Phishing and Ransomware

Healthcare is a prime target

Richard Free, CISSP, CISM

tw-Security

Lafayette, CO

tw Security
Healthcare Information Security

The Reality of Today's Cyber World

One person clicking on one link within an email or while visiting a website can lead to ransomware, resulting in a shutdown of the organization's infrastructure and the hijacking of their data

Healthcare workers are a prime target!

Information security is everyone's responsibility!

Hacking and Healthcare Breaches

Year Hacking Events Reported to HHS	Number of Hacking Events Reported	Number of Patients Affected in Hacking Events for the Year
2010	8	92,358
2011	17	297,775
2012	16	900,684
2013	24	238,207
2014	34	1,796,755
2015	57	111,812,172
2016	107	13,345,573

Source: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Why the surge in Healthcare?

- **Medical records are far more valuable on the black market than credit cards**
- **Medical records contain immutable data (unchangeable data) that can be used for years for identity theft and other cybercrimes**
  - Examples: Social Security number and date of birth
- **Credit card data changes more frequently**
  - Examples: Expiration date and security code

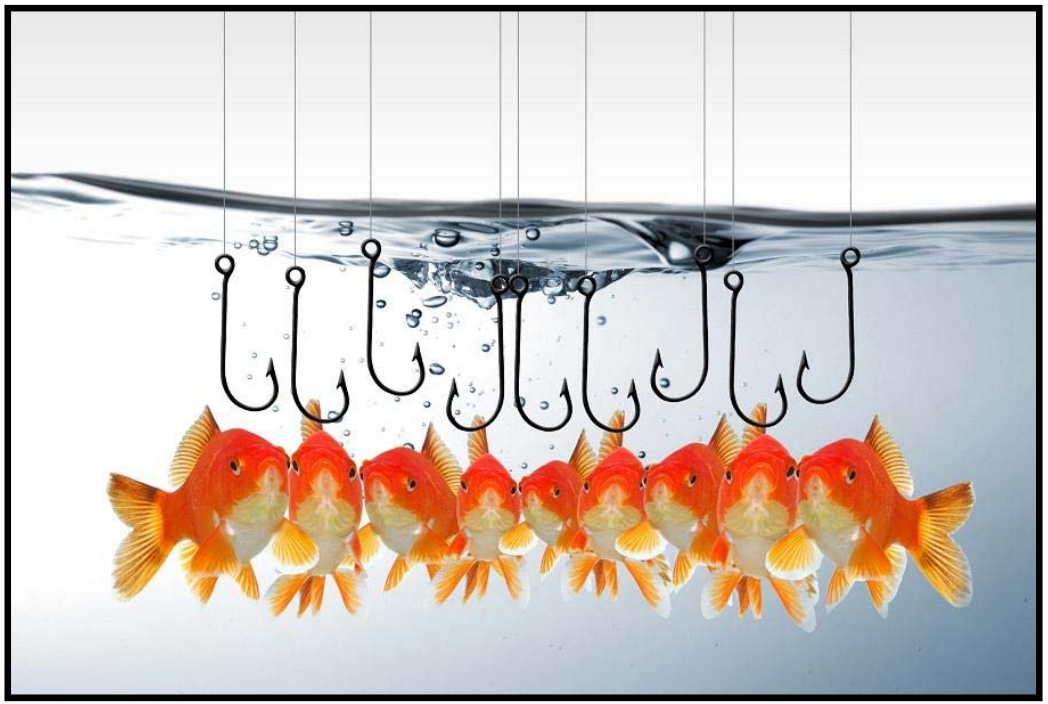
Session Objectives

- **Explain phishing and ransomware**
  - What it is and how it happens
  - Summarize the potential impacts of ransomware
- **Describe how to respond effectively**
- **Identify key defenses for preventing attacks**
  - Technical
  - Non-technical (Procedural)
- **Identify resources for staying informed**

Introduction – Richard Free

- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- Former - Director, Information Technology for a Federally Qualified Health Center (FQHC) with eight locations, 65 providers, 450 employees
- Chair of the Colorado statewide IT Directors group for community health center members through Colorado Community Health Network

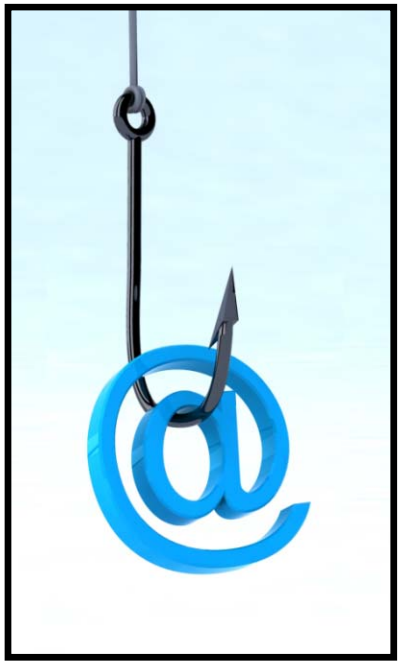
Phishing



Phishing – What is it?

Phishing **emails are designed to trick the recipient into believing that the sender of the message is legitimate or trustworthy in order to acquire sensitive information such as:**

- User IDs and passwords
- Patient data
- Personal information such as…
  - Social Security numbers
  - Credit card information



Phishing – How does it work?

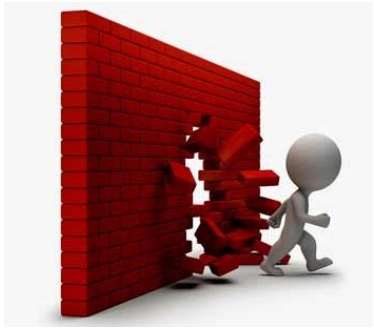
Phishing emails may prompt the recipient to:

- **Click a link** to a website that looks genuine and enter information that is collected by criminals and used without permission
- **Visit a website** that prompts the user to download a fix for a computer problem
- **Open an attachment** containing malware designed to steal information, prevent access to files until a ransom is paid, or provide unauthorized remote access (hacker) into a computer

Phishing – Why does it work?

- **Phishing is a popular way to steal sensitive information (or compromise a computer network) because it doesn't take as much talent or time as traditional hacking and it is very effective**

vs



- **When you want physical access to a building, it's always easier to ask someone or trick someone, than to use brute force**

Some Clues of Phishing

- **Suspicious email or text**
  - The sender's name or organization is unfamiliar
  - Generic greeting ("Dear Sir or Madam") instead of by name
- **Poor spelling and grammar**
- **URLs containing one character that is different from a real domain name**

  URL = Uniform Resource Locator, used to specify addresses on the World Wide Web/Internet
- **Request for personal or sensitive information**
- **Offers that seem too good to be true**
  - Recipient is asked to send money

Some Clues of Phishing

- **Something seems out of place**
  - Message appears to be coming from a co-worker but worded in a way that does not sound like something they would say or request
- **Appears to be from an official government agency**
  - When being audited, the IRS will not send an email
- **The action was not initiated by the user**
  - Notification of an attempted package delivery
  - Online purchase was not made
- **Unrealistic threats**

Ransomware

Ransomware – What is it?

- ***Ransomware*** **is a specific type of computer virus written by criminals for financial gain**
- **When it infects a computer, ransomware encrypts files on the internal hard drive**
  - Encryption is a way to secure files by scrambling information using a mathematical computation
  - Without the key to reverse the scrambling process (called decryption), encryption makes the information inaccessible
- **The ransomware creators possess the means to decrypt the files – returning the information back to its original format**
- **They expect payment in exchange for the decryption key**

Once Affected by Ransomware…

- **Encryption begins…**
  - The malicious code will begin encrypting many of the files stored (directory or drive) where the user has the ability to write data starting with the C: drive and then encrypting the directories on the network fileserver
- **A screen will appear with instructions**
  - *See next slide*

SAMPLE – Ransomware Screen

Ransomware – Targeted Files

- Data files such as Word documents, spreadsheets, and PDFs are common targets
- However, some ransomware may encrypt any file it comes across
- Consequently, program files and Windows files may become encrypted, preventing computer programs or the Windows operating system from functioning

What to do?

If you get a ransomware message:

- Unplug the network cable or turn off wireless network access but leave the computer powered on
- Unplug any external hard drives or USB drives
- Call IT support staff immediately
  - Make sure they preserve the audit logs
- Report what happened to the Information Security, Privacy, and/or Compliance Officer
- Think about recent activities that may have triggered the ransomware – useful for containment

Ransomware Impact

Choices are:

1. Recover from backup
2. Pay the ransom
3. Lose some data

… It is difficult to truly assess the full impact

For many of the healthcare organizations infected with ransomware, there was a disruption of patient services!

Ransomware Impact

The ransomware was able to spread from one computer to another computer because of unpatched or older operating systems.

Ransomware – Challenges

- **Hard to stop – evolving new variants**
  - Example: WannaCry ransomware – attackers exploited unpatched server vulnerabilities – info was obtained from leaked NSA toolkit
  - A change in focus from targeting individual end users to infecting entire networks
- **Ransomware now is the most predominant malware because it is the most profitable type of malware in history**
  - Not a single conviction to date because the ransom is paid in bitcoin which is untraceable

Tips to Prevent Ransomware

(Nontechnical)

- **Educate the workforce** - People are the root cause for ransomware, so start there; remind your staff to:
  - Stay vigilant and report anything suspicious to their managers
  - Report if they accidentally clicked on a link, opened an attachment, went to a website; do not hide it because they feel embarrassed
- **Ban all personal webmail and surfing on organizational devices -** Require the workforce to use their own personal mobile devices through the 'guest' wireless network
- **Review access rights on network drives** - "Least privilege"
- **Create incident response procedures** - It's no longer a matter of "If" but "When" a cyber-attack may happen
- **Improve data backup intervals and procedures**

Tips to Prevent Ransomware

(Technical)

- **Implement geo-fencing** - Block inbound and outbound traffic to foreign countries
- **Implement blacklisting /whitelisting**
- **Block email from domains that are less than 72 hours old**
- **Quarantine or strip away risky attachments** –
  - *.exe, *.scr,*.zip, *.cab *.rar, and *.pdf
- **Disable macro scripts from MS Office** - Use Active Directory (AD) Group Policy Object (GPO)
- **Stay current with patch management**
- **Deploy advanced endpoint protection** - Traditional antivirus may not be enough
- **Deploy a next-generation firewall**

What to do?

- **Proactively phish your workforce**
  - Establish your baseline click rate (and after-awareness effectiveness metric)
- **Train at time of "fail"**
  - Required training for "clickers"
  - Instruct "clickers" what they should have looked for
  - More intense training is provided if they clicked on an attachment or an embedded link
  - Consider the impact of your CEO delivering the message…

Ransomware:
Breach or no Breach of PHI?

Breach or No Breach?

"It depends…"

- Was protected health information (PHI) involved?
- If ransomware was able to encrypt your data, could it have read and copied your data as well?
- Only after a risk analysis has been performed can it be determined if a data breach occurred
- Forensic data is needed to prove that no data from the infected device(s) left the organization

Do not let IT solve the problem or ransomware alone. Require the Privacy Officer and/or Compliance Officer to get involved.

Challenges with IT Staff

- **IT staff like to "fix things" and get things back to normal as quickly as possible**
- **Unfortunately, IT staff may delete valuable forensic evidence needed to make a determination if a breach of PHI has occurred**

Terminology

- **Information Security Incident – An adverse event whereby some aspect of computer security could be threatened: loss of data confidentiality, disruption of data or system integrity, or disruption or denial of availability.**

  Source: NIST Special Pub 800-3

  Establishing a Computer Security Incident Response Capability

- **Breach – An "unauthorized acquisition, access, use or disclosure of PHI which compromises the security or privacy of the PHI, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information."**

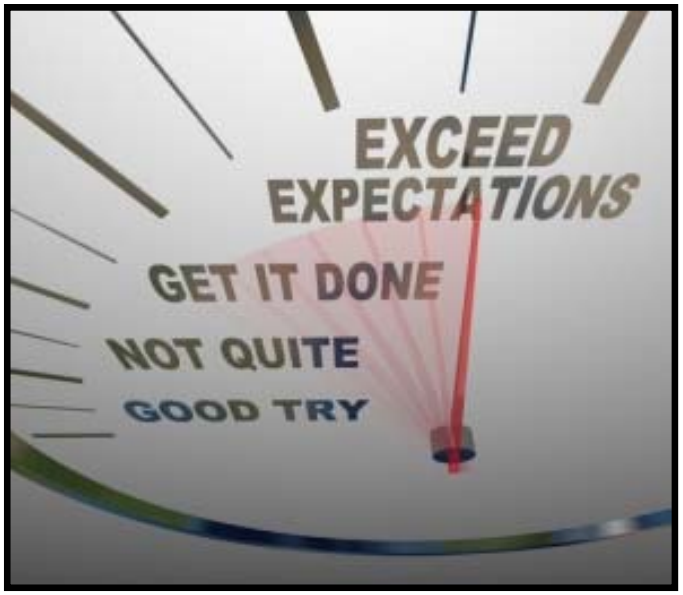
  Source: *The Health Information Technology for Economic and Clinical Health (HITECH) Act*

OCR Guidance on Ransomware

- Conducting a **risk analysis** to identify threats and vulnerabilities to electronic protected health information (ePHI) and **establishing a plan to mitigate** or remediate those identified risks;
- Implementing procedures to **safeguard against malicious software**;
- **Training** authorized users on detecting malicious software and report such detections;
- **Limiting access to ePHI** to only those persons or software programs requiring access; and
- Maintaining an overall **contingency plan** that includes **disaster recovery**, emergency operations, **frequent data backups**, and **test restorations**.

Incident Response

Tabletop exercises are important because incident response is a skill developed over time



Incident Response Phases

1. Detection

2. Analysis

3. Containment

4. Eradication

5. Recovery

6. Post Incident Activities

Reference: The National Institute of Standards and Technology (NIST) Special Publication SP 800-61 Computer Security Incident Handling Guide

Closing Thoughts and Summary

Guidance

- **Exercise discernment**
- **Change behaviors**
  - Prohibit the personal use of company workstations
- **Implement stronger technical controls**
  - Keep operating systems patched and updated
- **Get prepared for a breach**
  - It's no longer a matter of "If it happens…"
  - Making sure you understand the legal obligations under HIPAA

Resources

- **HHS**
  - https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf
- **Health Data Management**
  - https://www.healthdatamanagement.com
- **Healthcare IT News**
  - http://www.healthcareitnews.com
- **HealthcareInfoSecurity**
  - http://www.healthcareinfosecurity.com

Real Life Examples

- **It is not Halloween quite yet, but there are some horror stories out there**

Summary

During this session, we…

- Explained what phishing and ransomware is
- Described the impact and challenges
- Provided some ideas for preventive measures
- Identified the steps needed to determine if ransomware resulted in a breach of PHI
- Summarized the six steps of incident response

Questions?

Richard Free, CISSP, CISM

tw-Security

Lafayette, CO

www.tw-Security.com

Richard.Free@tw-Security.com

720-251-3825

tw-Security, a nationally recognized healthcare IT security consulting firm is dedicated to helping healthcare organizations protect their information resources with hands-on experience in creating and managing information security programs.