



---

---

---

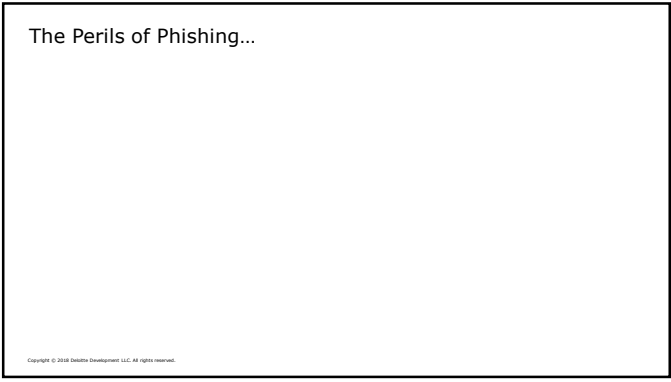
---

---

---

---

---



---

---

---

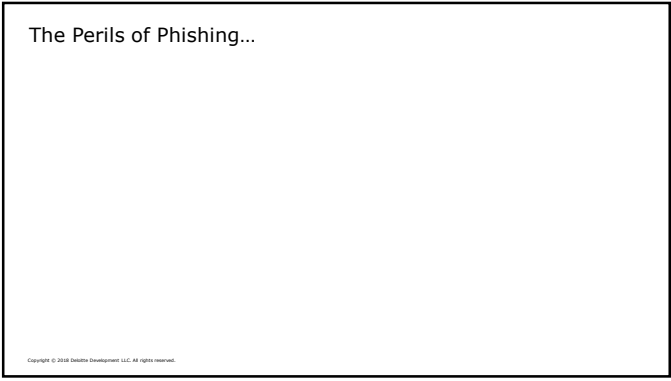
---

---

---

---

---



---

---

---

---

---

---

---

---

## Phishing Risk - Ransomware

You became victim of the [redacted]

The harddisks of your computer have been encrypted with an military grade encryption algorithm. There is no way to restore your data without a special key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy steps:

1. Download the Tor Browser at "<https://www.torproject.org/>". If you need help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:  
[http://\[redacted\].onion/GFCsUs](http://[redacted].onion/GFCsUs)  
[http://\[redacted\].onion/GFCsUs](http://[redacted].onion/GFCsUs)
3. Enter your personal decryption code there:  
3bPCQ7-cU6CaJ-v5GAP8-GvshR5-9yb6ff-9cffff-Nz4czH-qxvsSy-42PyL6-YxTFxz-Yput66-[redacted]-K3JXZU

If you already purchased your key, please enter it below.

Key: [redacted]

Copyright © 2018 Deloitte Development LLC. All rights reserved.



**Glenn Wilson**  
Senior Manager / Cyber for Internal Audit  
Deloitte & Touche LLP

+1 213 688 6976  
glennwilson@deloitte.com  
LinkedIn: <http://www.linkedin.com/in/gmw13>  
Twitter: @DeloitteGlenn

This presentation contains general information only and Deloitte Advisory is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional adviser. Deloitte Advisory shall not be responsible for any loss sustained by any person who relies on this presentation.

As used in this document, "Deloitte Advisory" means Deloitte & Touche LLP, which provides audit and enterprise risk services; Deloitte Financial Advisory Services LLP, which provides forensic, litigation, and other consulting services; and its affiliates, Deloitte Transactional and Business Analytics LLP, which provides a wide range of advisory and consulting services. Deloitte Transactional and Business Analytics LLP is not a limited liability partnership. These entities are separate legal entities of Deloitte LLP. Please see [www.deloitte.com/us/about](http://www.deloitte.com/us/about) for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to all clients under the rules and regulations of public accounting.

Copyright © 2018 Deloitte Development LLC. All rights reserved.  
36 USC 220506

## Middlesex Health System HCCA Phishing Presentation

## Middlesex Health System

Based in Middletown, Conn., the award-winning Middlesex Health System, a member of the Mayo Clinic Care Network, includes Middlesex Hospital, a not-for-profit, 296-bed magnet hospital, and the Middlesex Hospital Cancer Center. It also features three emergency departments, three urgent care centers and an assisted living facility, along with many other programs and services. The health system's primary care physicians, surgeons, specialists, nurses and other employees work hard to meet the needs of the Middlesex County and Connecticut shoreline communities.

The health system's vision is to be the clear, first choice for medical care, and its mission is to provide the safest, highest-quality care and best experience possible.

7

---

---

---

---

---

---

---

---



8

---

---

---

---

---

---

---

---

## Why is Healthcare a Target?

The value of information \$\$\$\$

- Social Security Number, \$1-\$3
- Credit Card Number, \$1-\$3
- Electronic Medical Record, \$50-\$1000
- On average, twice as long to detect.
  - Identity Theft
  - Insurance Fraud
  - Drug Diversion



9

---

---

---

---

---

---

---

---

## What is Phishing?

Phishing is fraudulent communications from an attacker to steal confidential information such as login credentials.



10

---

---

---

---

---

---

---

---

## Phishing Attack at MHS

**MAY 27, 2015**

- An outside Gmail account sent an email to 88 Hospital employees.

Four (4) staff responded to the email and provided their username and password.

1 Nurse

3 Physicians

- Auto-forwarding was configured by the hacker, so any emails they received (including those with PHI) were forwarded. The employees had no idea.

**OCTOBER 9, 2015**

- Information Security Department when evaluating a new detection tool discovers the auto-forwarding and shuts it down.

11

---

---

---

---

---

---

---

---

## The Actual Phishing Email



The email addresses look correct at first glance but when you look closely are slightly wrong

The links go to: "nesba.apicustomhomes.com/mail/midhosp/index.php". This is not an MHS website!!!

Email from the help desk will always include contact information  
Improperly formatted Logo

Confidentiality notice is not the MHS standard notice

12

---

---

---

---

---

---

---

---

## HIPAA Breach

- 945 patient's protected health information were breached.
- Most of the PHI were on reports containing, full patient name, MRN#, diagnosis.

### Notifications sent to:

- All affected patients
- Media
- CT State Attorney General
- Office of Civil Rights
- Board Members



13

---

---

---

---

---

---

---

---

## Breach Notification

- Put notification of breach on hospital website.
- Set up a 1-800# using the call center for patient questions.
- Gave the call center with my name and number to have patient call me directly with questions or concerns.
- Provided credit monitoring to patients for 1 year.
- Notified Employees.
- It takes a village.



14

---

---

---

---

---

---

---

---

## Agencies Involved in Breach

- Centers for Medicare & Medicaid Services (CMS) and DPH
  - On-site visits (2016 Christmas Eve and New Year's Day)
  - Plan of Correction to remain a participant
- CT State Attorney General Office
  - Sent letter requesting information on the breach.
- Office of Civil Rights (OCR)
  - Sent letter requesting information on the breach.

15

---

---

---

---

---

---

---

---

### Mitigation Strategies

- Attended Department Meeting Presentations
- Mandated Social Engineering Testing for all employees through Healthstream to get 100% compliance.
- Created March as CyberSecurity Awareness Month.
- Articles in Hospital Newsletter.
- Quality & Audit Committee Reporting.
- Report Cleansing.



16

---

---

---

---

---

---

---

---

### OCR Final Response 11/2017

- Following discovery of the breach, Middlesex contacted all 945 affected individuals to notify them of the breach and opened a call center for these individuals to answer their questions.
- The Hospital privacy officer offered support to any individuals who called with questions as well.
- The Hospital also provided all affected individuals with twelve months of credit monitoring services and provided notice of the breach on its website and through a press release.

17

---

---

---

---

---

---

---

---

### OCR Final Response

- Further, as a result of this breach, the Hospital implemented a required approval process in order for employees to auto-forward emails, so as to prevent the auto-forwarding of emails.
- The Hospital also developed a mandatory Phishing Awareness and Response Training program for employees; all supervisors and managers were also provided additional training that they were required to provide to their staff.
- Additional mitigation included the designation of March as "Cyber Awareness" month, which includes the implementation of a number of tools to educate staff on cyber threats, separate personal meetings and trainings between those employees whose accounts had been compromised, and the procurement of a vendor to conduct social engineering testing to assess the effectiveness of the Hospital's staff training.

18

---

---

---

---

---

---

---

---

### OCR Final Response

- In addition, the Hospital provided OCR with a copy of its policies and procedures related to impermissible uses and disclosures, safeguards, information system activity review, response and reporting, security awareness and training, access control, audit controls and breach notification.
- These policies and procedures appear to be in compliance with the Privacy and Security Rules. The Hospital further provided evidence of staff HIPAA training.
- All matters raised by this complaint at the time it was filed have now been resolved through the voluntary compliance actions of Middlesex Hospital. Therefore, OCR is closing this case!!!!



19

---

---

---

---

---

---

---

### Lessons Learned

- Notify your Board as soon as you learn there will be a significant number of reportable breaches.
- Have Cyber Insurance and read the Policy.
- Review your reports to ensure they have the minimal amount of PHI in them and use patient initials whenever possible.
- Conduct monthly Phishing tests and continue to provide education.
- Confirm receipt of all responses sent to OCR.

20

---

---

---

---

---

---

---

### Preparation for a Breach

- ✓ Checklist
- ☐ Patient Notification/Credit Monitoring Service Agreement in place.
- ☐ Sample letters to the media, Board, and patients.
- ☐ Know your insurance policy and obligations.
- ☐ Need to tell the story of how the breach occurred, response, and mitigation efforts to investigators.
- ☐ Log dates/times and be able to provide report to investigators.
- ☐ Attorney on standby.
- ☐ Work with Business Associate to obtain needed information promptly.
- ☐ Begin education right away across the organization.
- ☐ Quality and Audit Governance of Information Security Program.
- ☐ Current comprehensive Risk Assessment available in accordance with HIPAA.

21

---

---

---

---

---

---

---

### MHS Sample Education

#### If You Have Opened a Suspicious Email:

**CALL** the IT Support Center **IMMEDIATELY** to report it!

Failing to report or ignoring a suspicious email, link, or attachment that you opened can have serious consequences for you, our patients, and the Health System.

The Office of Civil Rights mandates a sanctions policy that we are required to follow - not reporting could lead to disciplinary action up to and including termination.

22

---

---

---

---

---

---

---

---

### MHS Sample Education

#### If You Receive A Suspicious Email Message:

- **DO NOT:** Reply to the message
- **DO NOT:** Click hyperlinks in the message
- **DO NOT:** Download any attachments in the message
- **DO NOT:** Try to determine if the message is legitimate on your own
- **DO NOT:** Ignore the message or wait to report it

**DO:** Alert the IT Support Center **IMMEDIATELY** to report it!

23

---

---

---

---

---

---

---

---



**LINDA JO SPENCER, Chief Compliance Officer,**  
**Middlesex Health System, 860-358-6602**  
**[LindaJo.Spencer@midhosp.org](mailto:LindaJo.Spencer@midhosp.org)**

24

---

---

---

---

---

---

---

---



Elliot Health System



# Gone Phishing

Andy Seward, CISO

Elliot Health System

Confidential & Proprietary | ©2016 Elliot Hospital All Rights Reserved.

---

---

---

---

---

---

---

---

Elliot Health System

## Phishing, Cyber & Compliance

- What are phishing attackers looking for?
- How can we prevent their success?
- Educating, preparing & defending.

---

---

---

---

---

---

---

---

Elliot Health System

## What are phishing attackers looking for?

Access



User Credentials



Launch Points for More Attacks



---

---

---

---

---

---


---

---


Elliot Health System

### What do phishing attackers want?

Money



Revenge



Confidential & Proprietary | ©2018 Elliot Hospital All Rights Reserved.

---

---

---

---

---

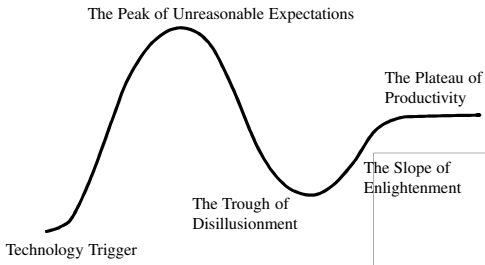
---

---

---

Elliot Health System

### The Standard Hype Cycle



The Peak of Unreasonable Expectations

Technology Trigger

The Trough of Disillusionment

The Slope of Enlightenment

The Plateau of Productivity

Confidential & Proprietary | ©2018 Elliot Hospital All Rights Reserved.

---

---

---

---

---

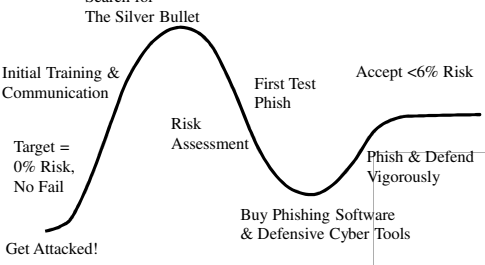
---

---

---

Elliot Health System

### Phishing Hype Cycle



Search for The Silver Bullet

Initial Training & Communication

Risk Assessment

First Test Phish

Phish & Defend Vigorously

Accept <6% Risk

Buy Phishing Software & Defensive Cyber Tools

Target = 0% Risk, No Fail

Get Attacked!

Confidential & Proprietary | ©2018 Elliot Hospital All Rights Reserved.

---

---

---

---

---

---

---

---

Elliot Health System

How can you prevent their success?

1



Defend & Shield

2



Improve Behaviors

Confidential & Proprietary | ©2018 Elliot Hospital. All Rights Reserved.

---

---

---

---

---

---


---

---

Elliot Health System

How can you prevent their success?

1



Defend & Shield

- Build a cyber-security technical and compliance-based defensive core capability that protects employees & technologies and reduced risk.
- Hire & employ a skilled team to deliver this strategy.
- Implement cyber tools to improve ability to detect and prevent malicious/suspicious phishing threats.
- Mature & streamline incident management process to quickly contain and recover from issues.

Confidential & Proprietary | ©2018 Elliot Hospital. All Rights Reserved.

---

---

---

---

---

---


---

---

Elliot Health System

Practical Steps for Defend & Shield

1



At your network perimeter:

- Firewalls: enable features that block phishes from entering your network environment (e.g. Wildfire, Sourcefire, Sandblast, Fortinet)
- Specialized email security: consider pre-screening software and URL (links) filtering (e.g. Proofpoint, Mimecast, etc.)
- O365: turn on advanced threat detection

On your network endpoint computers:

- Anti-virus software serves as your final defense (Cylance, Carbon Black, Symantec SEP v14, etc.)

Confidential & Proprietary | ©2018 Elliot Hospital. All Rights Reserved.

---

---

---

---

---

---


---

---

Elliot Health System

## How can you prevent their success?

2



### Improve Behaviors

- Conduct workforce training & incentivize awareness to raise awareness of phishing risks and empower better decisions.
- Standardize phishing security risk assessments, metrics & reporting to track the progress and maturity of your phishing awareness program.
- Update and communicate compliance, HR, and/or cyber security policies and procedures to set expectations for employee behaviors regarding phishing.

Confidential & Proprietary | ©2018 Elliot Hospital All Rights Reserved.

---

---

---

---

---

---


---

---

Elliot Health System

## Practical Steps for Improve Behaviors

2



### Gain leadership's consensus to address phishing risk

- Business case: cost of program vs. risk reduction
- "If peer organizations are phishing their employees, shouldn't we too?"

### Benchmark your vulnerability:

- Phish your employees and measure the results
- Report results to leadership & build confidence

### Develop program & train/test employees regularly:

- Monthly phishes
- Communicate & publicize successes
- Vary the difficulty level
- Phish the most likely targets (CEO, CFO, COO, VPs)

Confidential & Proprietary | ©2018 Elliot Hospital All Rights Reserved.

---

---

---

---

---


---

---


---

Elliot Health System

## Preparing Your Organization



Three Strikes, YOU'RE OUT!



### Build Incentives -- positive & negative -- with HR

Confidential & Proprietary | ©2018 Elliot Hospital All Rights Reserved.

---

---

---

---

---

---

---

---

12

Elliot Health System

Educate Your Organization

New Hire Orientation



New Hire Phishing Online Training



Confidential & Proprietary | ©2018 Elliot Hospital All Rights Reserved

---

---

---

---

---

---

---

---

Elliot Health System

Educate Your Organization

Deliver “when I want it” training & info

CHOOSE YOUR CYBER ADVENTURE...

FRESH AND NEW



TELL ME MORE



Confidential & Proprietary | ©2018 Elliot Hospital All Rights Reserved

---

---

---

---

---

---

---

---

Elliot Health System

Educate Your Organization

Cyber Security Training

Cyber Newsletter - May 2018

Cyber Security Job Aids

Cyber Security Games

Confidential & Proprietary | ©2018 Elliot Hospital All Rights Reserved

---

---

---

---

---

---

---

---

Elliot Health System

### Educate Your Organization

#### PHISHING IN ACTION

An information security professional shared this example of a real phishing email that came through her inbox. It made her pause because it looked so legitimate. Read through her notes about the thought process she used to figure out if it was real or not.

Inconsistencies in the link: "Service@paypal.com" was just the display name. "Service@pp.com" was the actual email URL.

They used my actual name, not something generic like "customer" so I had to really think about this.

PayPal

Account Status Update

Reference: APT-276-271-383

Response required

Example "Tips & Tricks" on internal website

---

---

---

---

---

---

---

---

Elliot Health System

### Tools give quick feedback

Oops! You clicked on a phishing email.

Remember these three 'Rules To Stay Safe Online'

✓ RULE NUMBER ONE:

- Stop, Look, Think
- Use that delete key.

✓ RULE NUMBER TWO:

- Do I spot a Red Flag?
- Verify suspicious email with the sender via a different medium.

✓ RULE NUMBER THREE:

- "When in doubt, throw it out". There are a thousand ways that internet criminals will try to scam you, and only one way to stay safe. Stay alert as YOU are the last line of defense!

---

---

---

---

---

---

---

---

Elliot Health System

### Real Life: It Takes Time

---

---

---

---

---

---

---

---

Elliot Health System

Thank you!



Compliance + Cyber = Teammates

Elliot Health System

Confidential & Proprietary | 2021 EHSI Hospital All Rights Reserved

---

---

---

---

---

---

---

Elliot Health System

Questions and Comments

Elliot Health System

Confidential & Proprietary | 2021 EHSI Hospital All Rights Reserved

---

---

---

---

---

---

---