Cybersecurity Update

Beyond the Headlines: The Everyday Cyber Threats Healthcare Providers Face

EXPLORE
HEALTHCARE SUMMIT

Disclaimer:

The information set forth in this presentation is intended as general risk management information. Beazley does not render legal services or advice. It should not be construed or relied upon as legal advice and is not intended as a substitute for consultation with counsel. Although reasonable care has been taken in preparing the information set forth in this presentation, Beazley accepts no responsibility for any errors it may contain or for any losses allegedly attributable to this information.

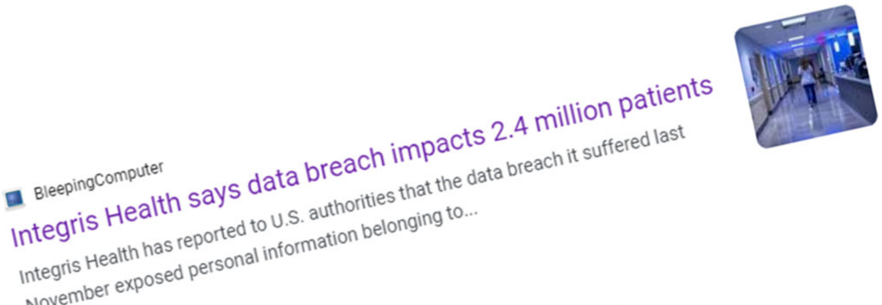
Today's Topics

- 2024 Year in Review
- Looking Forward
- Threats to Small Practices
- Incident Response & Business Continuity Planning
- When to Notify Insurance

2024 Year in Review

The Year of Vendor Data & Security Breaches

Third-Party vendor incidents stormed the media in 2024

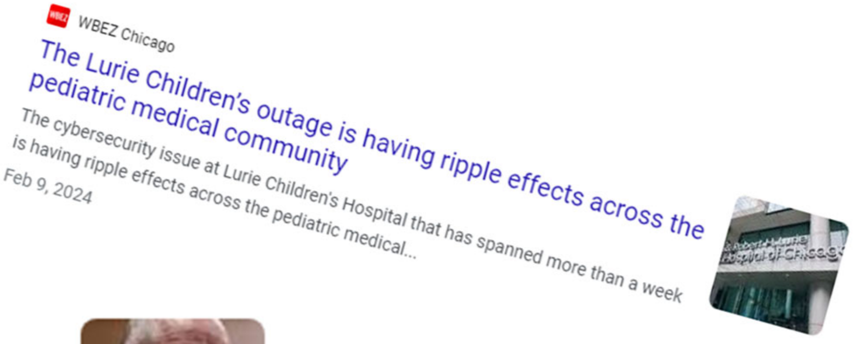


BleepingComputer

Integris Health says data breach impacts 2.4 million patients

Integris Health has reported to U.S. authorities that the data breach it suffered last November exposed personal information belonging to...

Feb 13, 2024

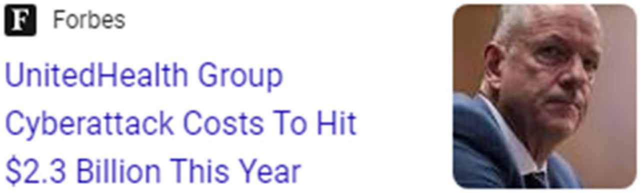


WBEZ Chicago

The Lurie Children's outage is having ripple effects across the pediatric medical community

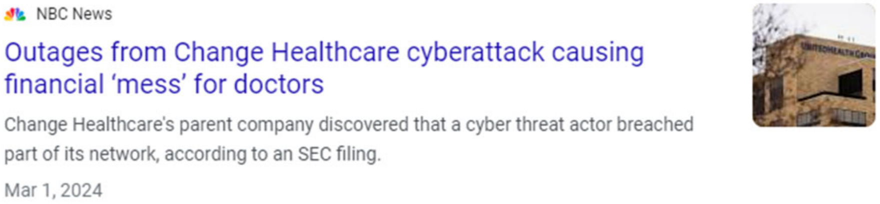
The cybersecurity issue at Lurie Children's Hospital that has spanned more than a week is having ripple effects across the pediatric medical...

Feb 9, 2024



Forbes

UnitedHealth Group Cyberattack Costs To Hit $2.3 Billion This Year

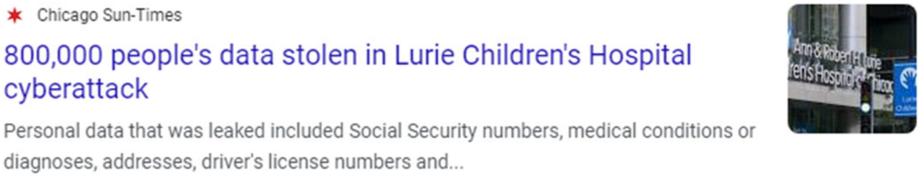


NBC News

Outages from Change Healthcare cyberattack causing financial 'mess' for doctors

Change Healthcare's parent company discovered that a cyber threat actor breached part of its network, according to an SEC filing.

Mar 1, 2024



Chicago Sun-Times

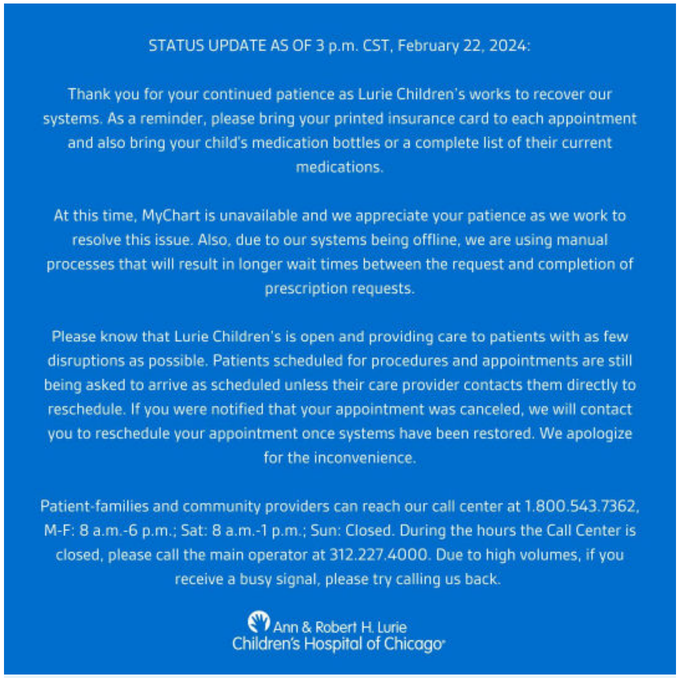
800,000 people's data stolen in Lurie Children's Hospital cyberattack

Personal data that was leaked included Social Security numbers, medical conditions or diagnoses, addresses, driver's license numbers and...

Ann & Robert H. Lurie Children’s Hospital

Rhysida Ransomware disrupted hospital operations and EMR/EHR for partners

- **January 31, 2024:** A cyberattack was discovered and systems were disrupted including EHR and the MyChart patient portal.
- **February 5, 2024:** Systems were partially restored.
- **February 15, 2024:** Email and Phones restored.
- **February 22, 2024:** Lurie Children’s continues operations without access to EHR.
- **March 4, 2024:** Lurie Children’s electronic health record platform (Epic) was reactivated.
- **March 14, 2024:** Lurie Children’s began reactivating their patient portal (MyChart)



STATUS UPDATE AS OF 3 p.m. CST, February 22, 2024:

Thank you for your continued patience as Lurie Children's works to recover our systems. As a reminder, please bring your printed insurance card to each appointment and also bring your child's medication bottles or a complete list of their current medications.

At this time, MyChart is unavailable and we appreciate your patience as we work to resolve this issue. Also, due to our systems being offline, we are using manual processes that will result in longer wait times between the request and completion of prescription requests.

Please know that Lurie Children's is open and providing care to patients with as few disruptions as possible. Patients scheduled for procedures and appointments are still being asked to arrive as scheduled unless their care provider contacts them directly to reschedule. If you were notified that your appointment was canceled, we will contact you to reschedule your appointment once systems have been restored. We apologize for the inconvenience.

Patient-families and community providers can reach our call center at 1.800.543.7362, M-F: 8 a.m.-6 p.m.; Sat: 8 a.m.-1 p.m.; Sun: Closed. During the hours the Call Center is closed, please call the main operator at 312.227.4000. Due to high volumes, if you receive a busy signal, please try calling us back.

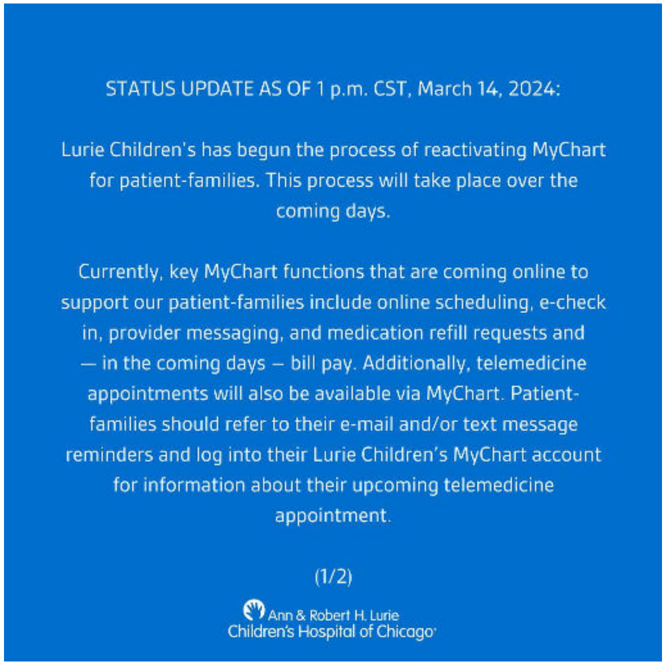
Ann & Robert H. Lurie
Children's Hospital of Chicago

(*Lurie Children’s Hospital’s X.com account*)

Lurie Children's Hospital of Chicago: Ransomware Attack Timeline (*Cyber Management Alliance*)

Ann & Robert H. Lurie Children's Hospital

Be prepared to pivot at a moment's notice. Recovery is not a quick flip of a switch.



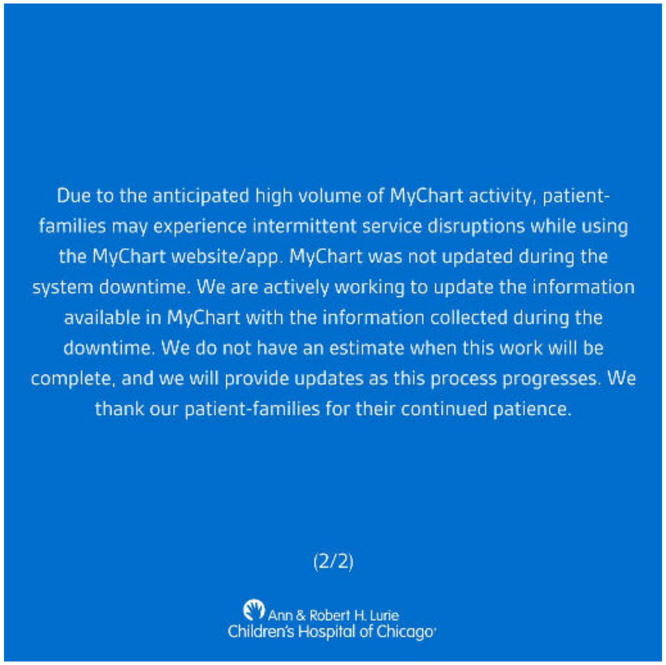
STATUS UPDATE AS OF 1 p.m. CST, March 14, 2024:

Lurie Children's has begun the process of reactivating MyChart for patient-families. This process will take place over the coming days.

Currently, key MyChart functions that are coming online to support our patient-families include online scheduling, e-check in, provider messaging, and medication refill requests and — in the coming days – bill pay. Additionally, telemedicine appointments will also be available via MyChart. Patient-families should refer to their e-mail and/or text message reminders and log into their Lurie Children's MyChart account for information about their upcoming telemedicine appointment.

(1/2)

Ann & Robert H. Lurie
Children's Hospital of Chicago



Due to the anticipated high volume of MyChart activity, patient-families may experience intermittent service disruptions while using the MyChart website/app. MyChart was not updated during the system downtime. We are actively working to update the information available in MyChart with the information collected during the downtime. We do not have an estimate when this work will be complete, and we will provide updates as this process progresses. We thank our patient-families for their continued patience.

(2/2)

Ann & Robert H. Lurie
Children's Hospital of Chicago

Can you go 33 days without access to your Electronic Health Records?

Change Healthcare

ALPHV/BlackCat Ransomware disrupted one of the worlds largest health payment processing companies

- **February 21, 2024:** Reports from Change Healthcare of a significant network interruption.
- **March 8, 2024:** Restoration of pharmacy services
- **March 15, 2024:** Restoration of electronic payment services
- **March 25, 2024 to April 21, 2024:** Restoration of additional key Change Healthcare products

The Impact

Patients:

- Inability to Process Claims
- Delayed or Denied Care
- Disruption in Pharmacy Services
- Financial Stress and Unexpected Costs
- Potential Data Privacy Concerns

Providers:

- Cash Flow Interruptions
- Furloughed Staff
- A Scramble for Loans

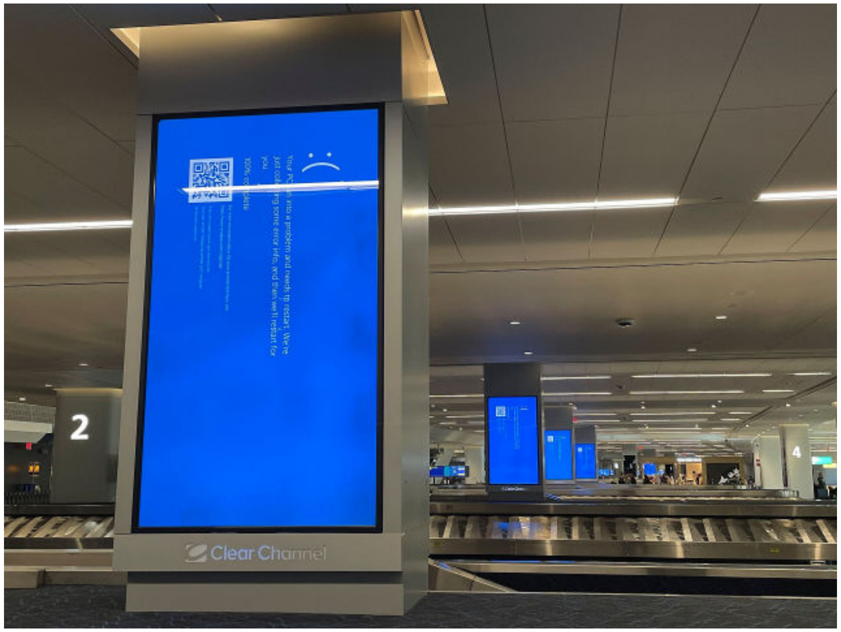
What We Learned: Change Healthcare Cyber Attack (House Committee on Energy and Commerce);

https://solution-status.optum.com/incidents/hqpjz25fn3n7

Not all large-scale cyber incidents are attacks

CrowdStrike Global IT Outage

International Blue Screen of Death (BSOD) day – July 19, 2024



LaGuardia Airport, New York City ***(Wikipedia)***

Sydney, Australia ***(Stella Qiu, Reuters)***

https://en.wikipedia.org/wiki/2024_CrowdStrike_incident#Healthcare

CrowdStrike Global IT Outage

What Happened?

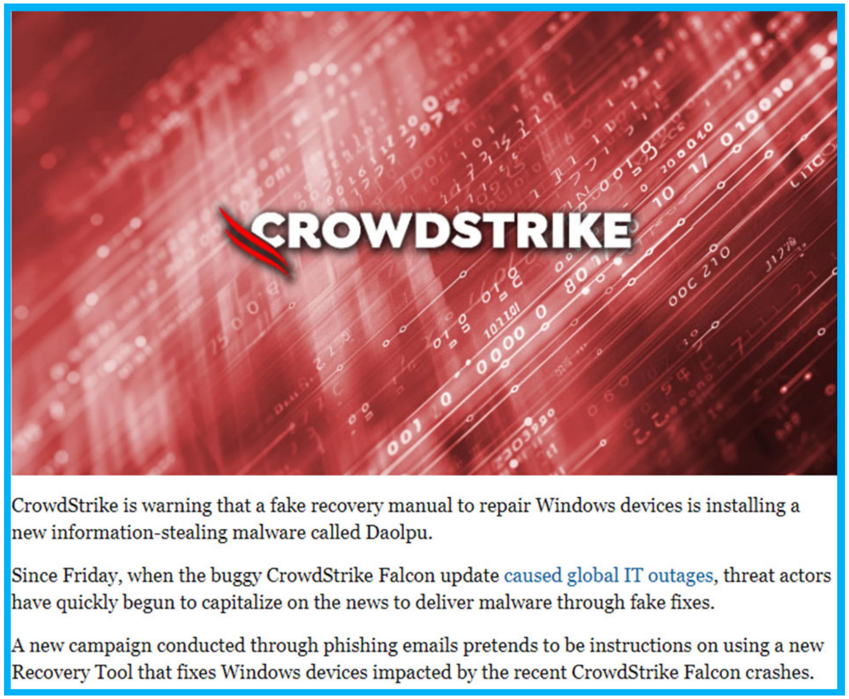
A software update caused millions of Windows users globally to experience the dreaded Blue Screen of Death, leading to system shutdowns, and a "Boot-Loop"

This caused widespread disruption affecting travel, shopping, banking, business operations and so much more.

Concerningly, the disruption impacted Emergency Services, Hospitals, and critical infrastructure.

This was **NOT** an attack. Instead, this was an error attributed for the time being to processes involved in "pushing" updates.

Criminals and other threat groups were equally surprised by this outage. However, they jumped on the opportunities opened.



CrowdStrike is warning that a fake recovery manual to repair Windows devices is installing a new information-stealing malware called Daolpu.

Since Friday, when the buggy CrowdStrike Falcon update caused global IT outages, threat actors have quickly begun to capitalize on the news to deliver malware through fake fixes.

A new campaign conducted through phishing emails pretends to be instructions on using a new Recovery Tool that fixes Windows devices impacted by the recent CrowdStrike Falcon crashes.

Fake CrowdStrike repair manual pushes new infostealer malware (Bleeping Computer)

CrowdStrike Global IT Outage

An easy fix in most cases, but a nightmare at scale.

https://beazley.security/alerts-advisories/guidance-support-windows-systems-experiencing-boot-loop-due-to-crowdstrike-update

CrowdStrike Global IT Outage

Notable Impacted Health Systems

- Kaiser Permanente
- Providence
- Henry Ford Health
- Nationwide Children’s Hospital
- Dana-Farber Cancer Institute
- RWJBarnabas Health
- Emory Healthcare
- Mass General Brigham
- Norton Healthcare
- Penn Medicine
- Seattle Children’s Hospital

The Disruption

- Canceled or Delayed Procedures
- Delayed Cases at Ambulatory Surgery Centers
- Delayed Lab and Pharmacy orders
- Implemented Downtime Procedures for Clinics

CrowdStrike outage hits US hospitals (Healthcare Dive)

4 Things to know About the CrowdStrike IT Outage's Effect on Healthcare (MedCity News)

CrowdStrike Global IT Outage

Notable Impacted Health Systems

- Kaiser Permanente
- **Providence**
- Henry Ford Health
- Nationwide Children's Hospital
- Dana-Farber Cancer Institute
- RWJBarnabas Health
- Emory Healthcare
- Mass General Brigham
- Norton Healthcare
- Penn Medicine
- Seattle Children's Hospital

The Impact

- Approximately 15,000 servers
- Approximately 40,000 of 150,000 devices

The Response

- Between July 19th and July 24th Providence leveraged more than 1,000 team members and volunteers to achieve 90% remediation of impacted systems.

"This is worse than a cyberattack" – Providence CIO, B.J. Moore

Hospitals Cancel Nonessential Surgeries After Global Technology Outage (New York Times)

Update: Providence response to CrowdStrike outage (Providence)

Looking Forward

Notice of Proposed Rulemaking (NPRM)

Published: January 6, 2025

Comment Period Closed: March 7, 2025

Comments: 4,745

Will it be shelved?

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
Office for Civil Rights

What are the proposed changes/requirements?

- Written documentation of all security rule policies
- Planning for contingencies and responding to security incidents
  - Procedures to restore the loss of Electronic Information Systems (EIS)
  - Written security incident response plans (IRPs)
  - Written procedures for testing and revising IRPs
- Annual Compliance Audits
- Technical Controls
  - Anti-malware protection
  - Disabling network ports
  - Multi-Factor Authentication
  - Vulnerability scanning and penetration testing
  - Network segmentation

https://www.hhs.gov/hipaa/for-professionals/security/hipaa-security-rule-nprm/factsheet/index.html

Cyber Security Health Check:

- Establish a Security Culture
- Protect Mobile Devices
- Maintain Good Computer Habits
- Use a Firewall
- Install and Maintain Anti-Virus Software
- Plan for the Unexpected
- Control Access to Protected Health Informaiton
- Use Strong Passwords and Change Them Regularly
- Limit Network Access and Control Physical Access

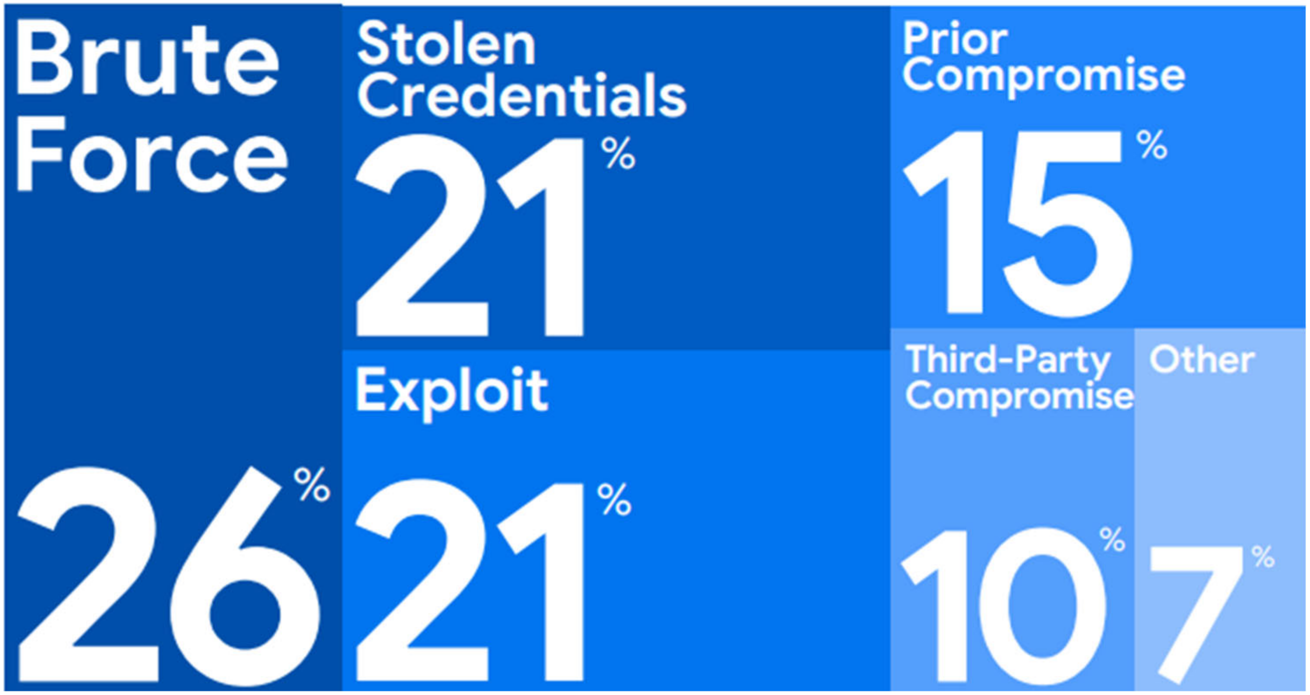
https://www.healthit.gov/sites/default/files/Top_10_Tips_for_Cybersecurity.pdf

Threats to Small Practices

Ransomware:

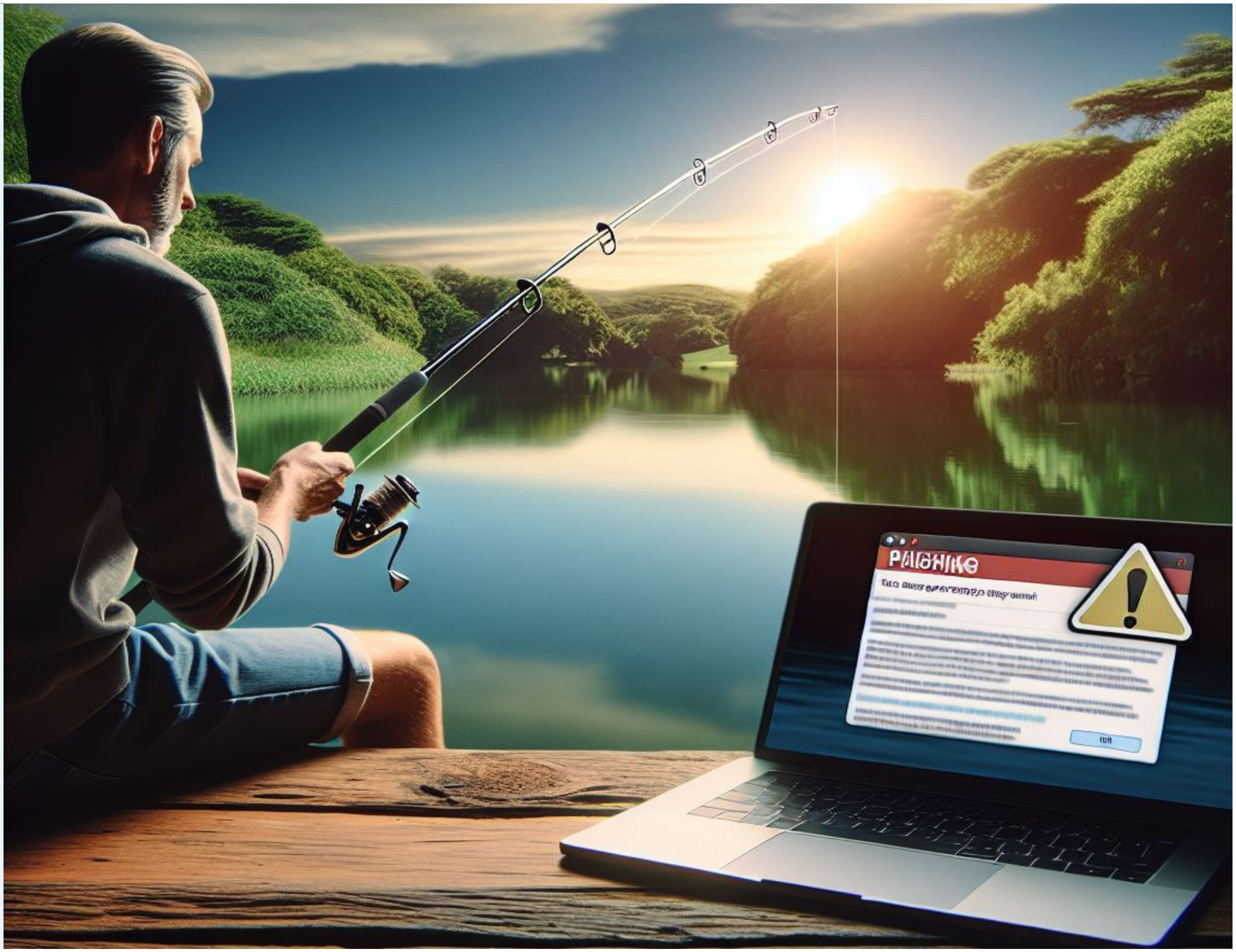
Initial Infection Vector, 2024

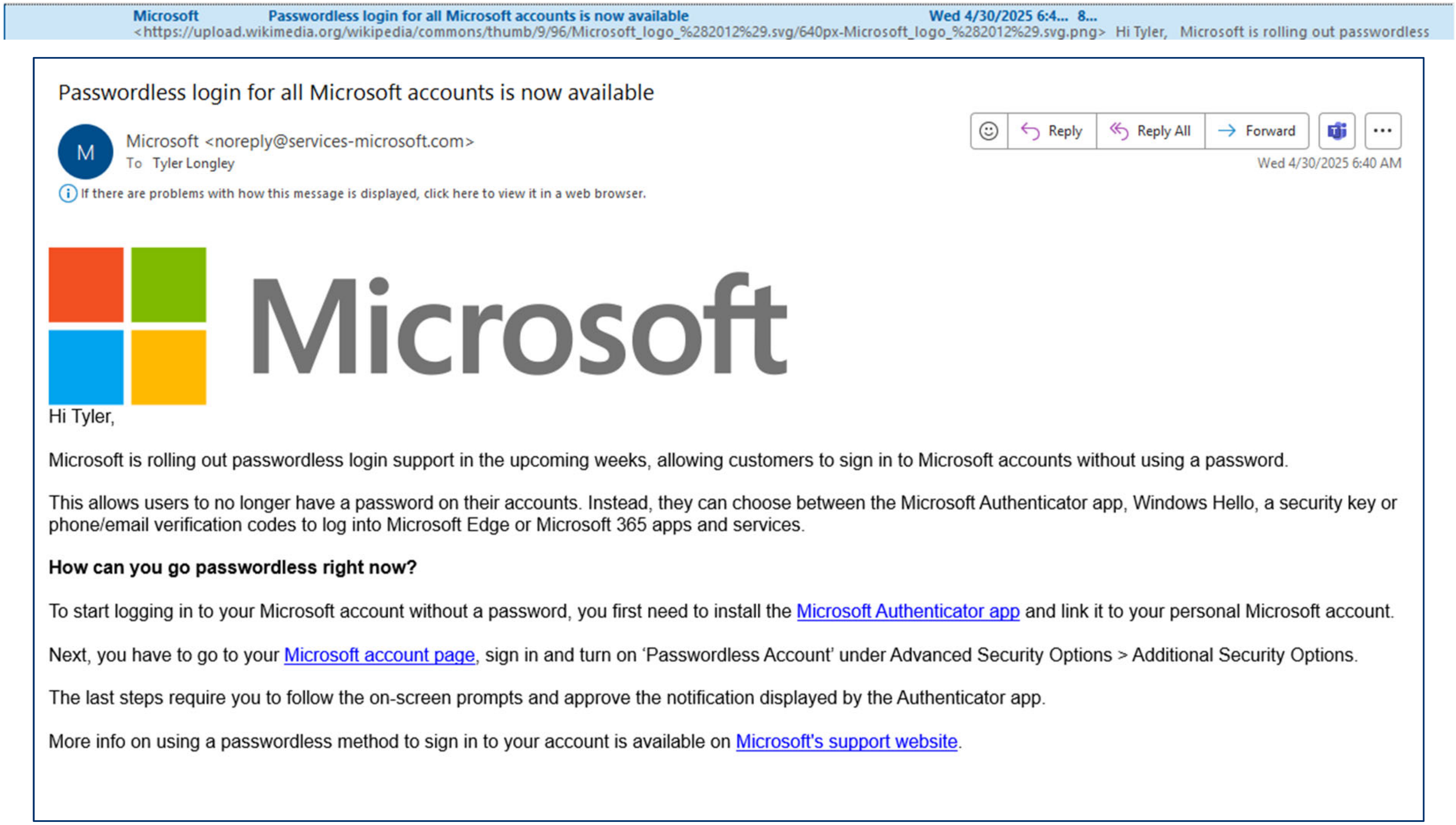
Ransomware-Related



Mandiant’s 2025 M-Trends Report

Phishing:





Microsoft Passwordless login for all Microsoft accounts is now available Wed 4/30/2025 6:4... 8...
<https://upload.wikimedia.org/wikipedia/commons/thumb/9/96/Microsoft_logo_%282012%29.svg/640px-Microsoft_logo_%282012%29.svg.png> Hi Tyler, Microsoft is rolling out passwordless

Passwordless login for all Microsoft accounts is now available

Microsoft <noreply@services-microsoft.com>
To Tyler Longley

Wed 4/30/2025 6:40 AM

If there are problems with how this message is displayed, click here to view it in a web browser.

Microsoft

Hi Tyler,

Microsoft is rolling out passwordless login support in the upcoming weeks, allowing customers to sign in to Microsoft accounts without using a password.

This allows users to no longer have a password on their accounts. Instead, they can choose between the Microsoft Authenticator app, Windows Hello, a security key or phone/email verification codes to log into Microsoft Edge or Microsoft 365 apps and services.

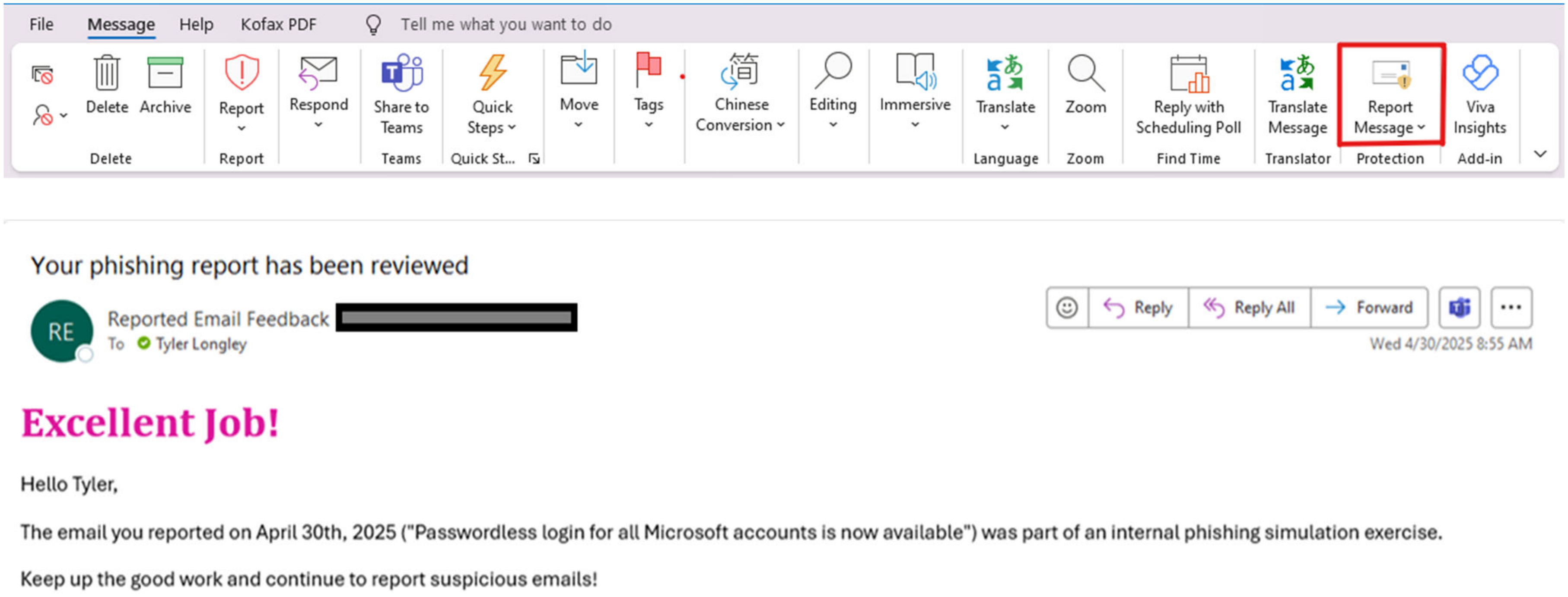
How can you go passwordless right now?

To start logging in to your Microsoft account without a password, you first need to install the Microsoft Authenticator app and link it to your personal Microsoft account.

Next, you have to go to your Microsoft account page, sign in and turn on ‘Passwordless Account’ under Advanced Security Options > Additional Security Options.

The last steps require you to follow the on-screen prompts and approve the notification displayed by the Authenticator app.

More info on using a passwordless method to sign in to your account is available on Microsoft's support website.



Your phishing report has been reviewed

RE Reported Email Feedback [redacted]
To Tyler Longley

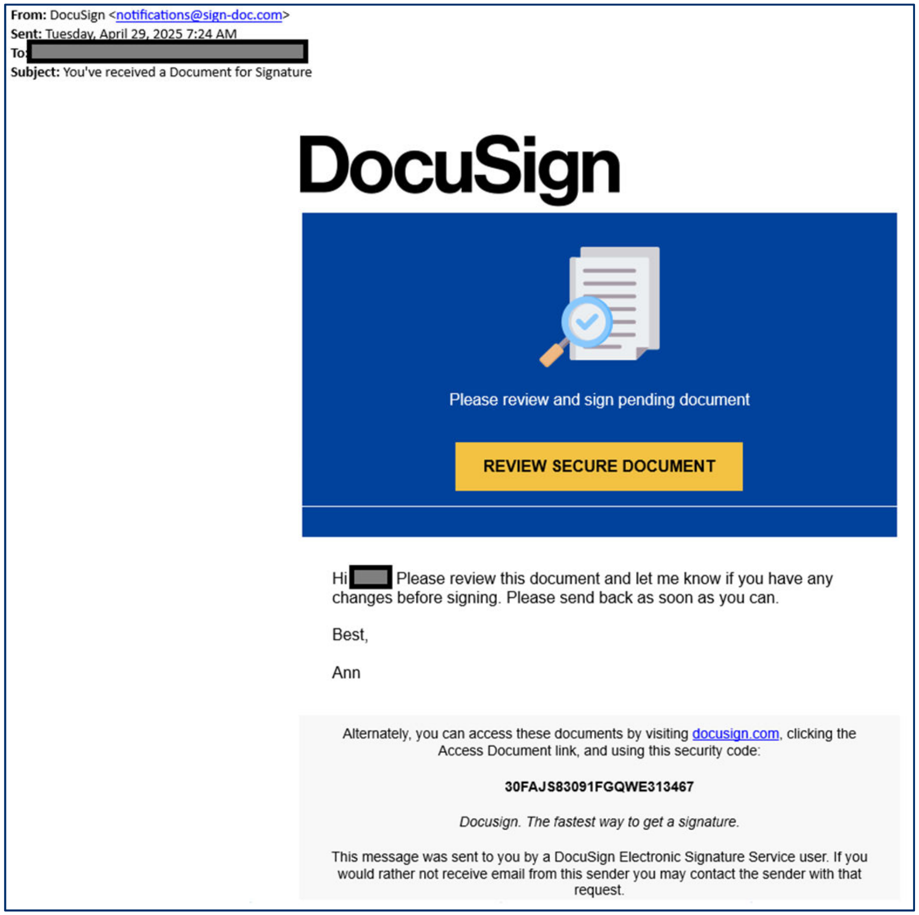
Wed 4/30/2025 8:55 AM

Excellent Job!

Hello Tyler,

The email you reported on April 30th, 2025 ("Passwordless login for all Microsoft accounts is now available") was part of an internal phishing simulation exercise.

Keep up the good work and continue to report suspicious emails!



From: DocuSign <notifications@sign-doc.com>
Sent: Tuesday, April 29, 2025 7:24 AM
To: [redacted]
Subject: You've received a Document for Signature

DocuSign

Please review and sign pending document

REVIEW SECURE DOCUMENT

Hi [redacted] Please review this document and let me know if you have any changes before signing. Please send back as soon as you can.

Best,

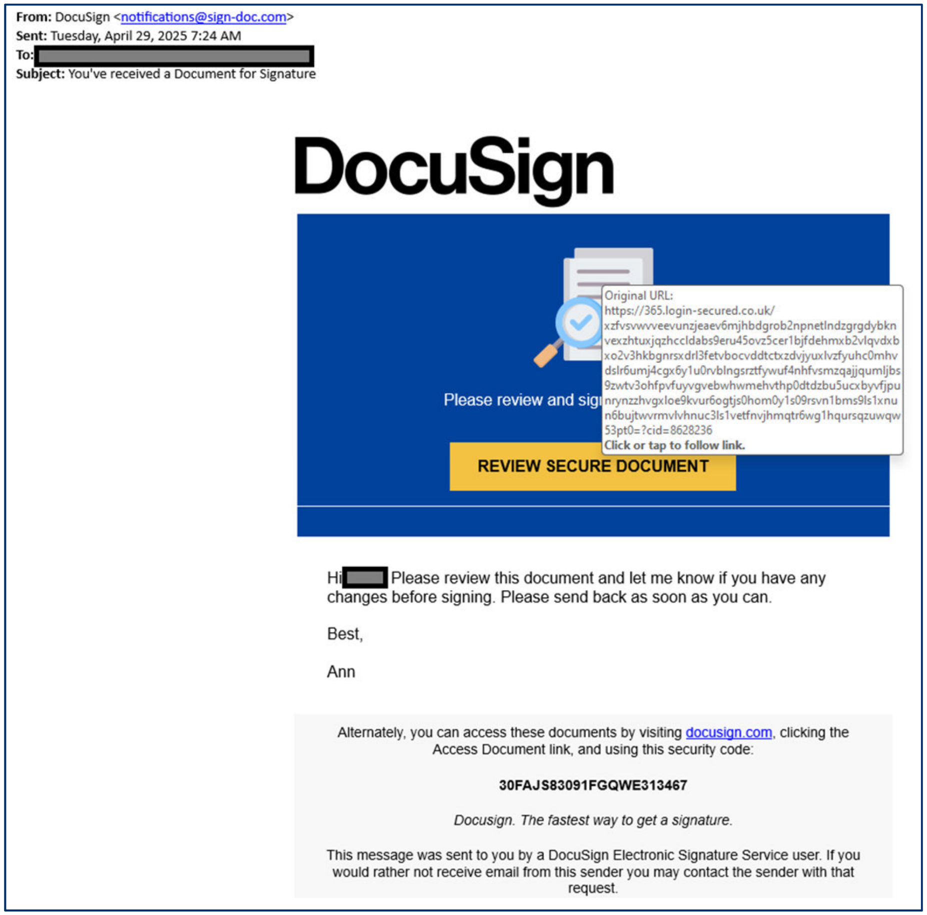
Ann

Alternately, you can access these documents by visiting docusign.com, clicking the Access Document link, and using this security code:

30FAJS83091FGQWE313467

Docusign. The fastest way to get a signature.

This message was sent to you by a DocuSign Electronic Signature Service user. If you would rather not receive email from this sender you may contact the sender with that request.



From: DocuSign <notifications@sign-doc.com>
Sent: Tuesday, April 29, 2025 7:24 AM
To: [redacted]
Subject: You've received a Document for Signature

DocuSign

Original URL:
https://365.login-secured.co.uk/
xzfvsvwvveevunzjeaev6mjhbdgrob2npnetlndzgrgdybkn
vexzhtuxjqzhccldabs9eru45ovz5cer1bjfdehmxb2vlqvdxb
xo2v3hkbgnrsxdrl3fetvbocvddtctxzdvjyuxlvzfyuhc0mhv
dslr6umj4cgx6y1u0rvblngsrztfywuf4nhfvsmzqajjqumljbs
9zwtv3ohfpvfuyvgvebwhwmehvthp0dtdzbu5ucxbyvfjpu
nrynzzhvgxloe9kvur6ogtjs0hom0y1s09rsvn1bms9ls1xnu
n6bujtwvrmvlvhnuc3ls1vetfnvjhmqtr6wg1hqursqzuwqw
53pt0=?cid=8628236
Click or tap to follow link.

Please review and sig

REVIEW SECURE DOCUMENT

Hi [redacted] Please review this document and let me know if you have any changes before signing. Please send back as soon as you can.

Best,

Ann

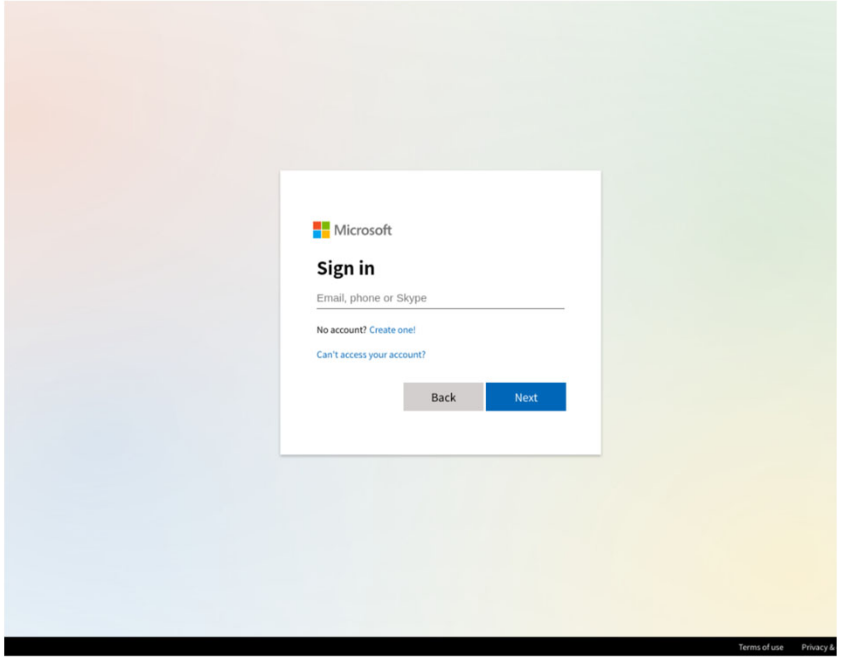
Alternately, you can access these documents by visiting docusign.com, clicking the Access Document link, and using this security code:

30FAJS83091FGQWE313467

Docusign. The fastest way to get a signature.

This message was sent to you by a DocuSign Electronic Signature Service user. If you would rather not receive email from this sender you may contact the sender with that request.

Threats Hiding In Plain Sight



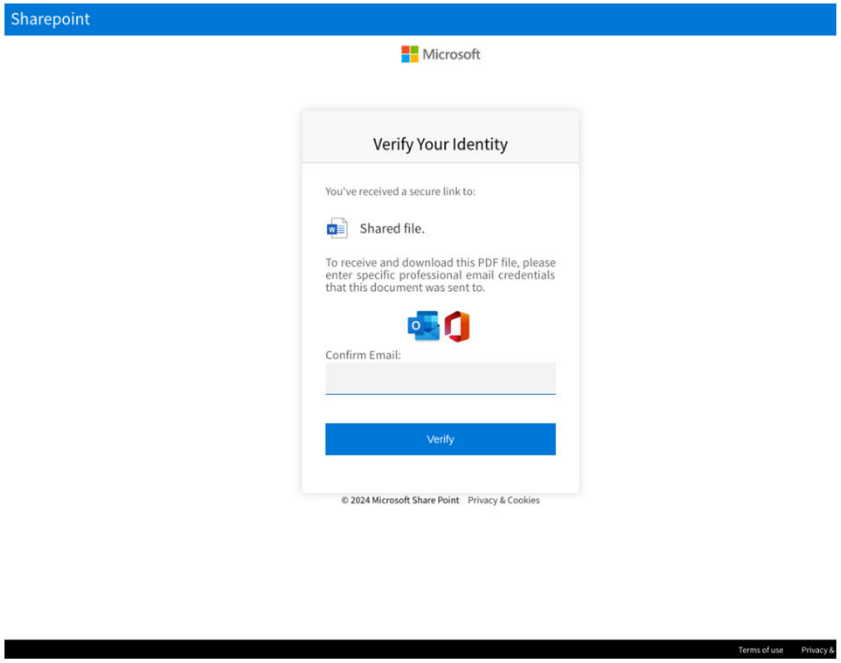
Microsoft

Sign in

Email, phone or Skype

No account? Create one!

Can't access your account?



Sharepoint

Microsoft

Verify Your Identity

You've received a secure link to:

Shared file.

To receive and download this PDF file, please enter specific professional email credentials that this document was sent to.

Confirm Email:

© 2024 Microsoft Share Point Privacy & Cookies

LabHost Phaas (2021 – 2024)

- 365-online-login.co
- 365-secure.online
- chase-authentication.com
- login.auth-chase.com
- bankofamerica-secured.com
- myappledevice.info
- auth-scotiabankonline.com

https://www.ic3.gov/CSA/2025/250429.pdf

Spot The Difference:

@Beazley.com	@Baezley.com
@Netfliix.com	@Netflix.com
@0nedrive.com	@Onedrive.com
@rnicrosoft.com	@microsoft.com
@gmail.com	@gmail.com

Phishing of all shapes and sizes:

Urgent or Threatening Language

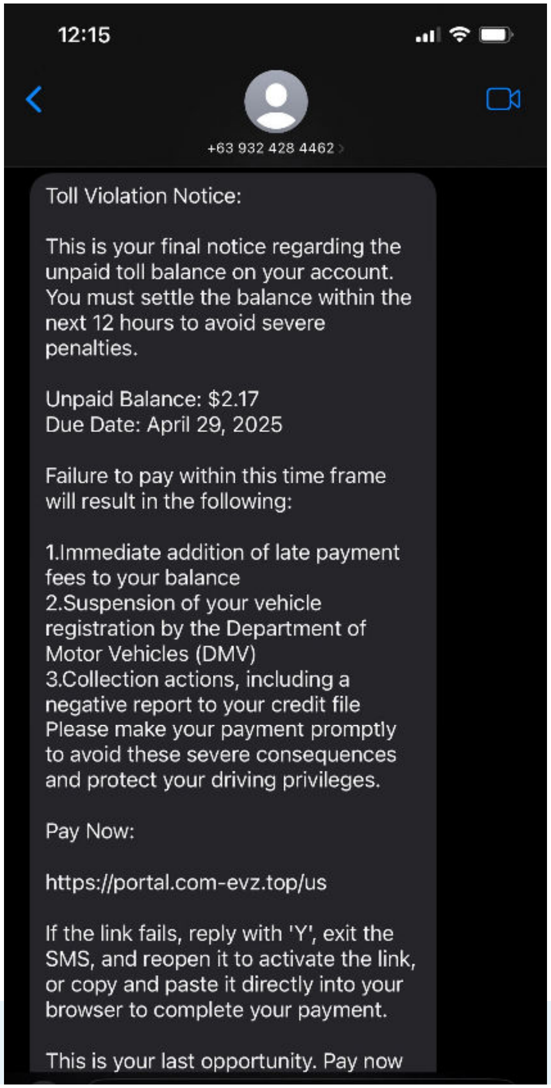
- 12 Hours to respond
- “Pay Now”
- Threats of registration suspension

Exploitation of Trust

- Purports to be a trusted entity

Creation of a False Sense of Legitimacy

- Convincing but generic website link



Toll Violation Notice:

This is your final notice regarding the unpaid toll balance on your account. You must settle the balance within the next 12 hours to avoid severe penalties.

Unpaid Balance: $2.17
Due Date: April 29, 2025

Failure to pay within this time frame will result in the following:

1.Immediate addition of late payment fees to your balance
2.Suspension of your vehicle registration by the Department of Motor Vehicles (DMV)
3.Collection actions, including a negative report to your credit file
Please make your payment promptly to avoid these severe consequences and protect your driving privileges.

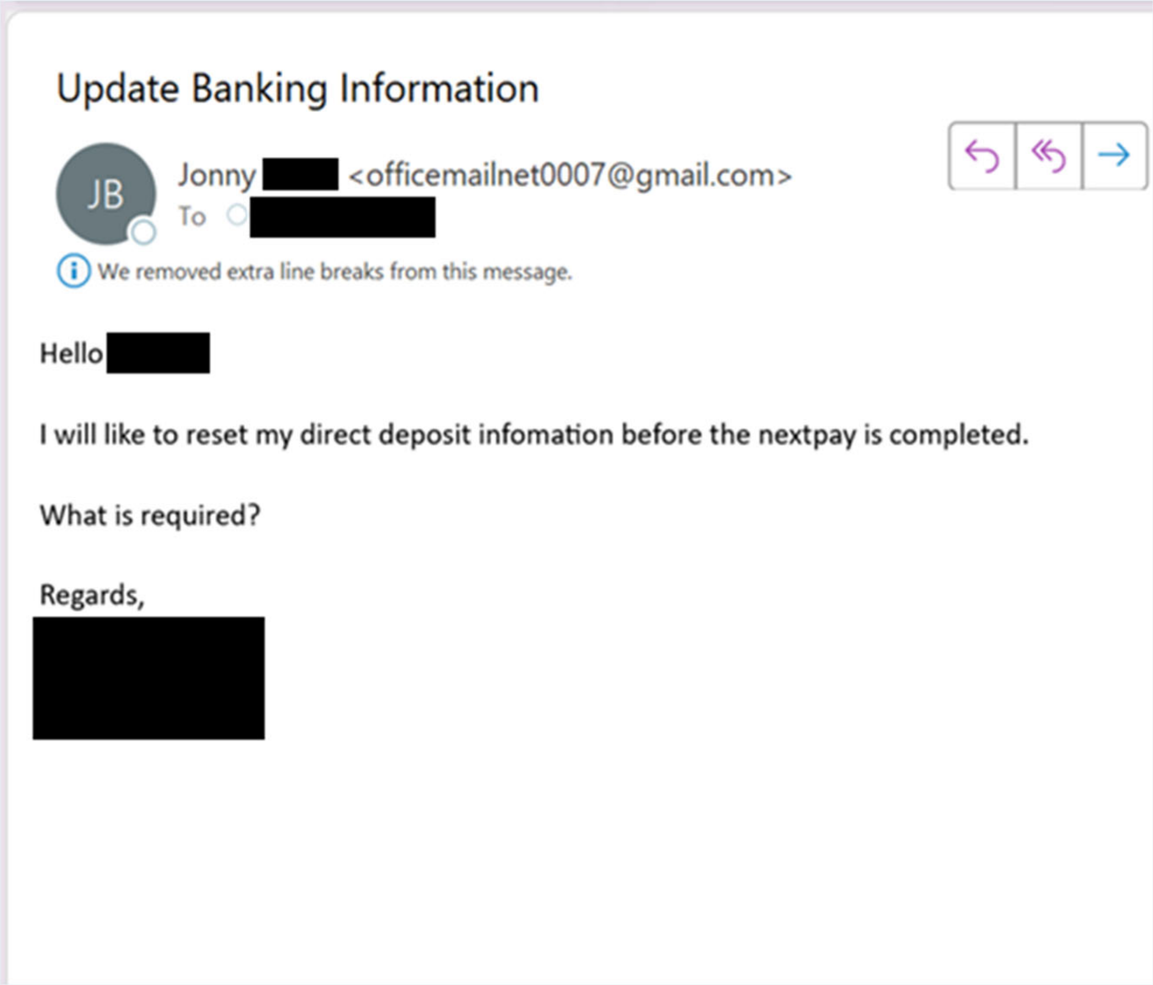
Pay Now:

https://portal.com-evz.top/us

If the link fails, reply with 'Y', exit the SMS, and reopen it to activate the link, or copy and paste it directly into your browser to complete your payment.

This is your last opportunity. Pay now

Payroll Redirect & Fraudulent Instruction Schemes



Update Banking Information

Jonny [redacted] <officemailnet0007@gmail.com>

To [redacted]

We removed extra line breaks from this message.

Hello [redacted]

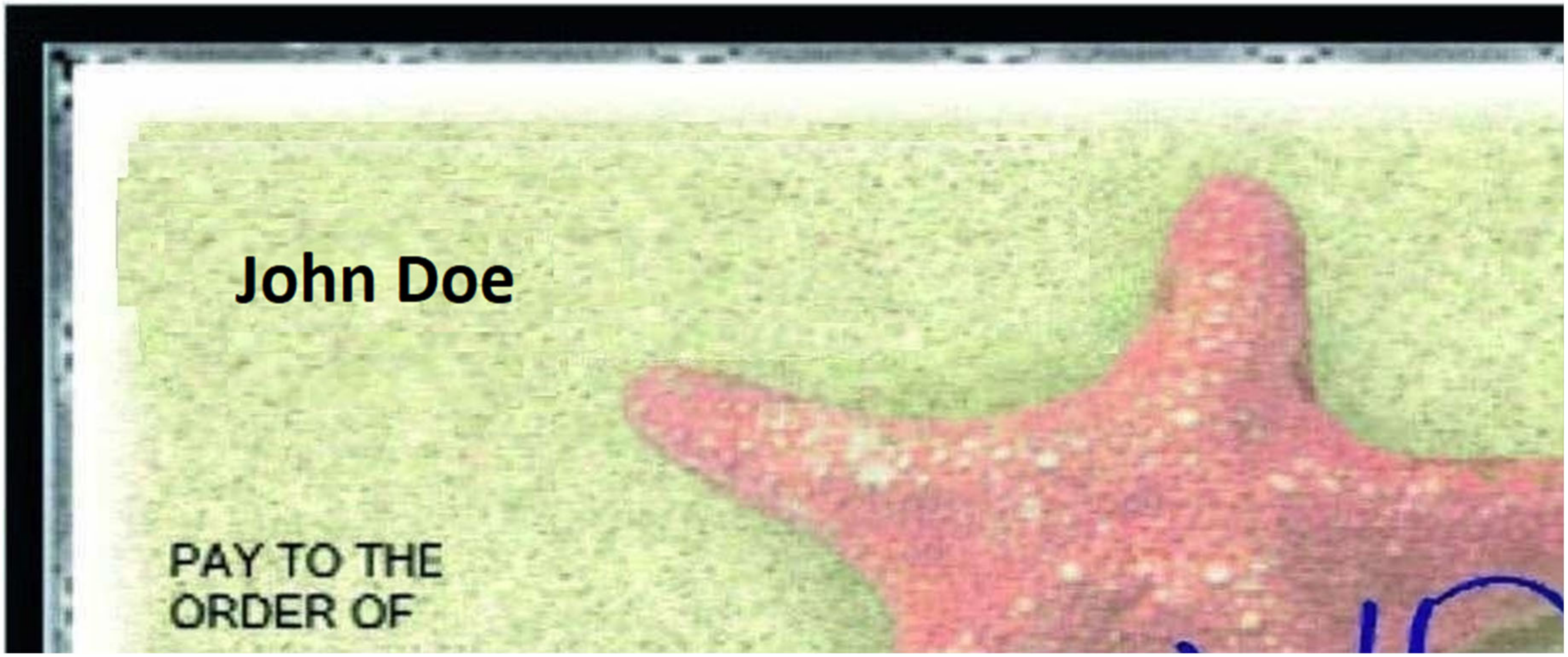
I will like to reset my direct deposit infomation before the nextpay is completed.

What is required?

Regards,

[redacted]

Spotting the Issues:



John Doe

PAY TO THE
ORDER OF

Incident Response & Business Continuity Planning

“If you fail to plan, you are planning to fail!”
— Benjamin Franklin

Only 63% of Healthcare organizations have a cybersecurity response plan in place

Software Advice’s 2024 Healthcare Data Security Survey

Incident Response Planning

You Do Not Need To Reinvent The Wheel When Creating An Incident Response Plan (IRP)

Overlooked Questions:

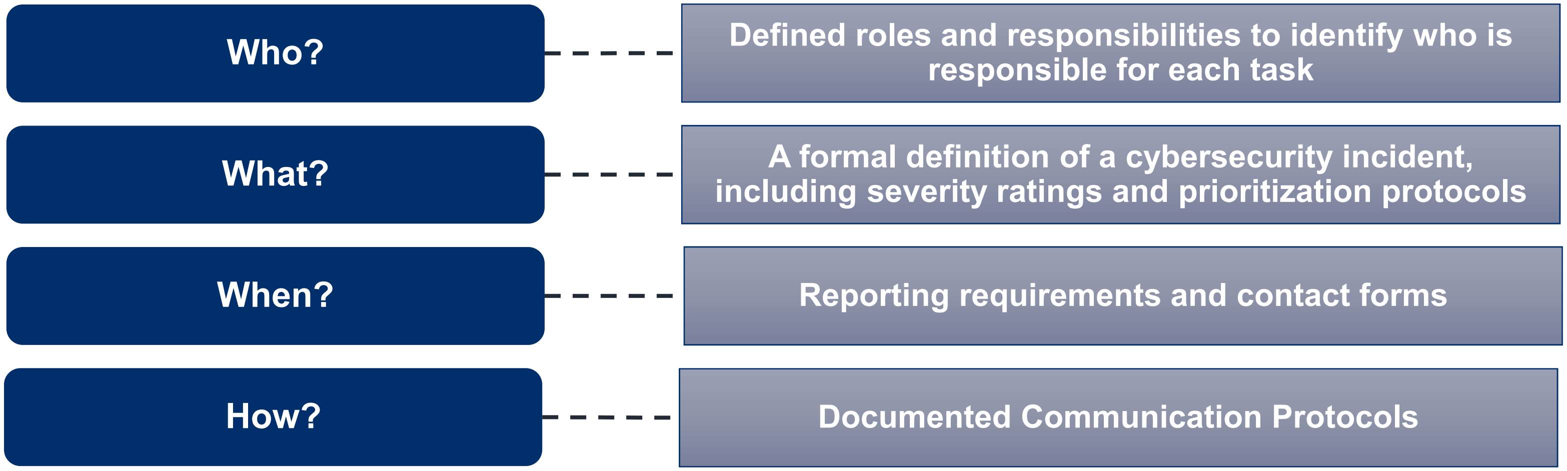
- **Do you have an Incident Response Plan?**
  - Where is it?
  - Who is the first person you contact?
    - How do you contact them?
  - What is your involvement in the IRP?
- **Do you have Cyber Insurance?**
  - Where is your policy?
  - How do you contact your insurer?
  - Do you have a panel requirement?

There Are Many Tried and Tested IRP templates

Incident Response Plan (IRP) Basics (CISA.gov)

Incident Response Planning

An incident response plan should ideally include:



Who?	Defined roles and responsibilities to identify who is responsible for each task
What?	A formal definition of a cybersecurity incident, including severity ratings and prioritization protocols
When?	Reporting requirements and contact forms
How?	Documented Communication Protocols

Incident Response Planning

Who is on your incident response team?

The Incident Response Team May Be:

- Legal
- Information Security/Information Technology
- Risk Management
- Communications
- Human Resources
- Privacy Office
- Physical Security
- Business Continuity

Or It Could Be:

- Practice Owner
- Practice Manager
- Internal/External IT Manager

Create the team that is right for your organization!

https://www.softwareadvice.com/resources/healthcare-cybersecurity-threat/

Business Continuity Planning

How do you keep moving forward during and after a cyber incident?

Business Continuity Planning

Uninterrupted patient care during and after a cyber incident is crucial

Operational Continuance

- What is your ability to see patients without an EMR?
- Do you retain paper records or on-prem backups?
- How can you coordinate scheduling?

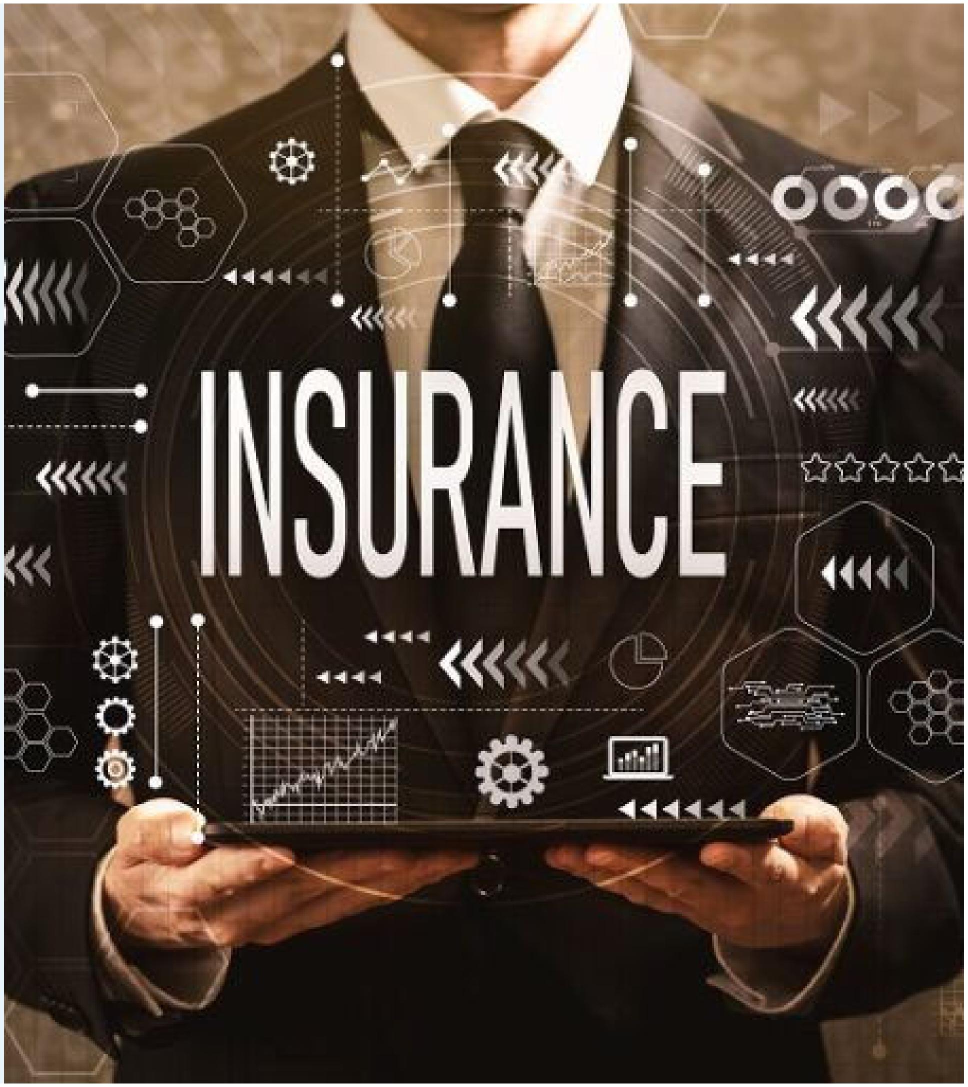
Third-Party Dependency

- What aspects of your practice rely on vendors?
- Are most systems with one vendor?

Financial Continuity

- How long can you go without processing claims?
- Do you have easy access to loans or lines of credit?

When To Notify Insurance



When To Notify Insurance

Use your judgement:

- Does the situation have the potential to result in an insurance claim

Notify out of an abundance of caution:

- Untimely reporting may lead to coverage issues
- Notifying out of an abundance of caution is often better than holding onto a claim

Avoid negative implications of responding on your own:

- Does your policy have a consent requirement?
- Does your policy have a panel requirement?
- Did you wipe systems and jeopardize a forensic investigation?
- Did you over notify?
- Did you exceed your notification window?

If you see something, say something!

Tyler Longley

Assistant Claims Manager

BPS Cyber & Technology | Claims

West Hartford, CT
Tyler.Longley@Beazley.com

beazley