INVESTING IN YOUR IT INFRASTRUCTURE:

SURVIVING A RANSOMWARE ATTACK

LESSONS LEARNED AFTER AN LPHA SUSTAINED A CYBER SECURITY BREACH

STEVE SIKES

EXECUTIVE DIRECTOR

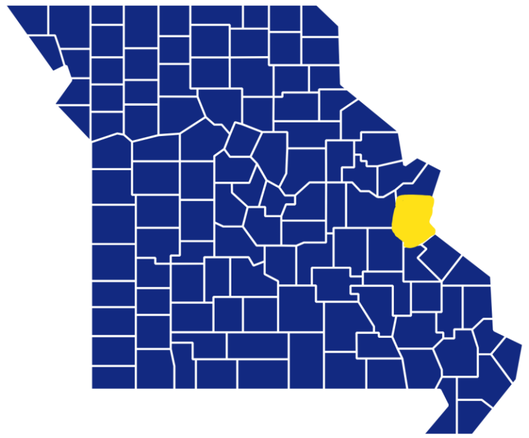
STEVE FERRY

IT MANAGER

Jefferson County Health DEPARTMENT

WHO ARE WE & WHO DO WE SERVE?

- Population 231,230
- 6th most populated county
- Urban/Rural County
- Two Office Locations and 3 Mobile Units
  - Mobile Heath Center
  - Dental Van
  - Medical Day Van



Our New Home

WHAT DO YOU THINK?

Scan to vote

How many of you have been affected by a Personal Data Breach?

Data Breach: A security incident where private or sensitive information is accessed, stolen, exposed, or disclosed without authorization by an unauthorized party.

How many of you have experienced a Data Breach event at work?

WHAT DO YOU THINK?

WHAT DO YOU THINK?

CTRL + ALT + AGENDA

- **JCHD DATA BREACH**
  - Review our pre-breach IT Infrastructure
  - Before the storm – Events Leading into the Breach
  - Review Data Breach and Response
  - Discuss Key Partners
  - Lessons Learned
  - Q&A

PRE-BREACH IT INFRASTRUCTURE

STAFFING

- **Internal IT Team**
  - 2 staff members: **IT Manager** and **IT Support Specialist**
  - Coverage includes **2 buildings** and **Mobile Health Units** across the county
- **Staffing Timeline**
  - **Steve Ferry** joined as IT Support Specialist in **March 2022**
  - **IT Manager** left in **April 2022**
  - Due to limited internal resources, a **Managed Service Provider (MSP)** was contracted
- **MSP Responsibilities**
  - Operates a **Support Service Desk** for complex IT issues
  - Manages **Datto backups**
  - Performs **PC and server updates/patching**
  - Assists with **network configuration and monitoring**
  - Manages our Endpoint Detection Response (EDR) **Datto**
  - Works with a Security Operations Center (SOC) for **Cybersecurity Threats**

PRE-BREACH IT INFRASTRUCTURE

CLOUD-BASED SAAS APPLICATIONS AT JCHD

- JCHD uses various **Software as a Service (SaaS)** tools for operations
- Examples include:
  - **Microsoft Office 365**
  - **Adobe Acrobat**
  - **Datto**
  - **CureMD EHR**
  - **Curve Dental**
  - **Citizen Serve**
  - **MIP**

SHAREPOINT FOR COVID RESPONSE

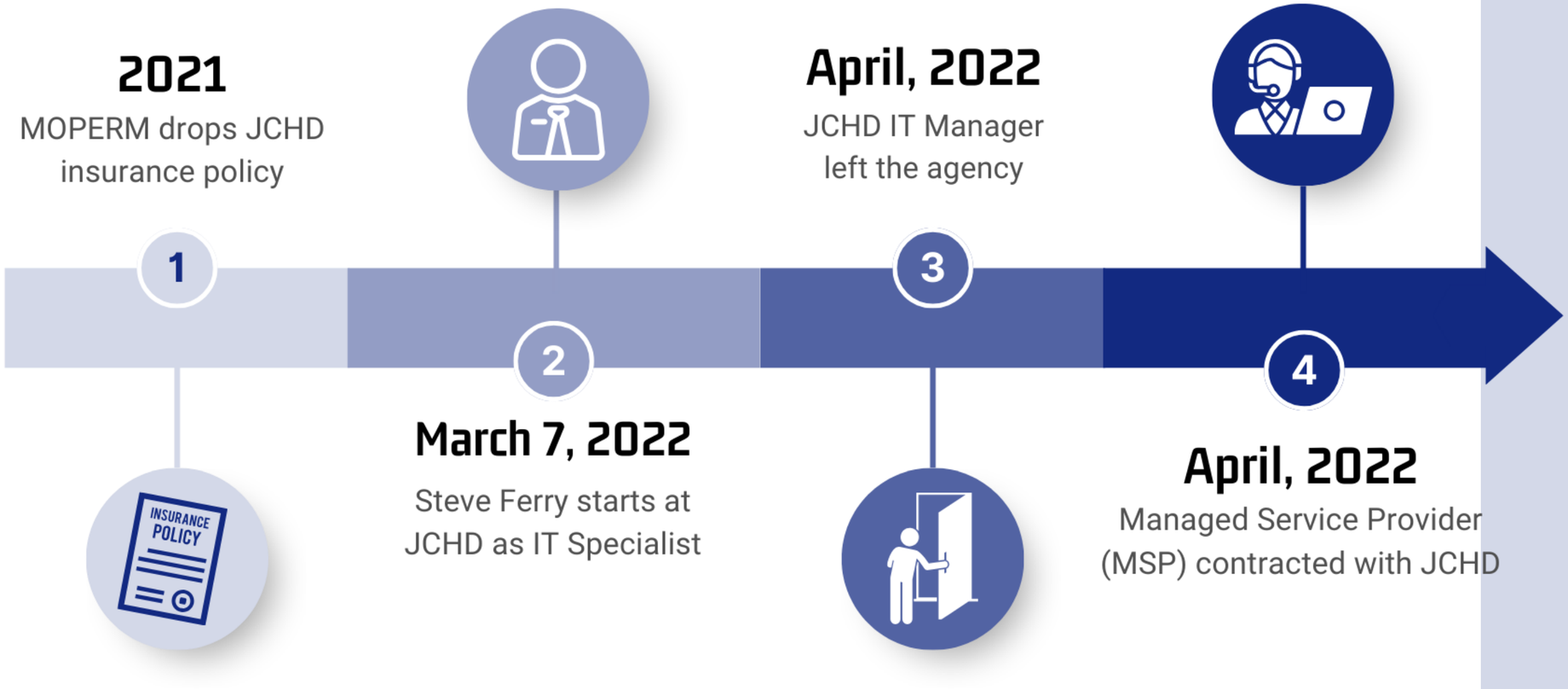
- SharePoint used within Office 365 for remote collaboration
- Enabled staff to work together without being physically present
- Reduced reliance on on-premise data storage

SYSTEM BACK-UPS

- JCHD uses Datto for third-party data backup
- Server data is backed up hourly
- Backups are stored locally and in the cloud
- Supports disaster recovery and ensures data redundancy

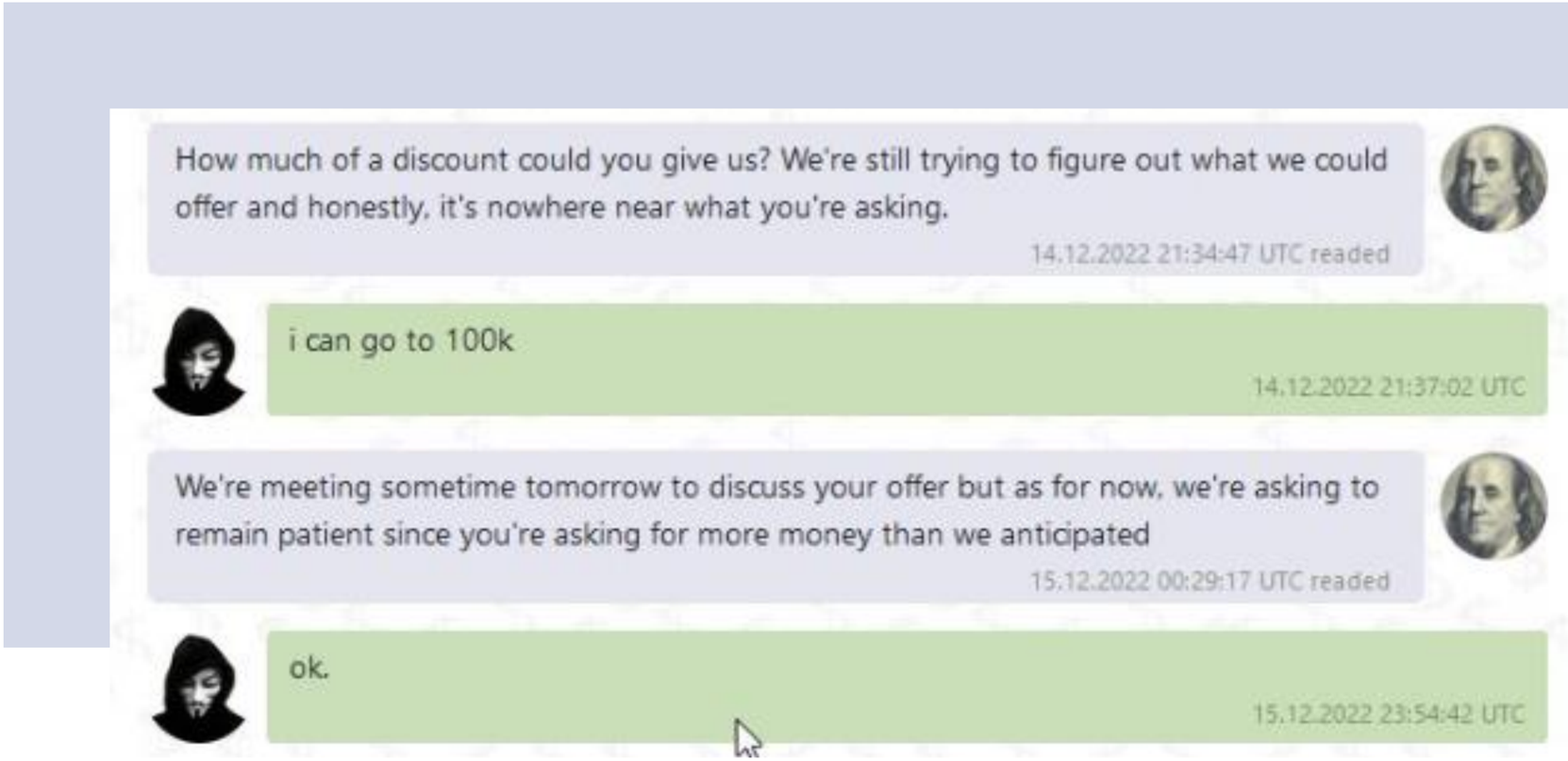
BEFORE THE STORM.EXE

- Received notice in 2021 from MOPERM they would no longer provide cybersecurity insurance starting in 2022. Applied with other carriers for coverage.
- IT Manager parted ways with JCHD – used a Managed Service Provider
- Breach occurred November of 2022



THE BREACH BRIEF

- Date we discovered attack:
  - November 15, 2022
- Ransom letter from Threat Actor (TA) LockBit 3.0 $1 million for code to unlock encryption
- Worked with our Managed Service Provider (MSP)



2021

MOPERM drops JCHD insurance policy

1

2

March 7, 2022

Steve Ferry starts at JCHD as IT Specialist

April, 2022

JCHD IT Manager left the agency

3

4

April, 2022

Managed Service Provider (MSP) contracted with JCHD

Oct. 31, 2022

Earliest indicator of compromise

5

6

Nov. 15, 2022

MSP notifies JCHD of unusual activity and insurance contacted

Nov. 16, 2022

Breach Counsel acquired and Incident Response Team activated

7

Key Partners

- **Insurance Breach Counsel**
  - Worked with the FBI and forensic team
  - Created email addresses outside our infrastructure

- **Forensic Team**
  - Investigated how they gained access
  - Negotiated with TA
  - TA stated they did not take data, only encrypted it
  - Provided a detailed report to help with reporting incident to The Office of Civil Rights (OCR)

2021
MOPERM drops JCHD insurance policy

1

2

March 7, 2022
Steve Ferry starts at JCHD as IT Specialist

April, 2022
JCHD IT Manager left the agency

3

4

April, 2022
Managed Service Provider (MSP) contracted with JCHD

Oct. 31, 2022
Earliest indicator of compromise

5

6

Nov. 15, 2022
MSP notifies JCHD of unusual activity and insurance contacted

Nov. 16, 2022
Breach Counsel acquired and Incident Response Team activated

7

Jan. 13, 2023
Adult and minor notification of breach

8

9

Jan. 24, 2023
Notification of breach in newspapers

Jan. 30, 2023
JCHD served with a lawsuit

10

11

March 17, 2023
Office of Civil Rights (OCR) was notified of breach

April, 2023
JCHD conducted Security Risk Analysis (SRA)

12

13

May, 2023
JCHD implemented regular HIPAA Policy reviews

- **Office of Civil Rights (OCR) – Health and Human Services (HHS)**
  - Followed HIPAA Breach Notification Rule
    - (45 CFR §§ 164.400–414)
  - Worked with breach counsel to guide process and create report
  - Reported to multiple states with varying timelines
  - Sent notification letters to affected clients
  - Established a call center (covered by insurance) for questions
  - Reviewed IT systems, training, and policies back to 2016
  - Completed a HIPAA Security Risk Analysis
  - Reviewed and updated Business Associate Agreements (BAAs)

LAWSUIT:

- Class Action Lawsuit – Can’t discuss details
- Currently still not settled
- Staff were deposed (thorough review of our IT policies and procedures, Risk Analysis, and training for past 7 years.)
  - HIPAA Security Officer
  - HIPAA Privacy Officer
- Mediation discussions

FROM GLITCH TO GROWTH

Lessons Learned

HAVE GOOD INSURANCE COVERAGE

Review your Cyber Security Policy

1. Breach Counsel
2. Forensic Expenses
3. Notification Expenses
4. Call Center
5. Post-event Monitoring Expenses
6. Extortion Threats
7. Defense and Settlement

FROM GLITCH TO GROWTH

Lessons Learned

Security Measures

- Implemented Multi Factor Authentication (MFA)
- Provided a Password Manager for All Staff
- Strengthened our Password Requirements

DON'T BE THE WEAKEST LINK

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	57 minutes	2 hours	4 hours
6	Instantly	46 minutes	2 days	6 days	2 weeks
7	Instantly	20 hours	4 months	1 year	2 years
8	Instantly	3 weeks	15 years	62 years	164 years
9	2 hours	2 years	791 years	3k years	11k years
10	1 day	40 years	41k years	238k years	803k years
11	1 weeks	1k years	2m years	14m years	56m years
12	3 months	27k years	111m years	917m years	3bn years
13	3 years	705k years	5bn years	56bn years	275bn years
14	28 years	18m years	300bn years	3tn years	19tn years
15	284 years	477m years	15tn years	218tn years	1qd years
16	2k years	12bn years	812tn years	13qd years	94qd years
17	28k years	322bn years	42qd years	840qd years	6qn years
18	284k years	8tn years	2qn years	52qn years	463qn years

Time it takes a hacker to brute force your password in 2025

Hardware: 12 x RTX 5090
Password hash: bcrypt (10)

Hive Systems

Read more and download at
hivesystems.com/password

FROM GLITCH TO GROWTH

Lessons Learned

Security Measures

- Implemented Multi Factor Authentication (MFA)
- Provided a Password Manager for All Staff
- Strengthened our Password Requirements
- Conducted a Security Risk Analysis

CYBER SIDEKICKS

Security Risk Analysis

CMIT Solutions
Your Technology Team

Assessment Report #910

CPS - SRA General Level (CE and BA) (10 21 21)

Assessment Description:
The HIPAA Security Rule requires that all covered entities and business associates perform a security risk analysis to accurately and thoroughly assess the potential risks and vulnerabilities of all electronic protected health information (ePHI) created, received, maintained, or transmitted. This assessment is intended to meet that criteria.

Site Info

Facility:
St. Louis SW

Department:
(blank)

Location:
Jefferson County Health Department

Asset:
(blank)

Primary Site Contact:

Additional Site Contact:
(blank)

Organization Background:
(blank)

Assessor:

Reviewer:
(blank)

Additional Info

Organization Name:
Jefferson County Health Department

Type of Entity Being Evaluated:
Governmental Agency

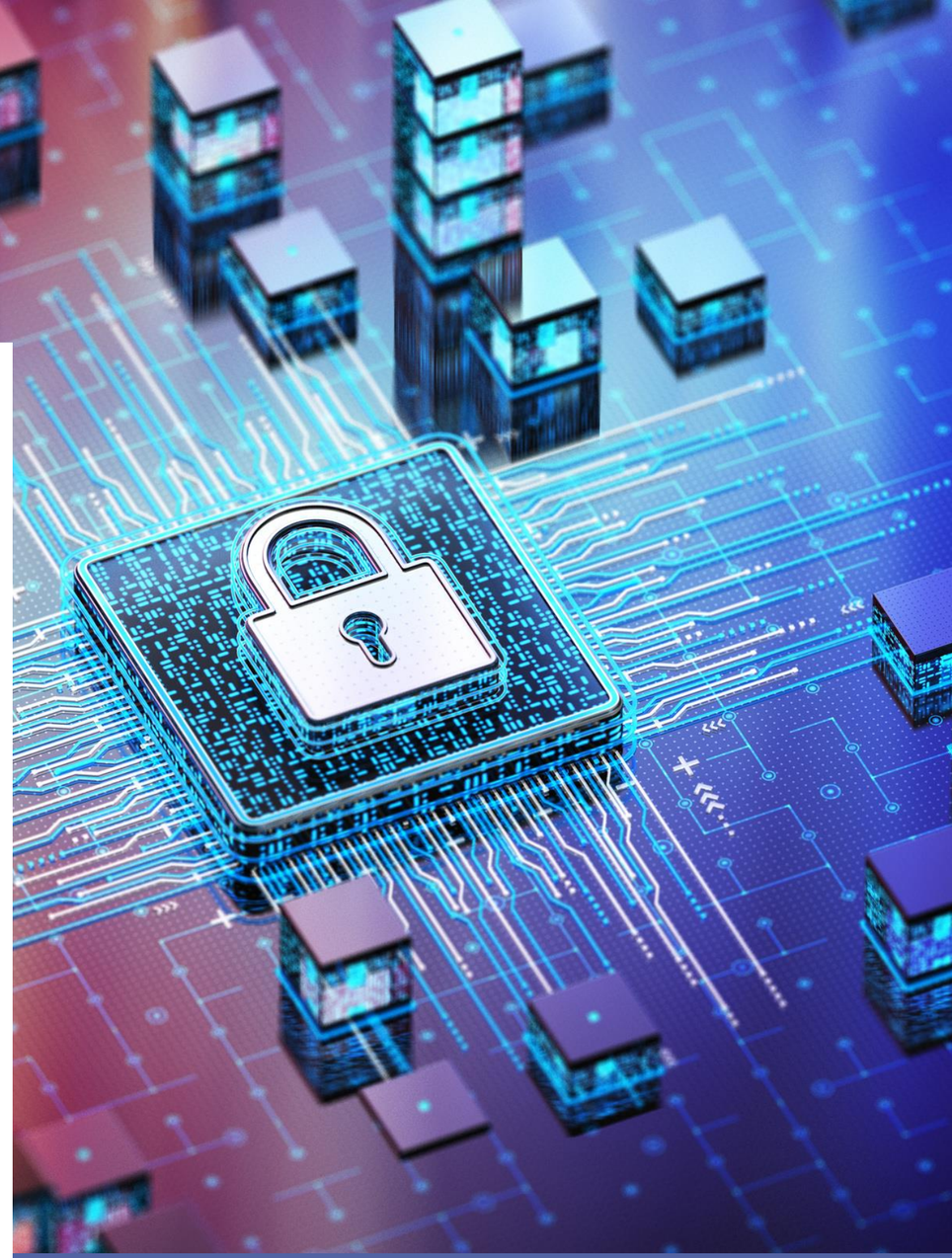
Name of Primary EHR:
CareMD and Curve

Primary EHR Version:
CureMD v. 10G

List of Major Systems Being Assessed:
(blank)

Additional Commentary About the Project:
(blank)

Findings Summary:
(blank)



FROM GLITCH TO GROWTH

Lessons Learned

Security Measures

- Implemented Multi Factor Authentication (MFA)
- Provided a Password Manager for All Staff
- Strengthened our Password Requirements
- Conducted a Security Risk Analysis
- Data Back-ups (New Datto Device)
- New Server

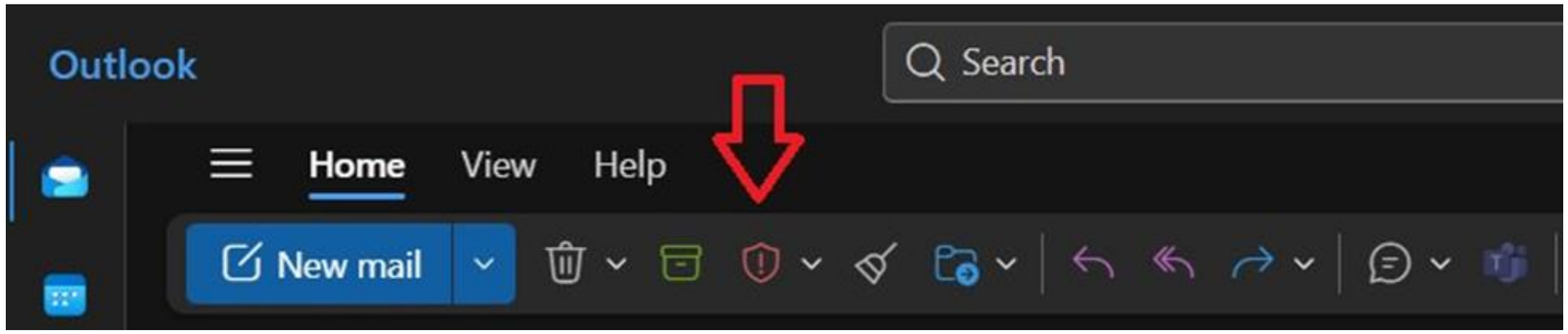
FROM GLITCH TO GROWTH

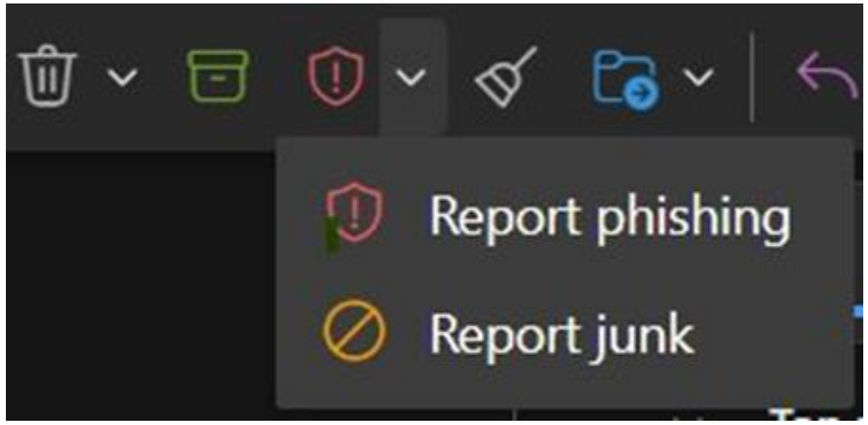
Lessons Learned

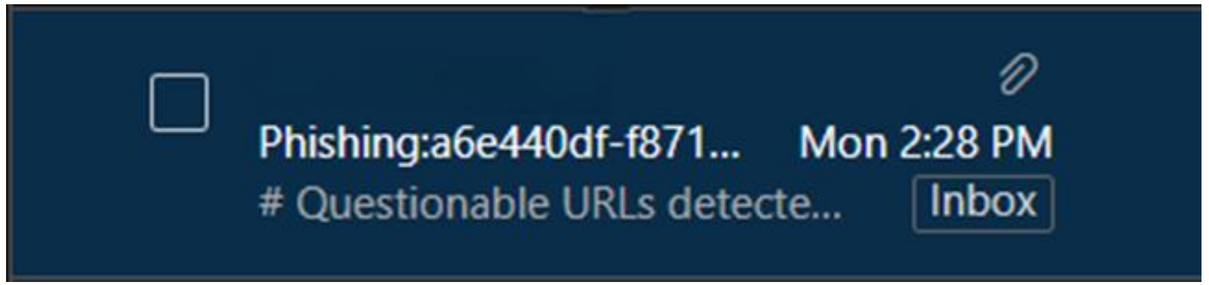
ROUTINE STAFF TRAINING

- Created a process for staff to report Phishing Emails Directly to IT

DON’T TAKE THE BAIT







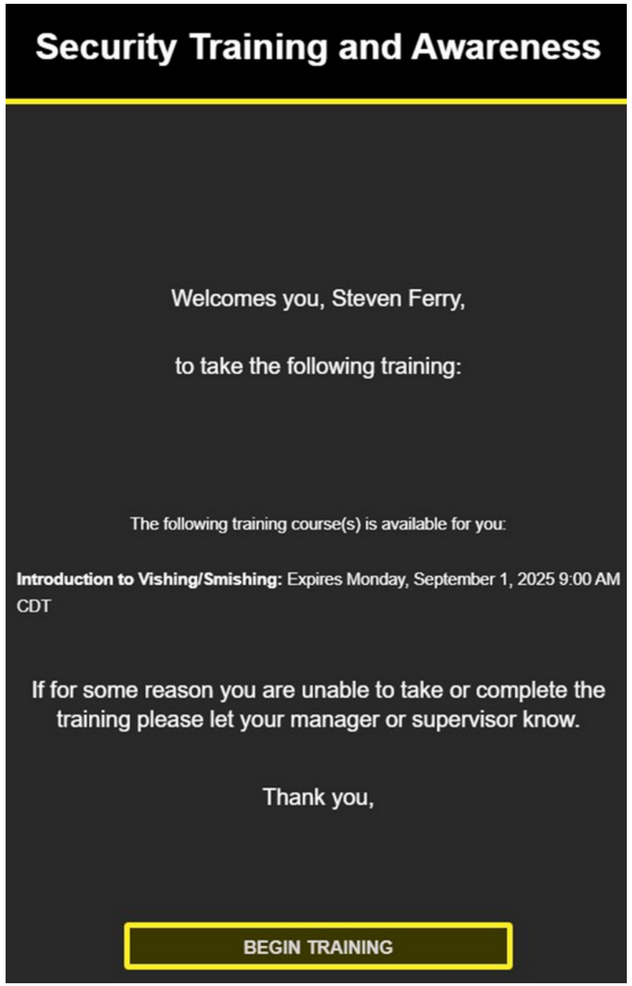
FROM GLITCH TO GROWTH

Lessons Learned

ROUTINE STAFF TRAINING

- Created a process for staff to report Phishing Emails Directly to IT
- Conducted Monthly Cybersecurity Training Campaigns for All Staff

TRAINING DAY: CYBER EDITION



- Monthly training videos for all staff and board to complete
  - Assessment at the end of each training
  - Goal set for compliance and high scores
- Provides education and shows you are proactive in case of a breach

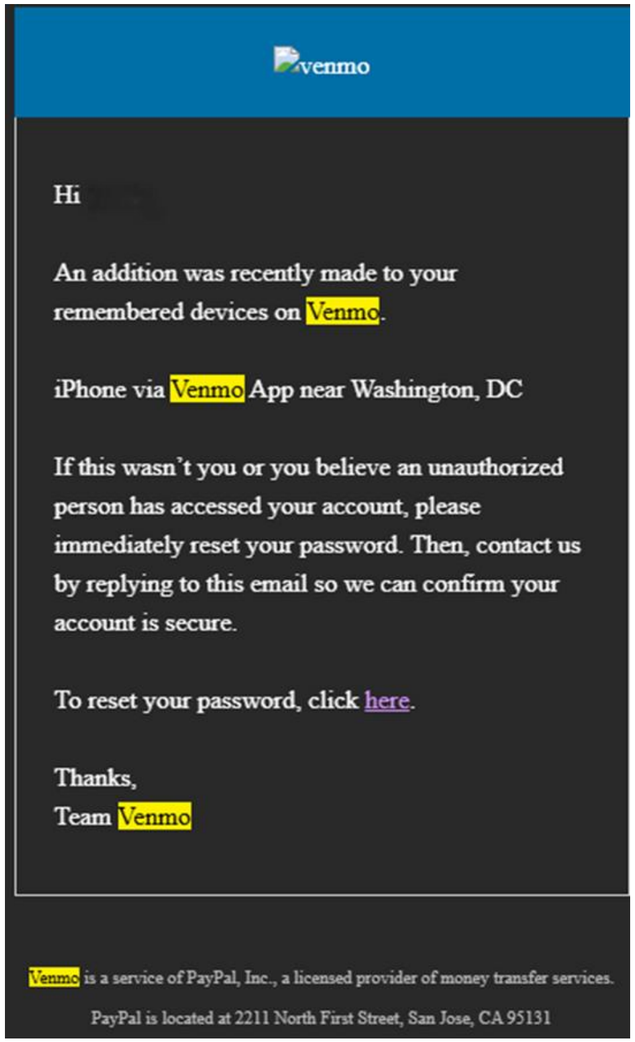
FROM GLITCH TO GROWTH

Lessons Learned

ROUTINE STAFF TRAINING

- Created a process for staff to report Phishing Emails Directly to IT
- Conducted Monthly Cybersecurity Training Campaigns for All Staff
- Organized “Spoof” Phishing e-mails that are sent out to All Staff

REEL TALK: SPOTTING THE PHISH



- Regular phishing emails are sent to staff to test whether they are paying attention and know how to report a phishing attempt
  - Realistic Phish = Real Readiness
- Keeps it top-of-mind and reinforces the concepts learned in monthly training

FROM GLITCH TO GROWTH

Lessons Learned

Additional Resources

- Cybersecurity Grants (SLCGP)
- Partnered with Cybersecurity and Infrastructure Security Agency (CISA)
- Nationwide Cyber Security Review (NCSR)

QUESTIONS

Steve Sikes, Executive Director
steve.sikes@jeffcohealth.org

Steve Ferry, IT Manager
steven.ferry@jeffcohealth.org