

Professional fees

Governance, Risk and Compliance	19.930,00
Global Mobility Policy and Compliance	16.746,50
Value-building and Succession Planning	8.183,50
VAT @ 0%	0.00
Total	**44.860,00**
Total VAT	0.00
Total amount due	**44.860,00**

Multistage Attacks



From [redacted] <app_ipods@lycos.com>

To [redacted]

Subject Re: Aging Report

Hi [redacted]

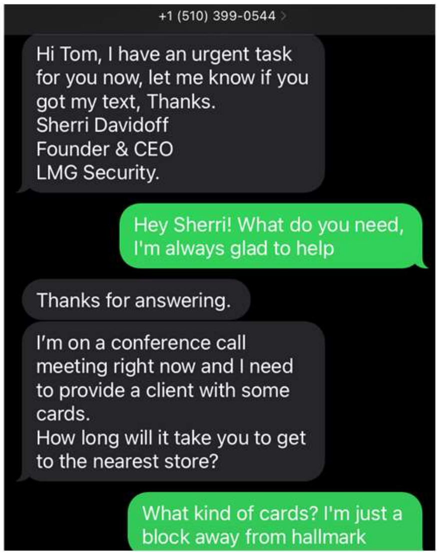
I need you to email me the aging report from A/R, and also include customer payable contact email on this report.

Looking forward to your reply.

Thanks,
[redacted]

17

Gift Card Scams



+1 (510) 399-0544 >

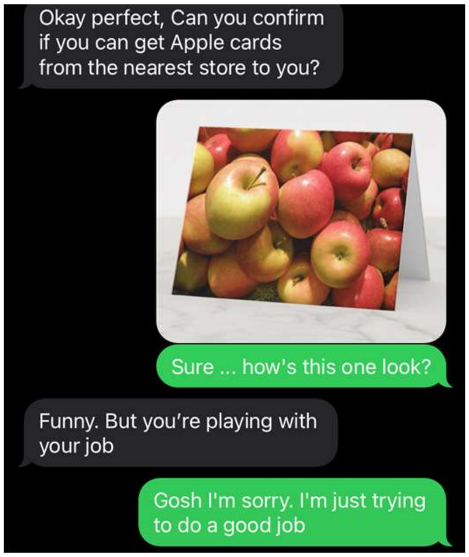
Hi Tom, I have an urgent task for you now, let me know if you got my text, Thanks.
Sherri Davidoff
Founder & CEO
LMG Security.

Hey Sherri! What do you need, I'm always glad to help

Thanks for answering.

I'm on a conference call meeting right now and I need to provide a client with some cards.
How long will it take you to get to the nearest store?

What kind of cards? I'm just a block away from hallmark



Okay perfect, Can you confirm if you can get Apple cards from the nearest store to you?

Sure ... how's this one look?

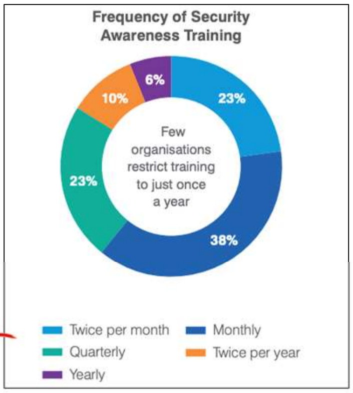
Funny. But you're playing with your job

Gosh I'm sorry. I'm just trying to do a good job

18

Conduct Cybersecurity Awareness Training

- On-Demand Awareness Videos
- Email Reminders
- Include Phishing Exercises
- Email, text, phone scams



Frequency of Security Awareness Training

Few organisations restrict training to just once a year

Employee training -$232,867

19

Use Multifactor Authentication

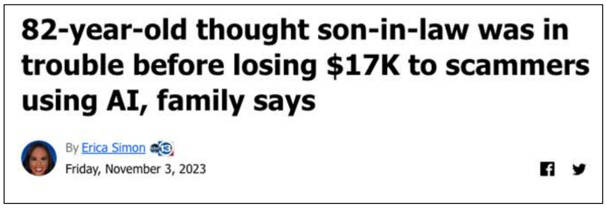
- Something you know (Type 1)
- Something you have (Type 2)
- Something you are (Type 3)

Multifactor = more than one

20

Voice Cloning Attacks are Here

- Scammers call a victim
- Claim to be a known person
  - Or that person is in the room
- The person has public audio or video
  - It just takes ~1 minute of audio
- Use voice cloning to instruct the victim to move $$
- "I heard Michael's voice. I thought I was talking to Michael"



82-year-old thought son-in-law was in trouble before losing $17K to scammers using AI, family says

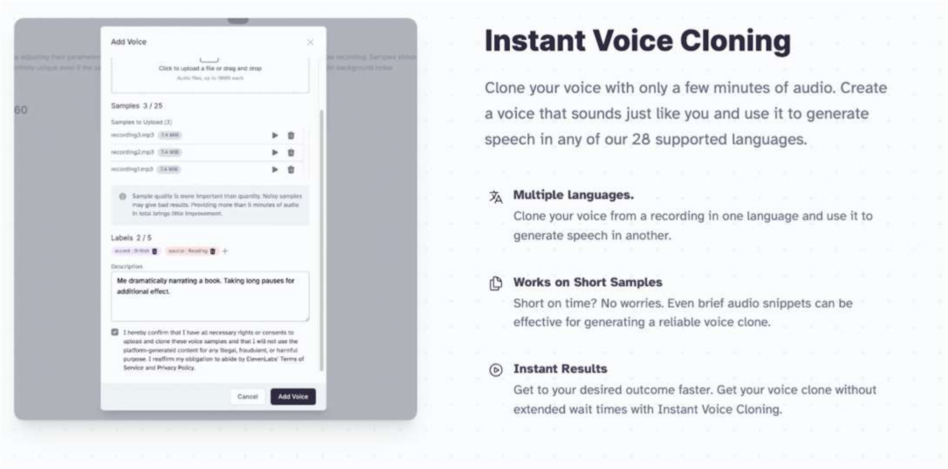
By Erica Simon

Friday, November 3, 2023

https://abc13.com/ai-generated-voice-cloning-scams-against-elderly-82-year-old-loses-17000/14009790/

21

Voice Cloning is Fast and Free



Add Voice

Click to upload a file or drag and drop

Audio files, up to 10MB each

Samples 3 / 25

Samples to Upload (3)

recording3.mp3 2.4 MB

recording2.mp3 2.4 MB

recording1.mp3 2.4 MB

Sample quality is more important than quantity. Noisy samples may give bad results. Providing more than 5 minutes of audio in total brings little improvement.

Labels 2 / 5

accent : British | source : Reading

Description

Me dramatically narrating a book. Taking long pauses for additional effect.

☑ I hereby confirm that I have all necessary rights or consents to upload and clone these voice samples and that I will not use the platform-generated content for any illegal, fraudulent, or harmful purpose. I reaffirm my obligation to abide by ElevenLabs' Terms of Service and Privacy Policy.

Cancel | Add Voice

Instant Voice Cloning

Clone your voice with only a few minutes of audio. Create a voice that sounds just like you and use it to generate speech in any of our 28 supported languages.

Multiple languages.
Clone your voice from a recording in one language and use it to generate speech in another.

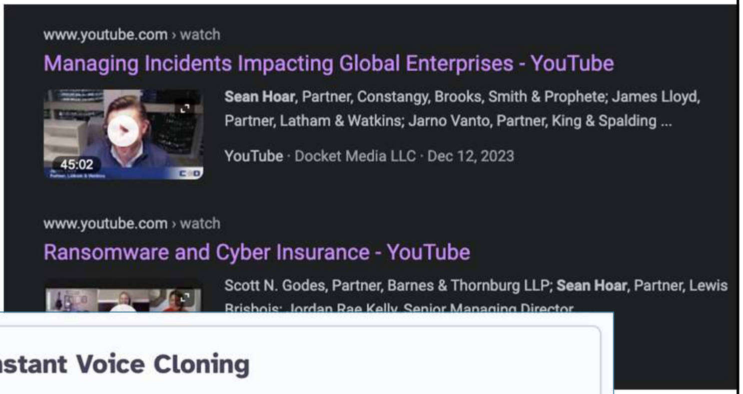
Works on Short Samples
Short on time? No worries. Even brief audio snippets can be effective for generating a reliable voice clone.

Instant Results
Get to your desired outcome faster. Get your voice clone without extended wait times with Instant Voice Cloning.

https://elevenlabs.io/voice-cloning

22

Demo: Cloning Sean's Voice



www.youtube.com › watch

Managing Incidents Impacting Global Enterprises - YouTube

Sean Hoar, Partner, Constangy, Brooks, Smith & Prophete; James Lloyd, Partner, Latham & Watkins; Jarno Vanto, Partner, King & Spalding ...

YouTube · Docket Media LLC · Dec 12, 2023

www.youtube.com › watch

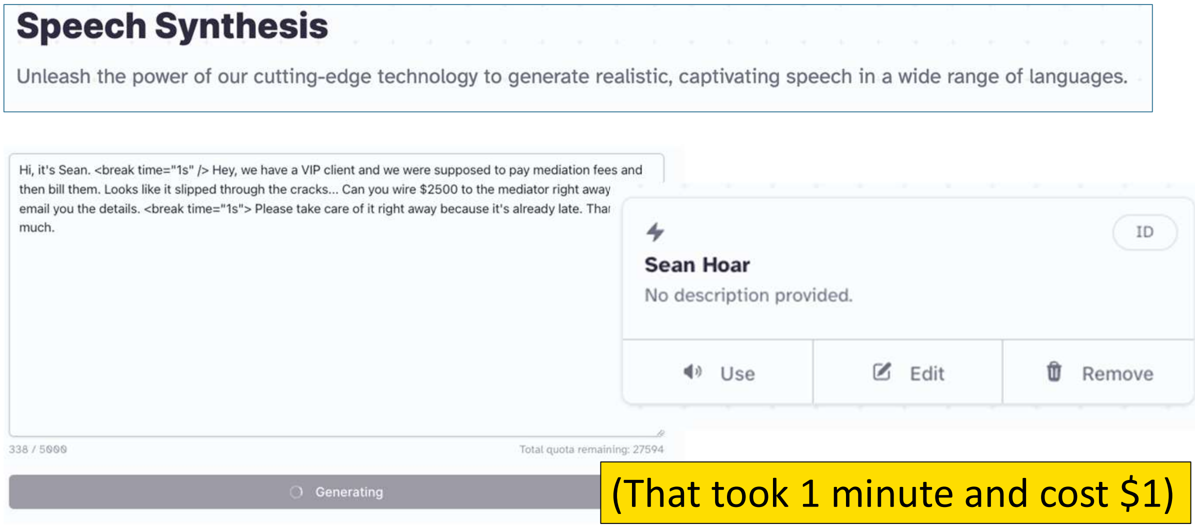
Ransomware and Cyber Insurance - YouTube

Scott N. Godes, Partner, Barnes & Thornburg LLP; **Sean Hoar**, Partner, Lewis Brisbois; Jordan Rae Kelly, Senior Managing Director

Instant Voice Cloning

Clone a voice from a clean sample recording. Samples should contain 1 speaker and be over 1 minute long and not contain background noise.

Demo: Cloning Sean's Voice



Speech Synthesis

Unleash the power of our cutting-edge technology to generate realistic, captivating speech in a wide range of languages.

Hi, it's Sean. <break time="1s" /> Hey, we have a VIP client and we were supposed to pay mediation fees and then bill them. Looks like it slipped through the cracks... Can you wire $2500 to the mediator right away email you the details. <break time="1s"> Please take care of it right away because it's already late. Tha much.

338 / 5000

Total quota remaining: 27594

Sean Hoar

No description provided.

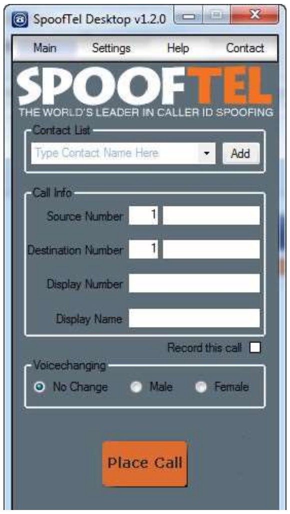
(That took 1 minute and cost $1)

Potential Threats to Attorneys

- Pretend to be you
  - Direct staff to move funds
- Pose as clients
  - Direct you to pay $ and bill them, or move funds held in trust
- Scam your bank
  - Pose as your finance clerk, etc.

25

It’s Easy to Spoof Caller ID…



SpoofTel Desktop v1.2.0

Main Settings Help Contact

SPOOFTEL

THE WORLD'S LEADER IN CALLER ID SPOOFING

Contact List

Type Contact Name Here ▾ Add

Call Info

Source Number 1

Destination Number 1

Display Number

Display Name

Record this call □

Voicechanging

● No Change ○ Male ○ Female

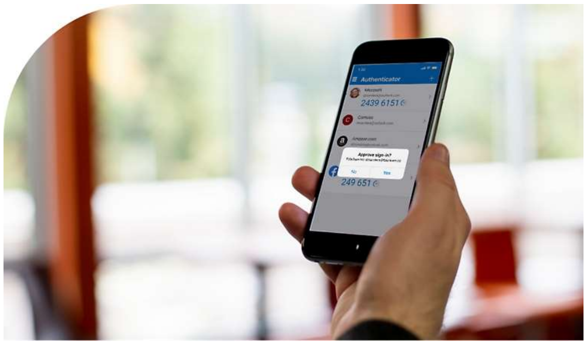
Place Call

“There was also an increasingly prevalent tactic by BEC bad actors of spoofing legitimate business phone numbers to confirm fraudulent banking details with victims.” -FBI 2022 IC3 report

26

Carefully Verify Callers

- We can’t rely on voice any more
- **Call back** a number or email address that you know is legit
- **Consider video verification**
  - (Until the scammers get good at faking videos)
- **Be cautious using Knowledge Based Authentication (KBA)**
  - i.e. security questions
  - Can be stolen, guessed or phished



Source: https://www.microsoft.com/en-us/security/mobile-authenticator-app

27

Demo: A Sting Operation!

Your one-stop shop for experienced legal services!

Sue Septebel
Finance Clerk

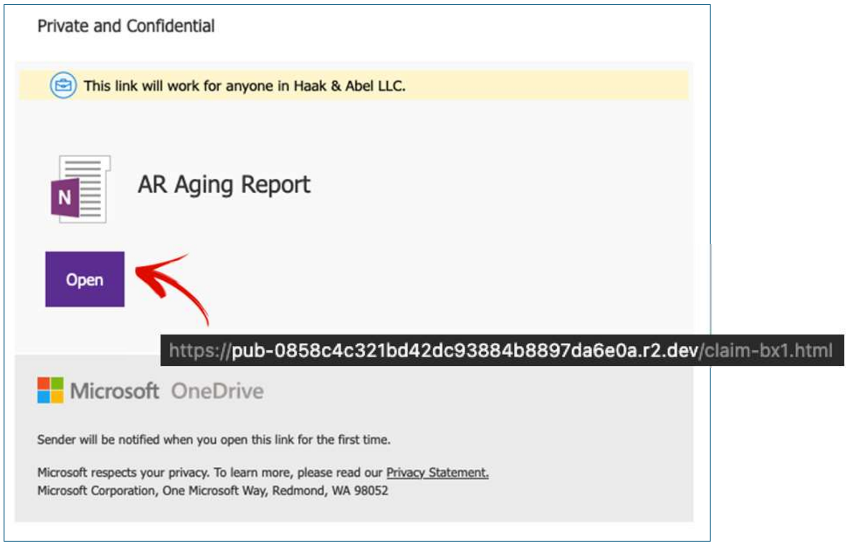
28

Sue is Helping with A Big Purchase!

- Haak & Abel is buying a new building!
- An ACH payment of $250k needs to be sent ASAP
- The recipient is Paul Allen, who owns a real estate business
- Sue needs to send Paul a form so he can confirm his bank details

29

Sue Gets Phished!



Private and Confidential

This link will work for anyone in Haak & Abel LLC.

AR Aging Report

https://pub-0858c4c321bd42dc93884b8897da6e0a.r2.dev/claim-bx1.html

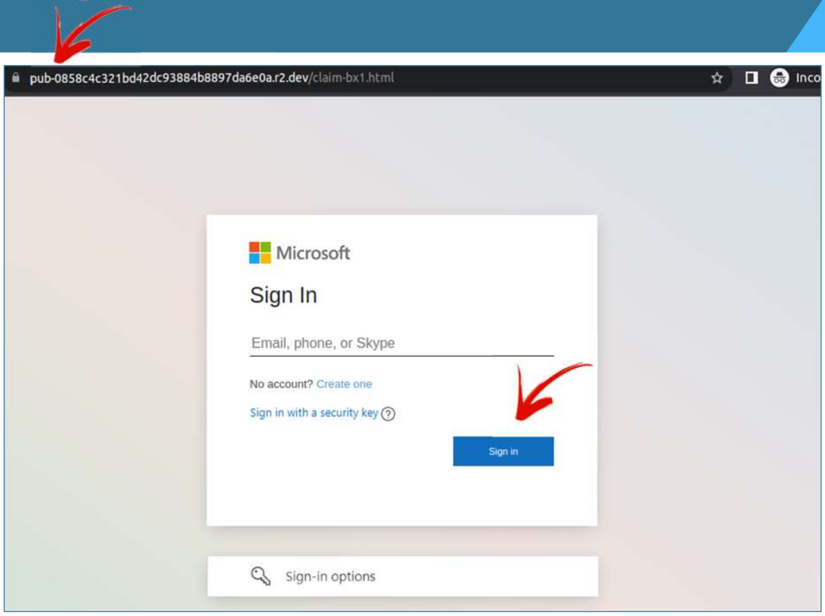
Microsoft OneDrive

Sender will be notified when you open this link for the first time.

Microsoft respects your privacy. To learn more, please read our Privacy Statement.
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

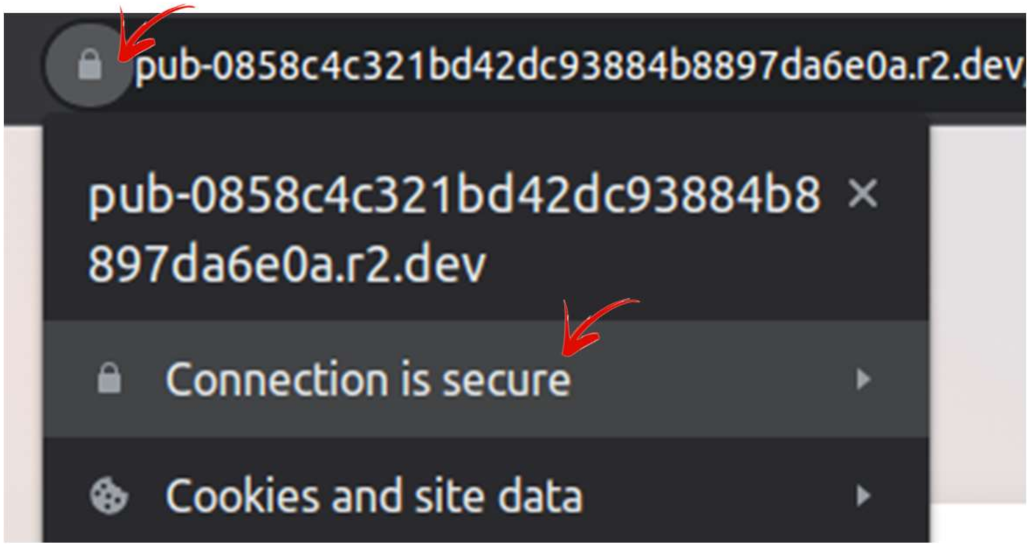
30

The Phishing Website



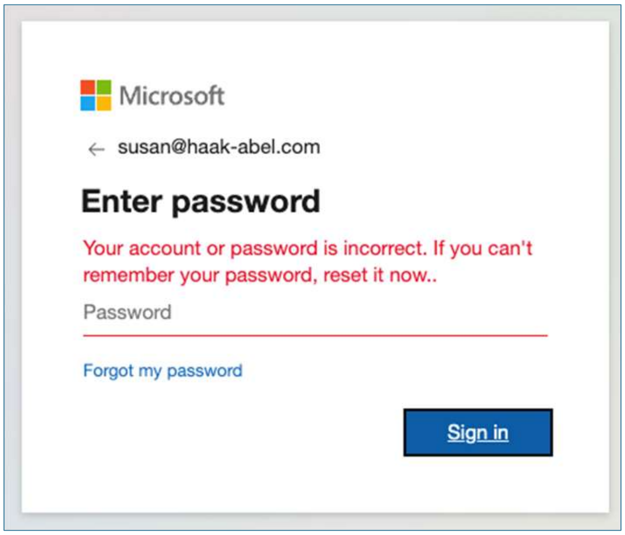
31

It Must Be Safe, Right? …Right?


pub-0858c4c321bd42dc93884b8897da6e0a.r2.dev
pub-0858c4c321bd42dc93884b8897da6e0a.r2.dev
Connection is secure
Cookies and site data

32

Hackers Often Want Multiple Passwords…



Microsoft

← susan@haak-abel.com

Enter password

Your account or password is incorrect. If you can't remember your password, reset it now..

Password

Forgot my password

Sign in

- Phishing sites often try to collect multiple passwords
- Confirms to the adversary that you entered the correct password
- Can also lead to the theft of multiple passwords at the same time

33

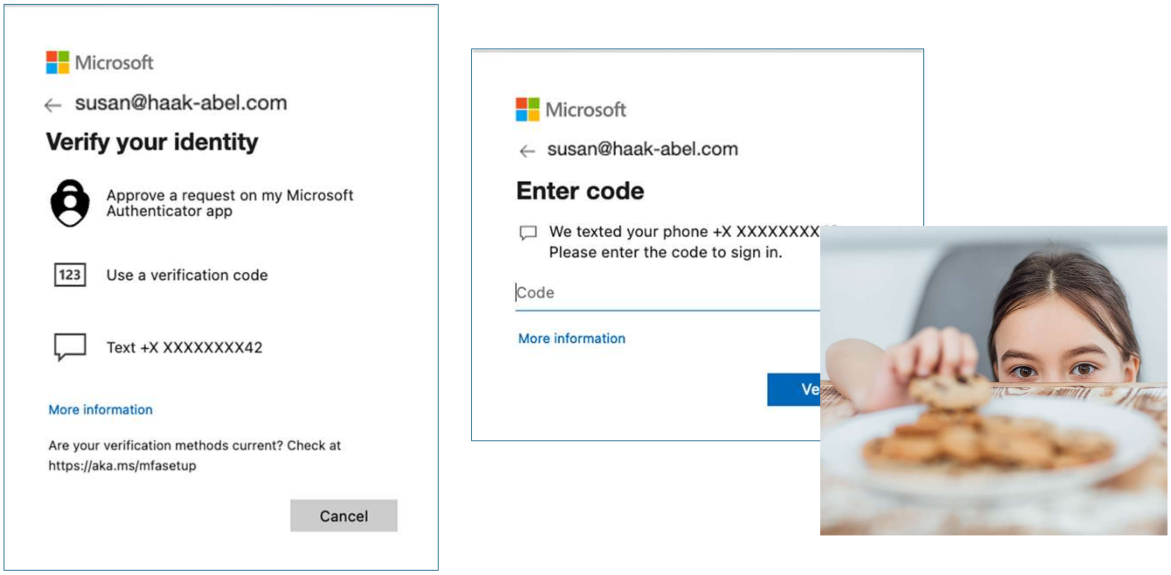
Sue is Using Multifactor Authentication!

- Something you know (Type 1)
- Something you have (Type 2)
- Something you are (Type 3)

Multifactor = more than one

34

The Hackers Steal Sue's MFA Code, Too



Microsoft

← susan@haak-abel.com

Verify your identity

Approve a request on my Microsoft Authenticator app

Use a verification code

Text +X XXXXXXXX42

More information

Are your verification methods current? Check at https://aka.ms/mfasetup

Cancel

Microsoft

← susan@haak-abel.com

Enter code

We texted your phone +X XXXXXXXX

Please enter the code to sign in.

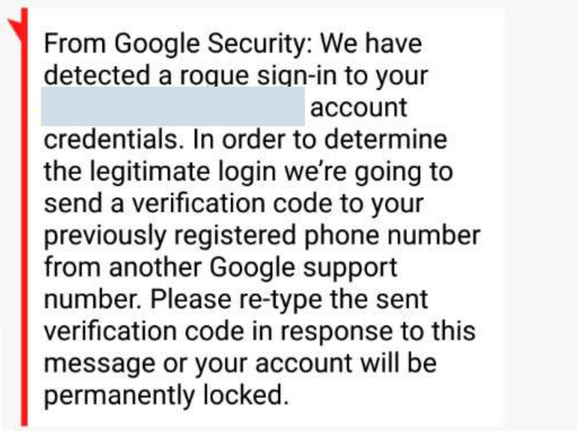
Code

More information

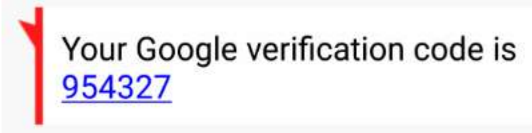
35

One-Time Passcodes (OTP) are Phishing-Prone

- Phishing web sites captures codes and use in real time
- Attackers text/call and request codes
  - Sometimes for "verification" purposes



From Google Security: We have detected a rogue sign-in to your [redacted] account credentials. In order to determine the legitimate login we're going to send a verification code to your previously registered phone number from another Google support number. Please re-type the sent verification code in response to this message or your account will be permanently locked.

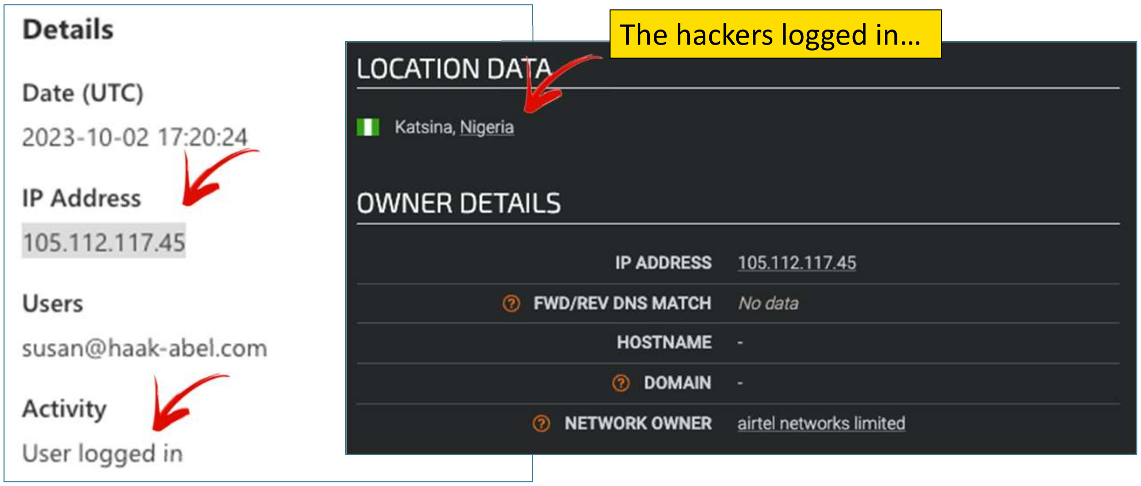


Your Google verification code is 954327

https://blog.knowbe4.com/u.s.-government-says-to-use-phishing-resistant-mfa

36

The Hackers Quickly Login to Sue's Account!



The hackers logged in…

Details

Date (UTC)
2023-10-02 17:20:24

IP Address
105.112.117.45

Users
susan@haak-abel.com

Activity
User logged in

LOCATION DATA

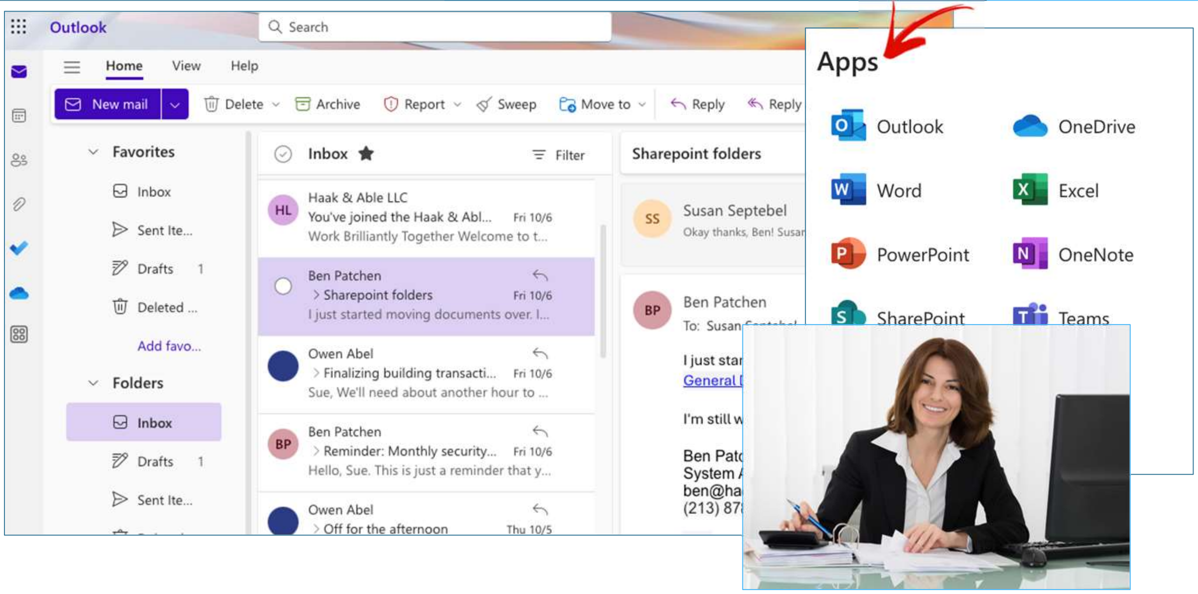
Katsina, Nigeria

OWNER DETAILS

IP ADDRESS	105.112.117.45
FWD/REV DNS MATCH	*No data*
HOSTNAME	-
DOMAIN	-
NETWORK OWNER	airtel networks limited

37

Now They Have Full Access to Sue's O365 Account



Haak & Able LLC
You've joined the Haak & Abl... Fri 10/6
Work Brilliantly Together Welcome to t...

Ben Patchen
Sharepoint folders Fri 10/6
I just started moving documents over. I...

Owen Abel
Finalizing building transacti... Fri 10/6
Sue, We'll need about another hour to ...

Ben Patchen
Reminder: Monthly security... Fri 10/6
Hello, Sue. This is just a reminder that y...

Owen Abel
Off for the afternoon Thu 10/5

Susan Septebel
Okay thanks, Ben! Susan

Ben Patchen
To: Susan

I just star
General

I'm still w

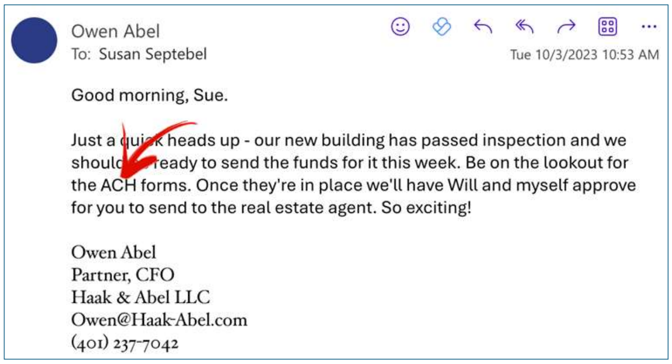
Ben Patc
System A
ben@ha
(213) 87

Apps

38

The Hackers Searched Sue's Mailbox

- Searched for key terms:
  - Invoice
  - Payment
  - etc.
- Viewed Mailbox contents



Owen Abel
To: Susan Septebel
Tue 10/3/2023 10:53 AM

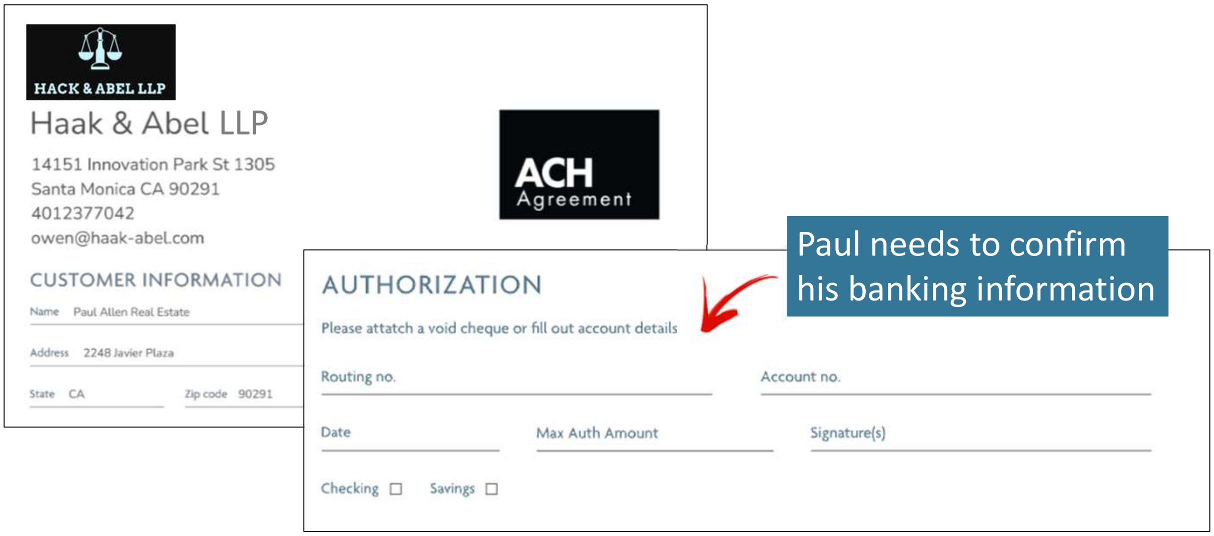
Good morning, Sue.

Just a quick heads up - our new building has passed inspection and we should be ready to send the funds for it this week. Be on the lookout for the ACH forms. Once they're in place we'll have Will and myself approve for you to send to the real estate agent. So exciting!

Owen Abel
Partner, CFO
Haak & Abel LLC
Owen@Haak-Abel.com
(401) 237-7042

39

The Hackers Find the ACH Form



HACK & ABEL LLP

Haak & Abel LLP

14151 Innovation Park St 1305
Santa Monica CA 90291
4012377042
owen@haak-abel.com

ACH Agreement

CUSTOMER INFORMATION

Name Paul Allen Real Estate

Address 2248 Javier Plaza

State CA Zip code 90291

AUTHORIZATION

Please attatch a void cheque or fill out account details

Routing no. ______ Account no. ______

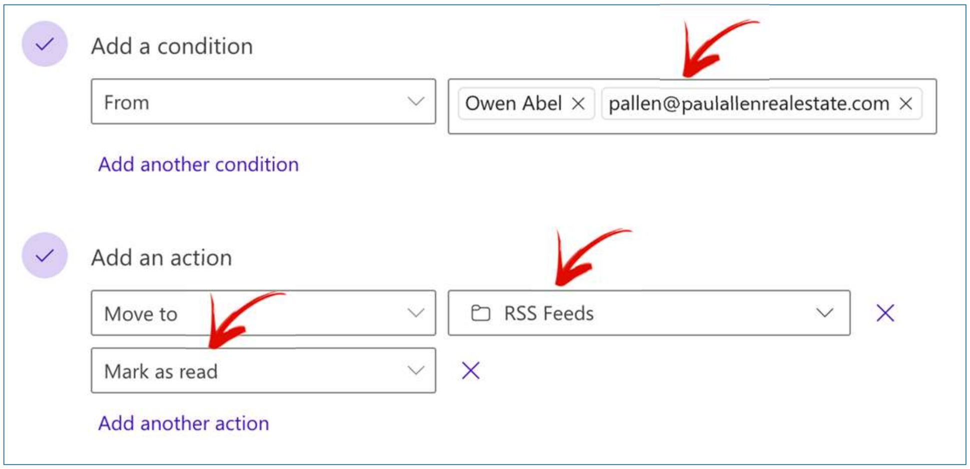
Date ______ Max Auth Amount ______ Signature(s) ______

Checking □ Savings □

Paul needs to confirm his banking information

40

The Attackers Set Up Mail Forwarding Rules!



Add a condition

From	Owen Abel × pallen@paulallenrealestate.com ×

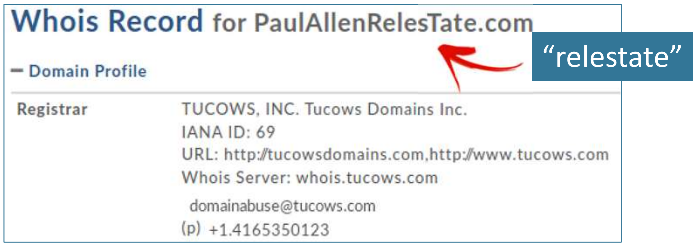
Add another condition

Add an action

Move to	RSS Feeds
Mark as read	

Add another action

The Attackers Register a Fraudulent Domain

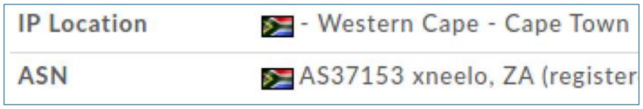


Whois Record for PaulAllenRelesTate.com

“relestate”

− Domain Profile

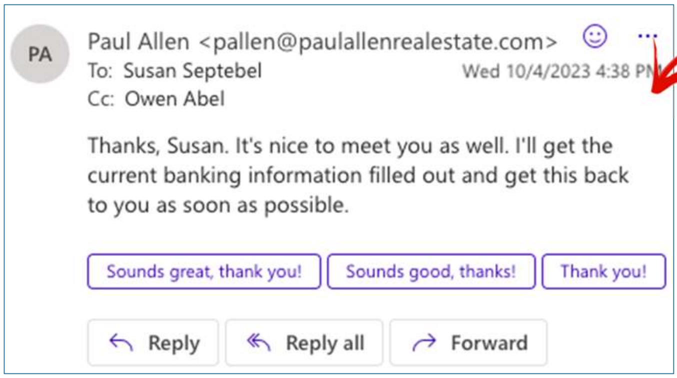
Registrar	TUCOWS, INC. Tucows Domains Inc. IANA ID: 69 URL: http://tucowsdomains.com,http://www.tucows.com Whois Server: whois.tucows.com domainabuse@tucows.com (p) +1.4165350123



IP Location	- Western Cape - Cape Town
ASN	AS37153 xneelo, ZA (register

- A spoofed domain is registered so the attacker can impersonate Paul
- Almost identical, except “Real Estate” is missing a letter

They Deleted the “Real” Response from Paul

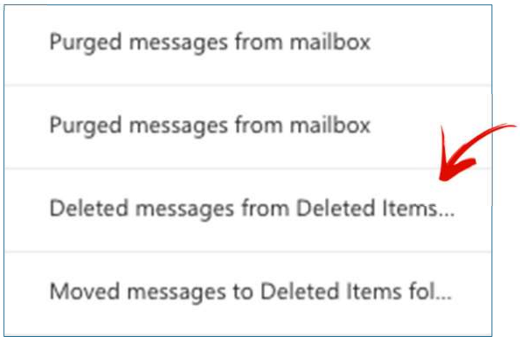


PA

Paul Allen <pallen@paulallenrealestate.com>
To: Susan Septebel
Cc: Owen Abel
Wed 10/4/2023 4:38 PM

Thanks, Susan. It's nice to meet you as well. I'll get the current banking information filled out and get this back to you as soon as possible.

The attackers saw this, deleted it, and then…



Purged messages from mailbox

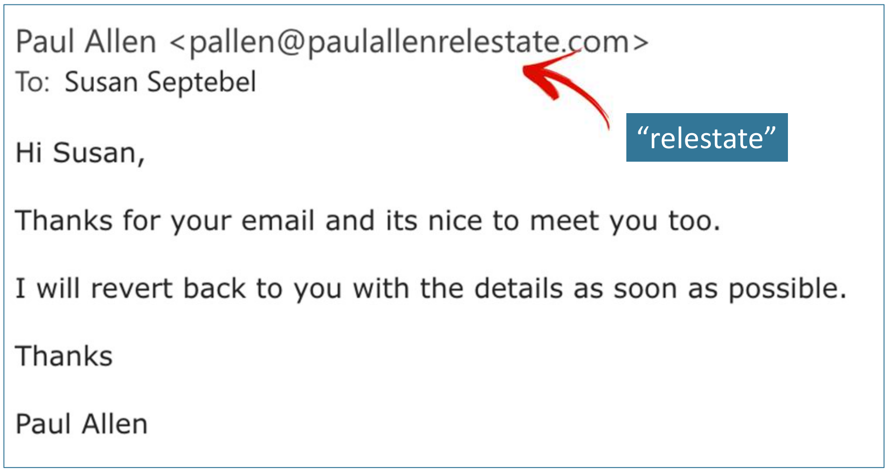
Purged messages from mailbox

Deleted messages from Deleted Items...

Moved messages to Deleted Items fol...

43

Hacker “Paul” Emails Sue



Paul Allen <pallen@paulallenrelestate.com>
To: Susan Septebel

Hi Susan,

Thanks for your email and its nice to meet you too.

I will revert back to you with the details as soon as possible.

Thanks

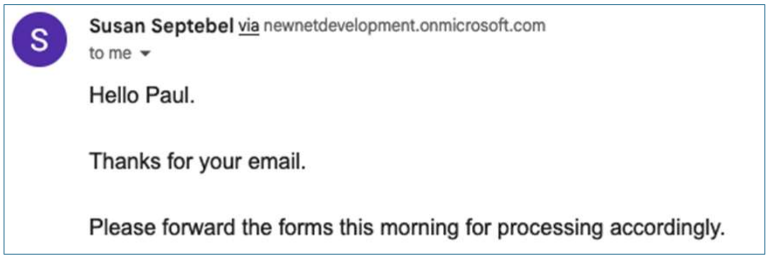
Paul Allen

“relestate”

44

The Hackers Also Sneakily Send Emails to “Real” Paul

- The attackers use Sue’s email to communicate with the real Paul
- That way he won’t get suspicious
- Routinely deleted these emails from the “Sent” folder



Susan Septebel via newnetdevelopment.onmicrosoft.com
to me

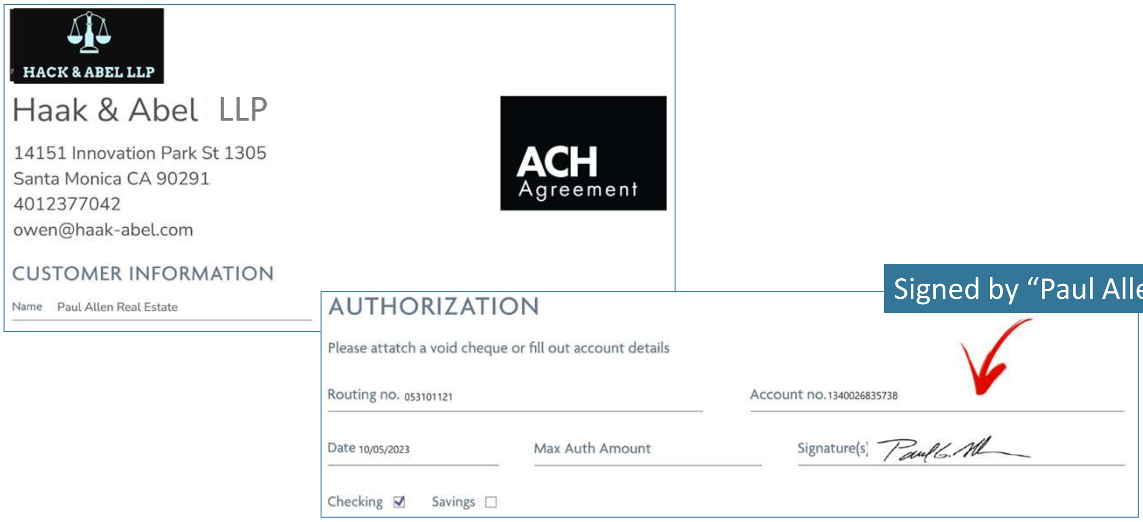
Hello Paul.

Thanks for your email.

Please forward the forms this morning for processing accordingly.

45

Hacker “Paul” Sends the Completed ACH Paperwork!!!



HACK & ABEL LLP

Haak & Abel LLP

14151 Innovation Park St 1305
Santa Monica CA 90291
4012377042
owen@haak-abel.com

ACH Agreement

CUSTOMER INFORMATION

Name Paul Allen Real Estate

AUTHORIZATION

Please attatch a void cheque or fill out account details

Routing no. 053101121

Account no. 1340026835738

Date 10/05/2023

Max Auth Amount

Signature(s) Paul G. Al

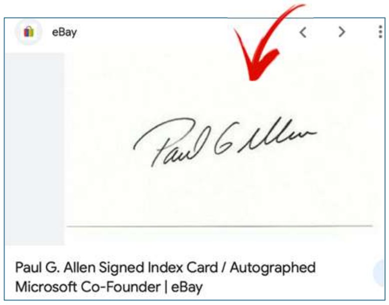
Checking ☑ Savings □

Signed by “Paul Allen”

46

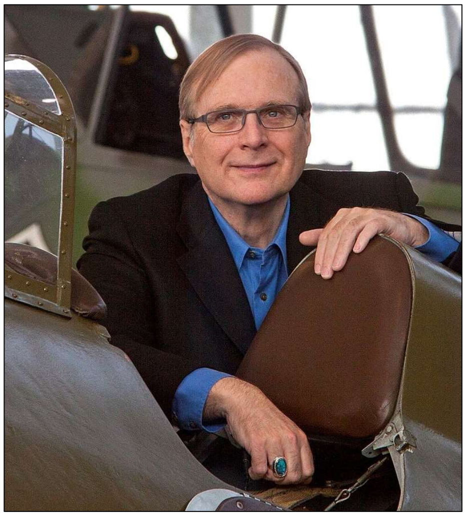
The Actual Paul Allen…

- Co-Founder of Microsoft
- Died in 2018
- The hackers found his signature online…
- Copied it into the ACH form!



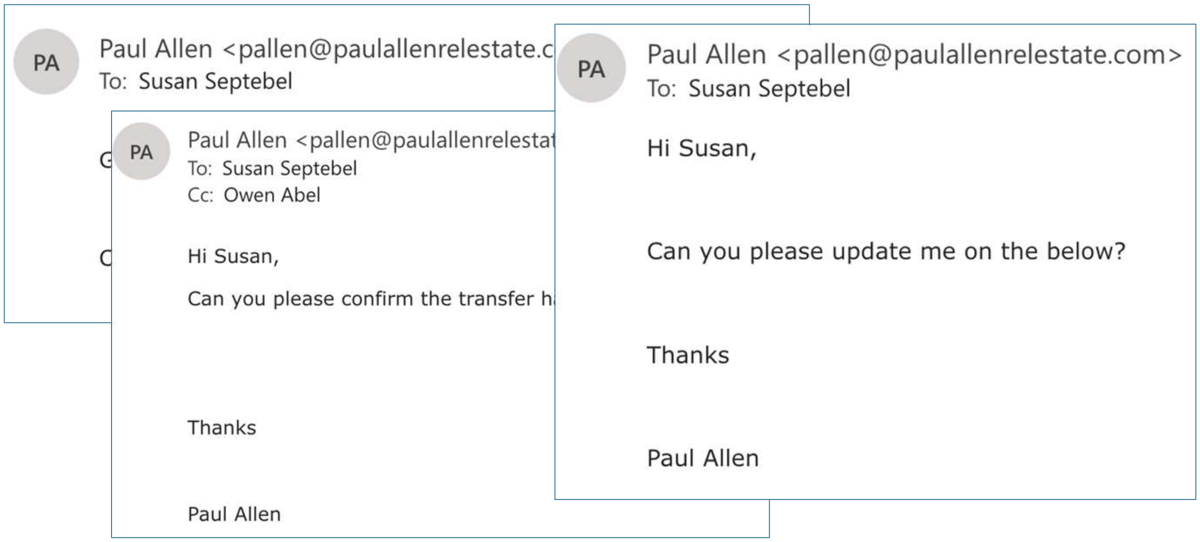
Paul G Allen

Paul G. Allen Signed Index Card / Autographed Microsoft Co-Founder | eBay



47

The Hackers Did Not Give Up Easily…



Paul Allen <pallen@paulallenrelestate.c
To: Susan Septebel

G

C

Paul Allen <pallen@paulallenrelestat
To: Susan Septebel
Cc: Owen Abel

Hi Susan,

Can you please confirm the transfer h

Thanks

Paul Allen

Paul Allen <pallen@paulallenrelestate.com>
To: Susan Septebel

Hi Susan,

Can you please update me on the below?

Thanks

Paul Allen

48

Recap – Email Hacking for $$

1. Criminals use stolen passwords to access email
2. Search email for invoice/wire transfers etc.
3. Steal data, if desired
4. Add mail forwarding rules, if desired
5. Send fake invoice/wire transfer requests
6. Profit

49

Out-of-Band Verification Can Help!

- Receive an email with:
  - Updated bank account info?
  - Request for wire transfer?
  - Request for financial data?
- Always verify using a second method of communication
- Phone, face-to-face, Zoom, etc.
- Use contact info you already have
  - Not from the email!

50

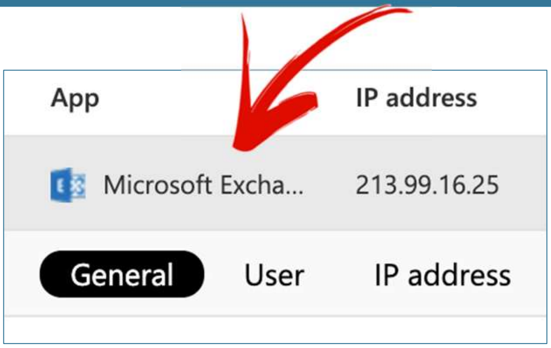
Additional Damage…

- Your data may also have been stolen
- Potential data breach

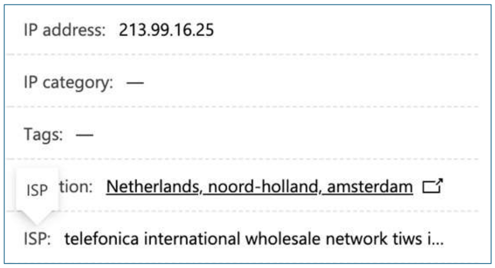
4/9/2024

51

Hackers Might Sync Your Whole Mailbox



App	IP address
Microsoft Excha...	213.99.16.25



IP address: 213.99.16.25

IP category: —

Tags: —

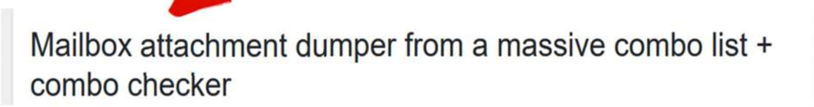
tion: Netherlands, noord-holland, amsterdam

ISP: telefonica international wholesale network tiws i...

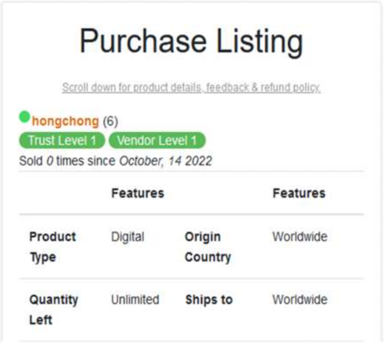
The attackers synced the whole mailbox to their local computer!

52

Hackers Comb Through Attachments



Mailbox attachment dumper from a massive combo list + combo checker

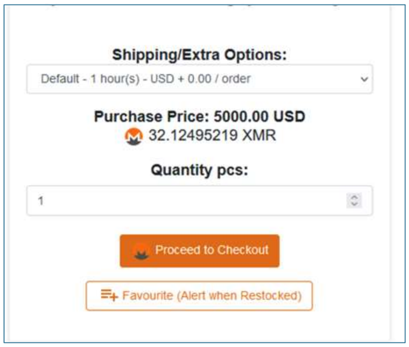


Purchase Listing

Scroll down for product details, feedback & refund policy.

● hongchong (6)
Trust Level 1 Vendor Level 1
Sold 0 times since October, 14 2022

	Features		Features
Product Type	Digital	Origin Country	Worldwide
Quantity Left	Unlimited	Ships to	Worldwide



Shipping/Extra Options:

Default - 1 hour(s) - USD + 0.00 / order

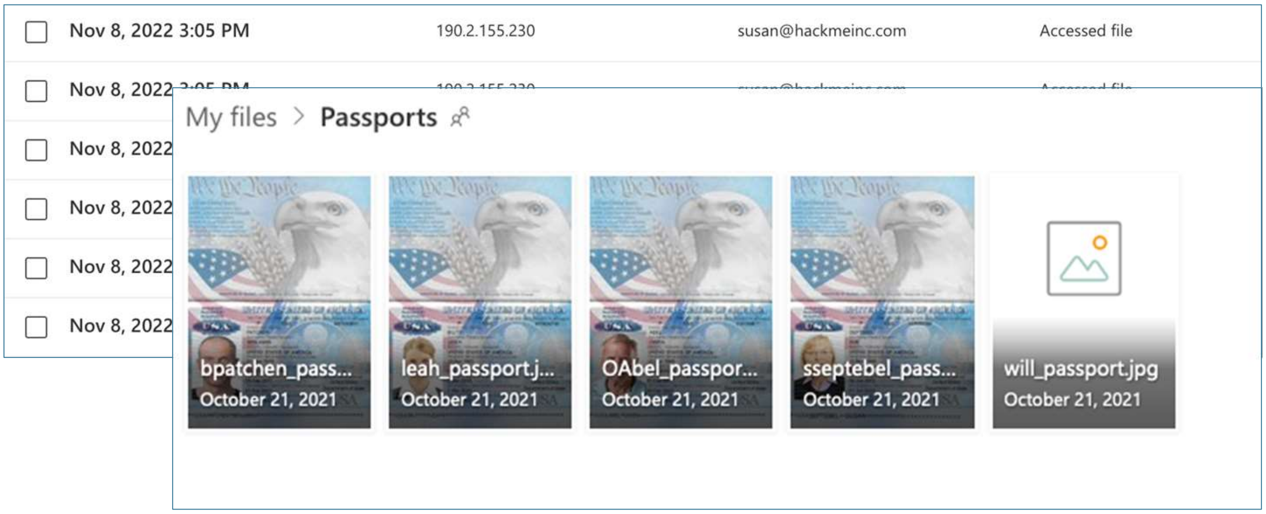
Purchase Price: 5000.00 USD
32.12495219 XMR

Quantity pcs:

1

53

Hackers Access & Download Files from SharePoint



□	Nov 8, 2022 3:05 PM	190.2.155.230	susan@hackmeinc.com	Accessed file
□	Nov 8, 2022 3:05 PM	190.2.155.230	susan@hackmeinc.com	Accessed file
□	Nov 8, 2022			
□	Nov 8, 2022			
□	Nov 8, 2022			
□	Nov 8, 2022			

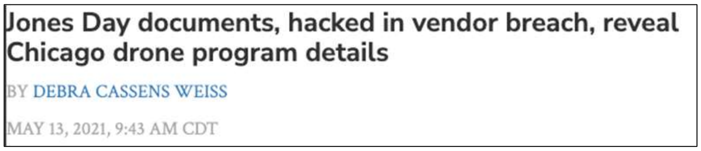
My files > Passports

bpatchen_pass...	October 21, 2021
leah_passport.j...	October 21, 2021
OAbel_passpor...	October 21, 2021
sseptebel_pass...	October 21, 2021
will_passport.jpg	October 21, 2021

54

Damage from Cyber Incidents

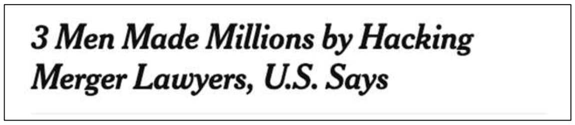
- Your reputation
- Client trust
- Lawsuits
- Financial damage
- IT outages
- Risk for clients
  - Identity theft
  - Financial losses
  - & more, depending on the data



Jones Day documents, hacked in vendor breach, reveal Chicago drone program details

BY DEBRA CASSENS WEISS

MAY 13, 2021, 9:43 AM CDT



3 Men Made Millions by Hacking Merger Lawyers, U.S. Says

55

Cybersecurity Incidents are VERY expensive

Per-record cost of a data breach

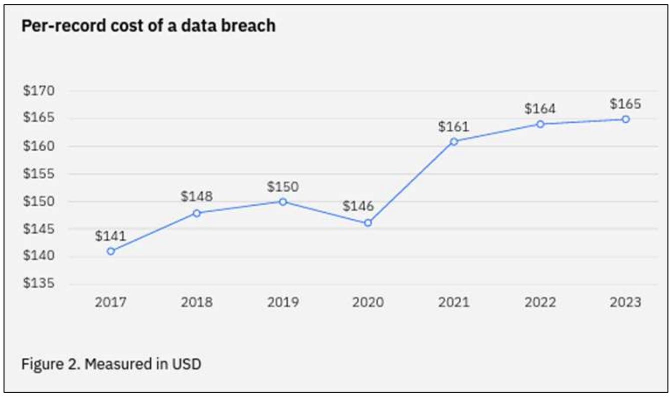
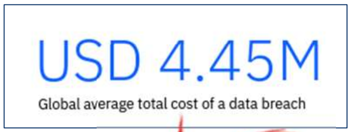
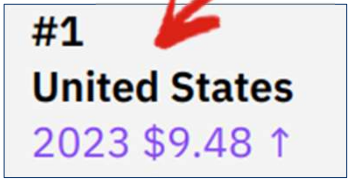


Figure 2. Measured in USD



USD 4.45M

Global average total cost of a data breach



#1

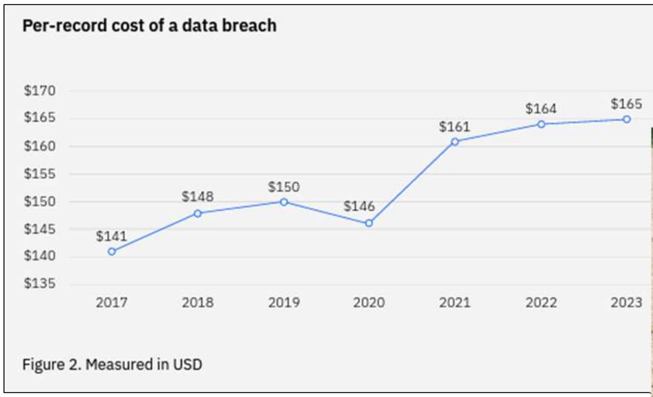
United States

2023 $9.48 ↑

IBM

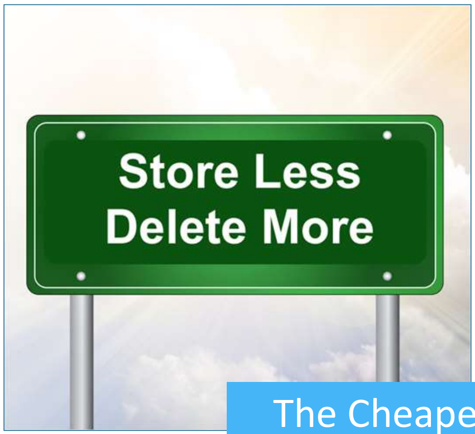
56

More Data = Higher Damages When it Leaks



57

Reduce Your Data



The Cheapest Way to Reduce Your Risk!

58

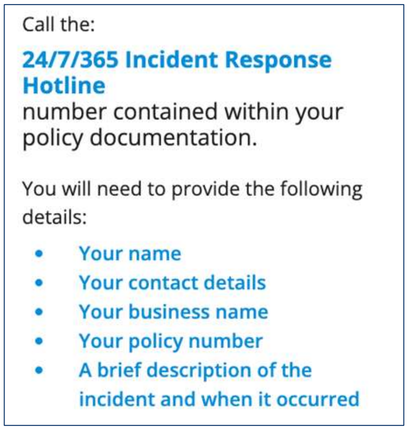
Cyber Insurance is More Important than Ever

- Information security & privacy liability
  - Legal defense
  - Investigative expense
  - Claims & damages due to privacy violations
- Regulatory fines (state/federal laws, etc.)
- Business interruption
  - Lost revenue (after a waiting period)
  - Recovery/remediation costs
  - May not provide coverage due to 3rd party provider outages
    - Contingent/dependent business interruption

59

Cyber Insurance Can Help if You're Hacked!

- Call your insurer's hotline
  - Typically staffed by attorneys
  - May also be staffed by insurer's team
- Hotline staff identify parties to bring in
  - IR partner
  - Ransomware negotiator
  - etc.
- Get on a call with attorneys and IR partner
- Triage & develop initial response strategy



Call the:

24/7/365 Incident Response Hotline
number contained within your policy documentation.

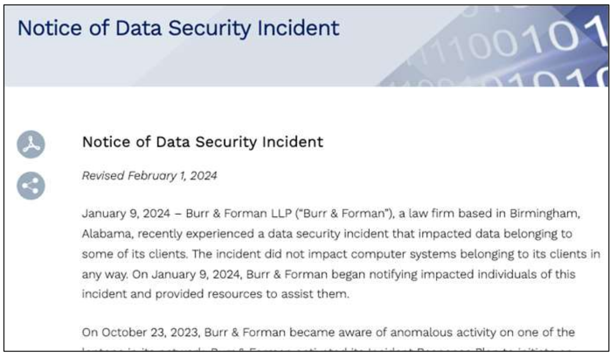
You will need to provide the following details:

- Your name
- Your contact details
- Your business name
- Your policy number
- A brief description of the incident and when it occurred

60

Proper Notification is Critical

- Ethics
- Current vs. former clients
- 3rd party liability



Notice of Data Security Incident

Notice of Data Security Incident

Revised February 1, 2024

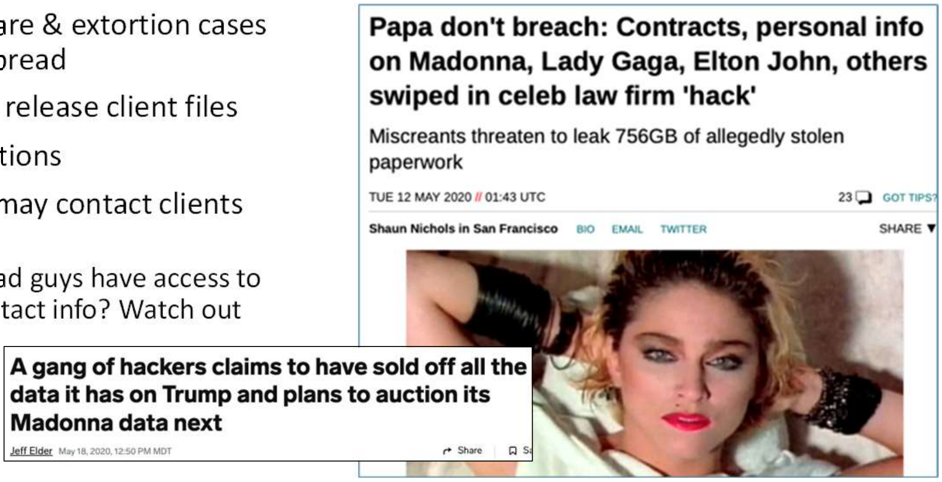
January 9, 2024 – Burr & Forman LLP ("Burr & Forman"), a law firm based in Birmingham, Alabama, recently experienced a data security incident that impacted data belonging to some of its clients. The incident did not impact computer systems belonging to its clients in any way. On January 9, 2024, Burr & Forman began notifying impacted individuals of this incident and provided resources to assist them.

On October 23, 2023, Burr & Forman became aware of anomalous activity on one of the

61

The Criminals May Notify For You

- Ransomware & extortion cases are widespread
- Threats to release client files
- Public auctions
- Criminals may contact clients directly
  - Did the bad guys have access to client contact info? Watch out



Papa don't breach: Contracts, personal info on Madonna, Lady Gaga, Elton John, others swiped in celeb law firm 'hack'

Miscreants threaten to leak 756GB of allegedly stolen paperwork

TUE 12 MAY 2020 // 01:43 UTC

Shaun Nichols in San Francisco

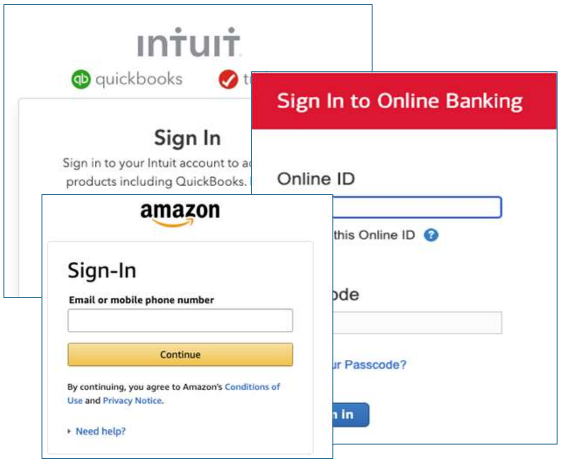
A gang of hackers claims to have sold off all the data it has on Trump and plans to auction its Madonna data next

Jeff Elder May 18, 2020, 12:50 PM MDT

62

Password Re-Use is a Top Cause of Breaches

- Criminals steal your passwords
  - Or buy them on the dark web
- Try them everyplace they can!
- Personal sites, work sites
- “Credential stuffing”
- Automated tools
- All your cloud apps are at risk



intuit

quickbooks

Sign In

Sign in to your Intuit account to a
products including QuickBooks.

Sign In to Online Banking

Online ID

this Online ID

ode

r Passcode?

n in

amazon

Sign-In

Email or mobile phone number

Continue

By continuing, you agree to Amazon's Conditions of Use and Privacy Notice.

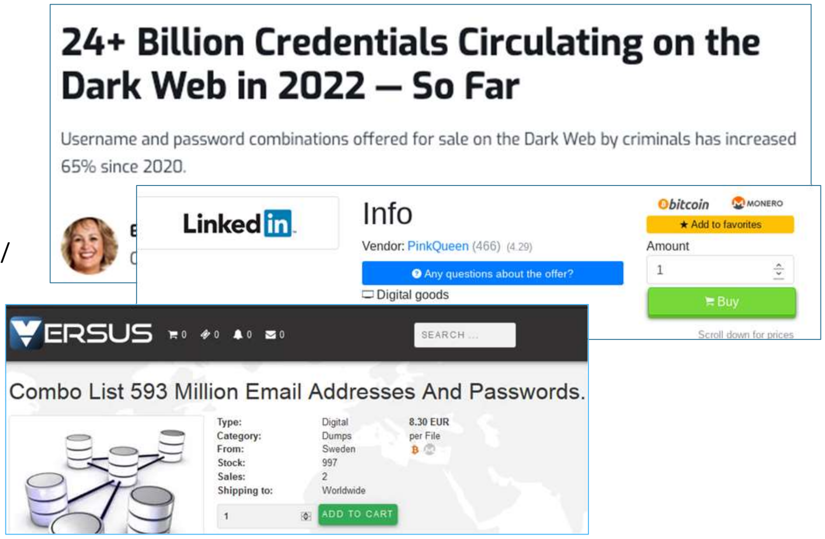
Need help?

> “Hackers don’t break in, they log in”
>
> - Bret Arsenault, Microsoft

Choose a Strong Password

- Unique
- Long
- ~~Complex~~
- ~~Changed routinely~~

https://pages.nist.gov/800-63-FAQ/



24+ Billion Credentials Circulating on the Dark Web in 2022 — So Far

Username and password combinations offered for sale on the Dark Web by criminals has increased 65% since 2020.

LinkedIn

Info

Vendor: PinkQueen (466) (4.29)

Any questions about the offer?

Digital goods

bitcoin MONERO

★ Add to favorites

Amount

1

Buy

Scroll down for prices

VERSUS

SEARCH ...

Combo List 593 Million Email Addresses And Passwords.

Type:	Digital	8.30 EUR
Category:	Dumps	per File
From:	Sweden	
Stock:	997	
Sales:	2	
Shipping to:	Worldwide	

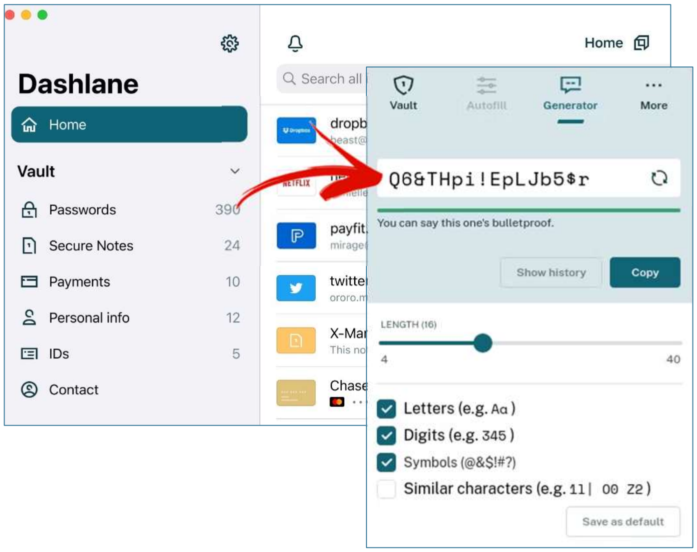
1

ADD TO CART

Password Managers Can Help!

- **Unique passwords can’t be re-used if stolen**
- **Make sure they are difficult to guess**
- **Use a password manager!**
- Team sharing
- Password escrow
- Popular:
  - ⍰ Dashlane, 1Password, BitWarden
  - ⍰ Low cost or even free

(Remember to use MFA for the login!)



Q6&THpi!EpLJb5$r

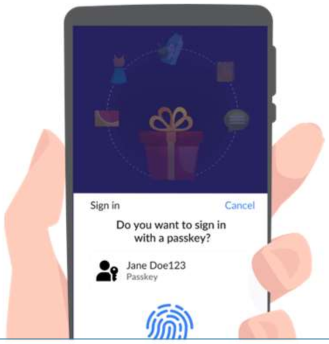
You can say this one's bulletproof.

LENGTH (16) — 4 … 40

- ☑ Letters (e.g. Aa)
- ☑ Digits (e.g. 345)
- ☑ Symbols (@&$!#?)
- □ Similar characters (e.g. 11| 00 Z2)

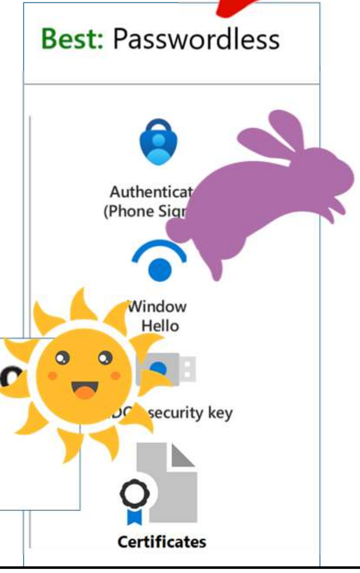
65

Embrace Passwordless Authentication!



Microsoft, Google and Apple Commit to Passwordless Future

By Chris Paoli | 05/05/2022



66

7 Key Takeaways

1. Use Multi-Factor Authentication
   - Ideally using strong authentication
   - Any MFA is better than no MFA
2. Conduct Cybersecurity Awareness Training
3. Reduce Your Data
4. Get (Good) Cyber Insurance
5. Pick Unique, Strong Passwords
6. Use a Password Manager Program
7. Embrace Passwordless Authentication

67

Questions?

- Sean Hoar
- Partner - Chair
- shoar@constangy.com
- 503-459.7707

- Sherri Davidoff
- CEO
- info@LMGsecurity.com
- 406-830-3165

CONSTANGY BROOKS, SMITH & PROPHETE LLP

LMG SECURITY

68

HOW TO:

PREVENT & RESPOND TO BUSINESS EMAIL COMPROMISE

LMG SECURITY

Email account break-ins seem to happen as often as the common cold— and yet they can lead to large financial losses, reputational damage, and more. In this handout, we'll discuss how criminals break into email accounts, and what you can do to protect yourself and your organization.

WHY DO CRIMINALS HACK YOUR EMAIL ACCOUNT?

YOUR DATA IS WORTH $$

Business email accounts are potential gold mines. Your emails contain valuable data, such as Social Security Numbers, passwords, credit-card numbers, and other details that can be sold for money on the dark web. In some cases, criminals copy entire accounts of correspondence, which can later be used for ransom or political gain.

CRIMINALS USE EMAIL FOR FINANCIAL FRAUD

Often, criminals hack into a business email account in order to commit financial fraud. For example, a criminal might break into an email account and then immediately search for data that could easily be monetized (such as invoices or wire transfer instructions). Next, the criminal creates a fake invoice or wire transfer notification to redirect the funds, and then waits for the money to arrive. Sophisticated criminals add mail filtering rules that lengthen the time to discovery.

YOUR CONTACTS BECOME THE NEXT VICTIMS

Once criminals break into an email account, they often made a point of targeting related accounts, such as co-workers, clients, or anyone listed as a contact.

EMAIL HACKS CAN BE DATA BREACHES

In addition to financial fraud, extortion, reputational damage and more, an email account break-in may "count" as a data breach. If an attacker had access to confidential information, you may be required to notify the data subjects and report a breach under state or federal law, depending on the contents of your email.

HOW DO CRIMINALS GET ACCESS?

In recent years, email has moved to the cloud, enabling users (and criminals) to access email from anywhere in the world. Here are three ways that criminals get access to your email:

1. **INFECT YOUR COMPUTER**
Criminals infect your computer by enticing you to click on a link or open a malicious attachment. When you do, your computer may be infected with malware that monitors your keystrokes or steals your login information when you submit a web form.

2. **FAKE A WEB SITE**
Criminals may set up fake web sites that look just like your email provider, bank or other common web service. Then, they trick you into visiting the web site, using phishing emails or other methods. When you type your password into the fake web site, they capture it and use it to login to your accounts.

3. **BUY YOUR PASSWORD ON THE DARK WEB**
There have been so many data breaches that billions of passwords are available for sale on the dark web. If your password was stolen in the past, it may be sold on the dark web to others who will use it to login to your accounts.

PROTECT YOUR ACCOUNTS

You can protect your email (and other data online) using strong passwords and login security. First, here are a few important terms to know:

AUTHENTICATION - A method for verifying a person's identity. For example, I might tell my computer that I am "jsmith," and I prove my identity by typing in a *password*.

VERIFICATION - There are three different ways that you can verify that you are who you say you are:

- ***Something you know*** (for example, a password).
- ***Something you have*** (for example, a key).
- ***Something you are*** (for example, a fingerprint).

TWO-FACTOR AUTHENTICATION - Verifying a person's identity using two methods combined.

PASSWORD MANAGERS - A smart way to remember strong passwords is to not remember them at all! A password manager is secure software that stores your passwords in an encrypted vault on your computer, or in the cloud.

Here are some video tutorials for setting up and using password managers and two-factor authentication: www.LMGsecurity.com/passwords

TIPS FOR STRONG PASSWORDS AND LOGIN SECURITY

DO

✓ **Use Two-Factor Authentication!** It's easy to set up with many providers, such as Office365 and Google.

✓ **Pick Strong Passwords** - Choose a password that is long- at least 14 characters or more. Use a passphrase (a sentence fragment, song lyrics, etc.) to help you remember it.

✓ **Use a Password Manager Program** to store your passwords securely, so you don't have to remember them all. Popular options include LastPass and KeePass.

DON'T

☒ **DON'T Share Your Password** with anyone—not friends, co-workers, vendors, or even IT staff.

☒ **DON'T Re-use Important Passwords**. Avoid using the same password for multiple different websites or services. Never re-use personal passwords for work, or vice versa.

☒ **DON'T Write Your Password Down on Paper**, unless it's secured in a locked location.

☒ **DON'T Store Passwords in Files on Your Computer**, such as Word documents or spreadsheets. Instead, use a secure password manager.

WHAT SHOULD YOU DO IF YOUR EMAIL GETS HACKED?

1. **Reset your password.**
2. **If possible, activate two-factor authentication.**
3. **Place a legal hold on any mailboxes that you suspect may have been compromised, to preserve all emails.** That way you can conduct an inventory and evaluate any data that may have been exposed.
4. **Preserve logs immediately.** Export and make copies of any logs that might show who logged into your email account, where they logged in from, or what they did. This can potentially help you narrow down the scope of the incident.
5. **Call for professional help.** Business email compromise can trigger breach notification laws, and lead to fraud and other crimes. Act quickly and get experienced guidance when you need it.

LMG™ SECURITY

145 W FRONT STREET
MISSOULA, MONTANA 59802
www.LMGsecurity.com

WE ARE HERE TO HELP

Please contact us any time you have a question or need additional support.
Phone: 406-830-3165 | Toll-Free: 1-855-LMG-8855 | E-mail: info@LMGsecurity.com

REFERRING A CLIENT

To refer a client to LMG Security, please email info@LMGsecurity.com

TIP SHEET:

MULTI-FACTOR AUTHENTICATION (MFA)

Overview & Best Practices

LMG SECURITY

WHAT IS MULTI-FACTOR AUTHENTICATION?

Authentication is the process of verifying a user's identity. Typically, this is done using any of the following factors:

- **SOMETHING YOU KNOW**
  such as a username or password
- **SOMETHING YOU HAVE**
  a physical token or authenticator app for example
- **SOMETHING YOU ARE**
  such as a fingerprint or retinal scan

Multi-factor authentication, or MFA, combines two or more factors to add extra layers of protection to your account. That way, if an attacker steals your password or your phone, you still have another layer of protection. LMG recommends that organizations enable MFA on any compatible internal and internet-facing applications, services, and accounts.

WHY DO YOU NEED MFA?

The 2022 Verizon Data Breach Investigation Report found that 82% of breaches involved a human element – e.g. social engineering – and over 60% of those attacks were a result of phishing. As organizations continue to grow their cloud portfolios, share credentials, and build trust relationships between platforms, criminals will increase their focus on compromising emails to gain access to your organization, on-premises systems, cloud environments, and even partner ecosystems.

Let's look at one recent example.

> A finance clerk fell victim to a phishing attack and typed her email password into a criminal's website by mistake. Since the organization did not require multi-factor authentication, the criminal easily accessed and searched the clerk's emails and identified the organization's payroll vendor. The criminal then entered the clerk's email password into the payroll login screen (unfortunately, the clerk used the same password for multiple accounts) and successfully accessed the company's payroll cloud platform. The lucky criminal used the access to divert the paychecks of multiple employees into the criminal's own bank account—which the criminal then emptied and closed after the next pay period—walking away with a hefty payday.

Implementing MFA is one of the most inexpensive ways to reduce your risk of fraud and data breaches.

BEST PRACTICES FOR IMPLEMENTING MFA

✓ Enable MFA on every compatible application, service, and account. Prioritize high-risk services such as Internet-facing accounts and cloud platforms.

✓ Whenever possible, used strong MFA such as a smartphone application or a hardware token. Simple SMS messages are more easily intercepted and misused by criminals. Consider implementing one of the following as your primary MFA solution:

Authenticator apps. Authenticator apps are designed to encrypt sensitive authentication tokens, authenticate endpoints, and resist attacks.

Hardware fobs. These small devices, such as Yubikey and Titan Security Key, are small enough to attach to your keychain. These options are either directly connected to your computer or are scanned using a protocol like Near Field Communication (NFC). This eliminates the risk from lost cell phones or SIM swapping attacks.

Biometric authentication. Go passwordless! You can use fingerprints, palm scans, facial recognition, or other options.

✓ If you must use SMS authentication (which is less secure and subject to SIM jacking / SIM swapping):

Contact your telecommunications provider and add a PIN or passphrase to your cellular accounts. This makes it much harder for a criminal to take over your phone number and have your texts sent to their phone. All major U.S. carriers support this option.

✓ Check the fallback options! Often, victims get hacked because a criminal forces the MFA system to use a backup method such as SMS. Make sure you understand what fallback options are enabled in your MFA system and disable any that don't fit your security model.

✓ Check that your cloud providers support strong authentication (not just SMS) before you sign up. If you're already using a platform that does not support strong authentication, urge your vendor to roll out support, and carefully evaluate whether the risk is worth the benefit of that service.

HOW TO CHOOSE AN MFA SOLUTION

You have multiple options for MFA solutions. But our first caveat is that no matter which solution you choose, HOW you configure and implement any of these solutions impacts their performance.

Three of the most common and most supported options are Duo, Microsoft Authenticator, and Google Authenticator. Here's a quick overview of what sets them apart:

Microsoft Authenticator. It's free with your Office 365 or Azure AD subscription! It supports all Microsoft services and can be used manually to sign into any traditional TOTP MFA integration. As an added bonus: the Microsoft Authenticator can also act as a password manager with direct mobile integration and available apps for both Google Chrome and Microsoft Edge.

Google Authenticator: It's free! The authenticator is a code generator and is supported by a large number of vendors and services right out of the box. While it shares many features in common with Microsoft and Duo, it lacks many of the management, response, and more sophisticated options. Google Authenticator is especially appropriate for individual and small business usage.

Duo. Requires a fee (although it is relatively inexpensive) for more than 10 seats, but it's a full-featured and robust solution with the following benefits:

- Supports a variety of authentication methods
- Facilitates push notifications
- Works natively with a large variety of services (out of the box support for Slack, Akamai, Atlassian, etc.)
- Includes strong logging and monitoring features
- Enables self-enrollment for a user's personal or work devices
- Integrates directly with Identity Providers like Azure AD to facilitate Single Sign-on (SSO) services

Any MFA is better than no MFA, but some solutions provide more features and are easier to manage. Implementing the right solution for your needs can quickly and easily provide your organization with a much stronger security posture.

Want LMG to implement or manage MFA for you? **Contact us**. We offer MFA as a managed service or handle the implementation for you to take the burden off your team.

HOW TO:

PROTECT YOUR PASSWORD – A CHEAT SHEET

Do you hate passwords? Have trouble remembering them? You're not alone! Passwords are both incredibly important and challenging to manage. Strong passwords are the foundation of cybersecurity and may be the difference between a data breach and just another day at the office. Here are simple steps you can take to make your passwords strong and stress-free.

TIPS FOR STRONG PASSWORDS AND LOGIN SECURITY

DO

✓ **Use Two-Factor Authentication!** It's easy to set up with many providers, such as Office365 and Google.

✓ **Pick Strong Passwords.** Choose a password that is long - at least 14 characters or more. Use a passphrase (a sentence fragment, song lyrics, etc.) to help you remember it. Passphrase Example: Jan 1st is NewYears!$ *or* Won'tyoubemyNeighbor?

✓ **Use a Password Manager Program.** Store your passwords securely, so you don't have to remember them all. Popular options include LastPass and KeePass.

DON'T

☒ **DON'T Share Your Password** with anyone—not friends, co-workers, vendors, or even IT staff.

☒ **DON'T Re-use Important Passwords**. Avoid using the same password for multiple different websites or services. Never re-use personal passwords for work, or vice versa.

☒ **DON'T Write Your Password Down on Paper,** unless it's secured in a locked location.

☒ **DON'T Store Passwords in Files on Your Computer,** such as Word documents or spreadsheets. Instead, use a secure password manager.

IMPORTANT TERMS

AUTHENTICATION

A method for verifying a person's identity. For example, I might tell my computer that I am "sdavidoff," and I prove my identity by typing in a *password*.

VERIFICATION

There are three different ways that you can verify that you are who you say you are:

- *Something you know* (for example, a password).
- *Something you have* (for example, a key).
- *Something you are* (for example, a fingerprint).

TWO-FACTOR AUTHENTICATION

Verifying a person's identity using two methods combined.

PASSWORD MANAGERS

A smart way to remember strong passwords is to not remember them at all! A password manager is secure software that stores your passwords in an encrypted vault on your computer, or in the cloud.

Here are some video tutorials for setting up and using password managers and two-factor authentication: www.LMGsecurity.com/passwords

LMG SECURITY

145 W FRONT STREET
MISSOULA, MT 59802
www.LMGsecurity.com

WE ARE HERE TO HELP

Please contact us any time you have a question or need additional support.
Phone: 406-830-3165 | Toll-Free: 1-855-LMG-8855
E-mail: info@LMGsecurity.com

REFERRING A CLIENT

To refer a client to LMG Security, please email info@LMGsecurity.com