Healthcare Cybersecurity Developments: What You Need to Know

Lee Kim, JD, CISSP, CIPP/US, FHIMSS

Director, Privacy and Security/
Thought Advisory

HIMSS

Cybersecurity: In the Crosshairs

- **Although we are now in unusual times given the COVID-19 pandemic, the cybersecurity threat landscape is still alive and well.**
- **Cybersecurity is important because it is directly linked to patient safety.**
- **Primary avenues of attack include phishing, credential stealing, and ransomware.**
- **Any technology may be susceptible to compromise: hardware, software, and devices.**

Cybersecurity: Big Picture

- **Objective: Protect confidentiality, integrity, and availability of information.**
  - Robust cybersecurity is necessary for patient safety.
  - HIPAA compliance is only a minimum.
  - Robust cybersecurity is a must.
  - Robust cybersecurity requires the following:
    - End-to-end risk assessment and management of the risks
    - Multiple security controls (defense in depth) to protect confidentiality, integrity, and availability of information
      - If one security control fails, another control will take over
    - Rigorous cybersecurity awareness training for all personnel
    - Robust detection and incident response capabilities
      - See something, say something: an incident will be triaged, contained, and eradicated quicker
    - Robust disaster recovery and business continuity capabilities

Healthcare Cybersecurity: Legislation & Regulation

- **State and Federal Laws**
  - Cybersecurity Act of 2015 – 6 USC 1533 – Improving Cybersecurity in the Health Care Industry Section 5 of FTC Act – 15 USC 45 (not healthcare-specific)
  - Other state laws may apply (medical privacy, breach notification, data disposal, etc.)
- **Regulations**
  - HIPAA Security Rule, HIPAA Privacy Rule, HIPAA Breach Notification Rule
  - 42 CFR Part 2 (disclosure of substance abuse disorder patient records)
  - Office for Civil Rights (OCR) at the US Department of Health and Human Services (HHS) interprets and enforces HIPAA
- **Healthcare and public health sector is part of the national critical infrastructure**

Patient Safety and Cybersecurity

- **The confidentiality, integrity, and availability of information must be protected at all times. Incorrect or inaccurate information may potentially lead to patient harm.**
- **Cybersecurity risks include information being tampered with (intentionally or unintentionally), unavailability of telehealth platforms/servers/applications, loss of network connectivity, loss of power, software malfunctions, unreliable or slow Internet connectivity, etc.**
- **Patient safety may be at risk due to any of these reasons. Risks to the patient include cancellation of elective surgeries, disruption of emergency services, disruption of non-emergency clinical care, transfer of patients to another facility (due to systems being down or unavailable, for example), etc.**

Top Threats

- Phishing
- Social engineering
- Ransomware or other malware
- Credential harvesting attacks
- Theft or loss
- Website and web application attacks (e.g., cross-site scripting, SQL injection, etc.)
- Malicious insider attacks; negligent insider attacks

Top Threat Actors

- **Online scam artists**
- **Cybercriminals**
- **Social engineers**
- **Malicious insiders**
- **Negligent insiders**
- **Hacktivists**
- **Nation state actors and non-state actors**

What are Threat Actors After?

- **Financial information**
- **Employee information**
- **Patient Information**
- **Intellectual property**
- **Competitive or proprietary information**

Top Threat: Phishing

- **Phishing is the #1 cause of significant security incidents.**
- **Phishing is also the #1 initial point of compromise for significant security incidents.**
- **E-mail phishing is the primary vehicle.**
- **Phishing may involve elicitation of sensitive information (e.g., health or financial information, credentials, and/or intellectual property) and/or malicious links/attachments (i.e., malware).**
- **Phishing attacks and other social engineering attacks have increased significantly since the inception of the COVID-19 pandemic.**

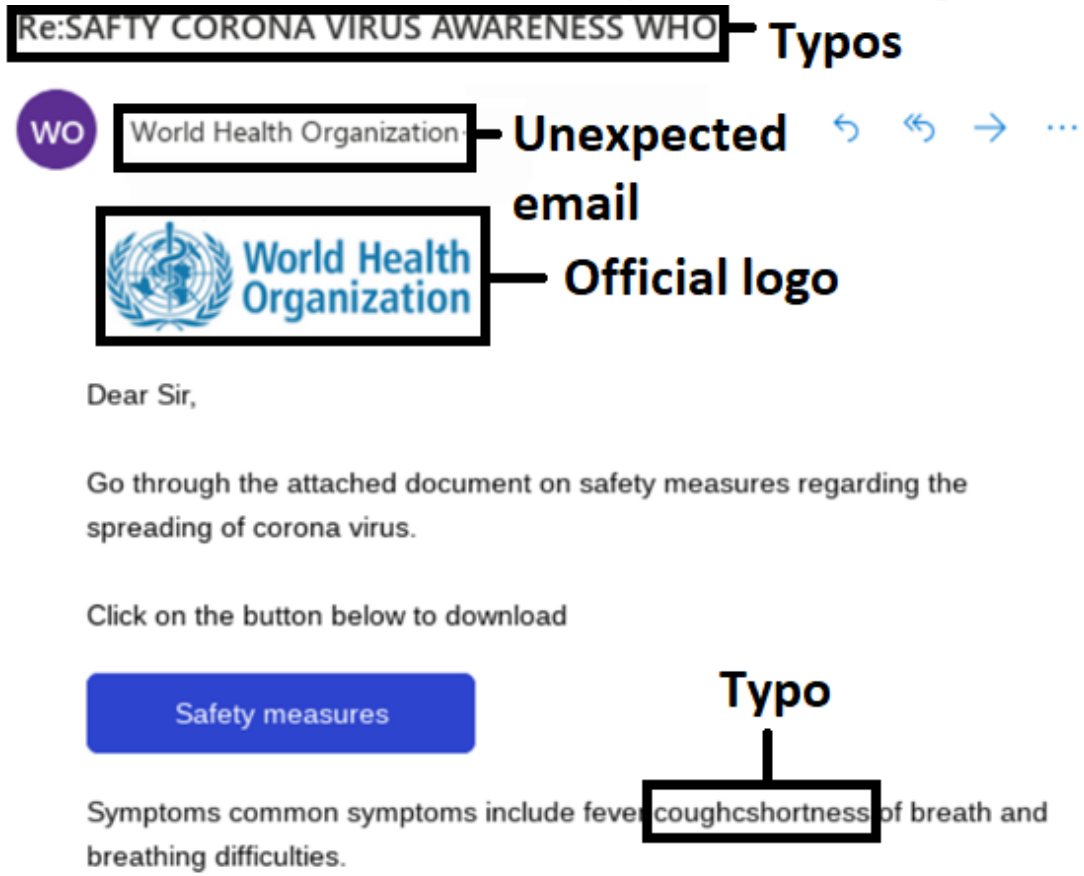
Top Threat: Phishing

- **General phishing e-mails and spear-phishing (i.e., targeted) e-mails are the primary modes of phishing**
- **Social media phishing also occurs**
  - Note: Shortened links via social media may be especially dangerous since you won't know where the link actually leads to (unless you use a URL lengthening service).

General Phishing Example

HIMSS

General Phishing Example



General Phishing Example

Tue 3/7/2017 9:20 AM

USPS <usps@uspsdelivery.com>

Shipment status change notification for parcel #61621750

To Sheri

Unexpected email

Your package could not be delivered by our courrier because no person was present at your address.
Your signature is required to successfully deliver the parcel.

Shipping service: Next Day Air
Box size: Large
Date : Mar 7th 2017

A new delivery can be scheduled, by calling the number on the delivery notice we left at your address. You need to confirm the shipping information, including the address and tracking number, wich can be found on the notice.

Typo

An electronic copy of the delivery notice can be viewed online on the USPS website:

https://tools.usps.com/web/pages/view.invoi ce?id=61621750&dest=s @ com

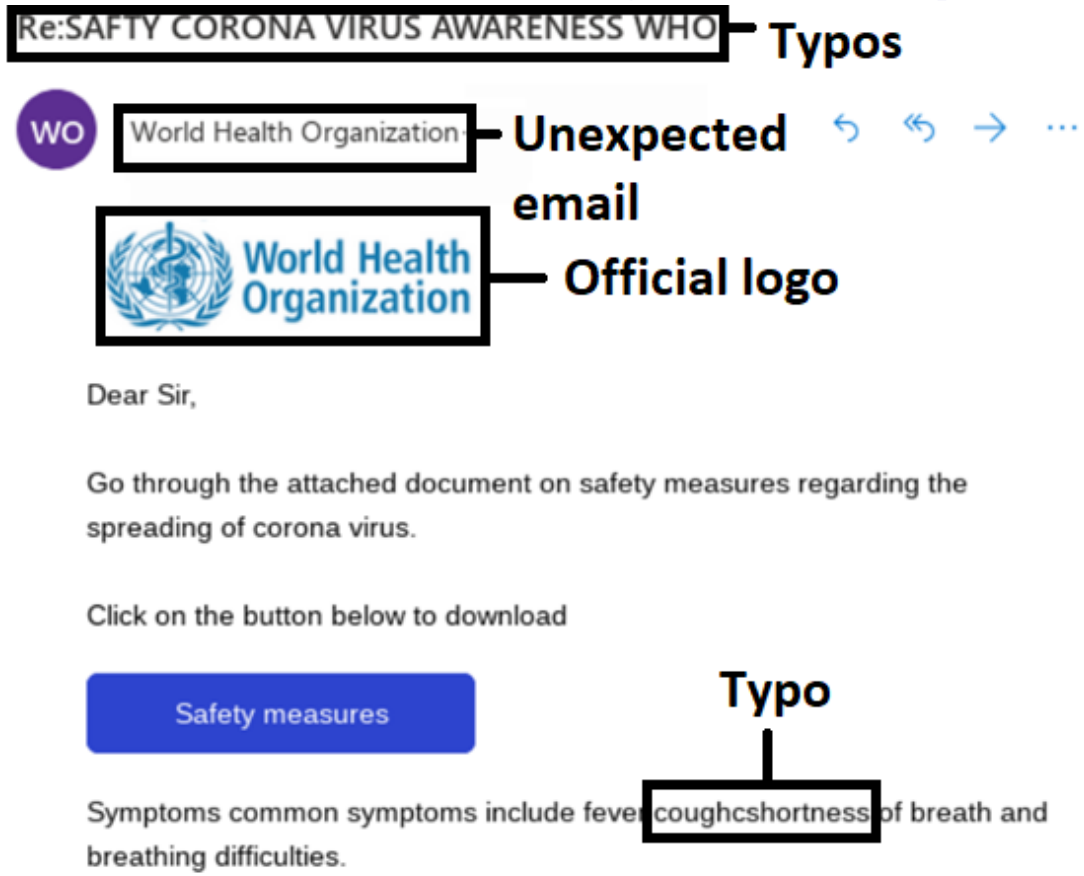
Actual URL is malicious

The shipment will be cancelled and the package returned to the sender if a new delivery is not scheduled within 24 hours.

Urgency

Thanks for shipping with USPS

General Phishing Example



Spear-Phishing Example

From Betty W Doyle <[redacted]@[redacted].com> — Name mismatch; unexpected
Date: September 11, 2017 at 11:13:06 AM EDT
To:
Subject: 1757064939:90

This email has been automatically generated and sent to you because BBB has got a complaint, claiming that your company is violating the Fair Labor Standards Act.

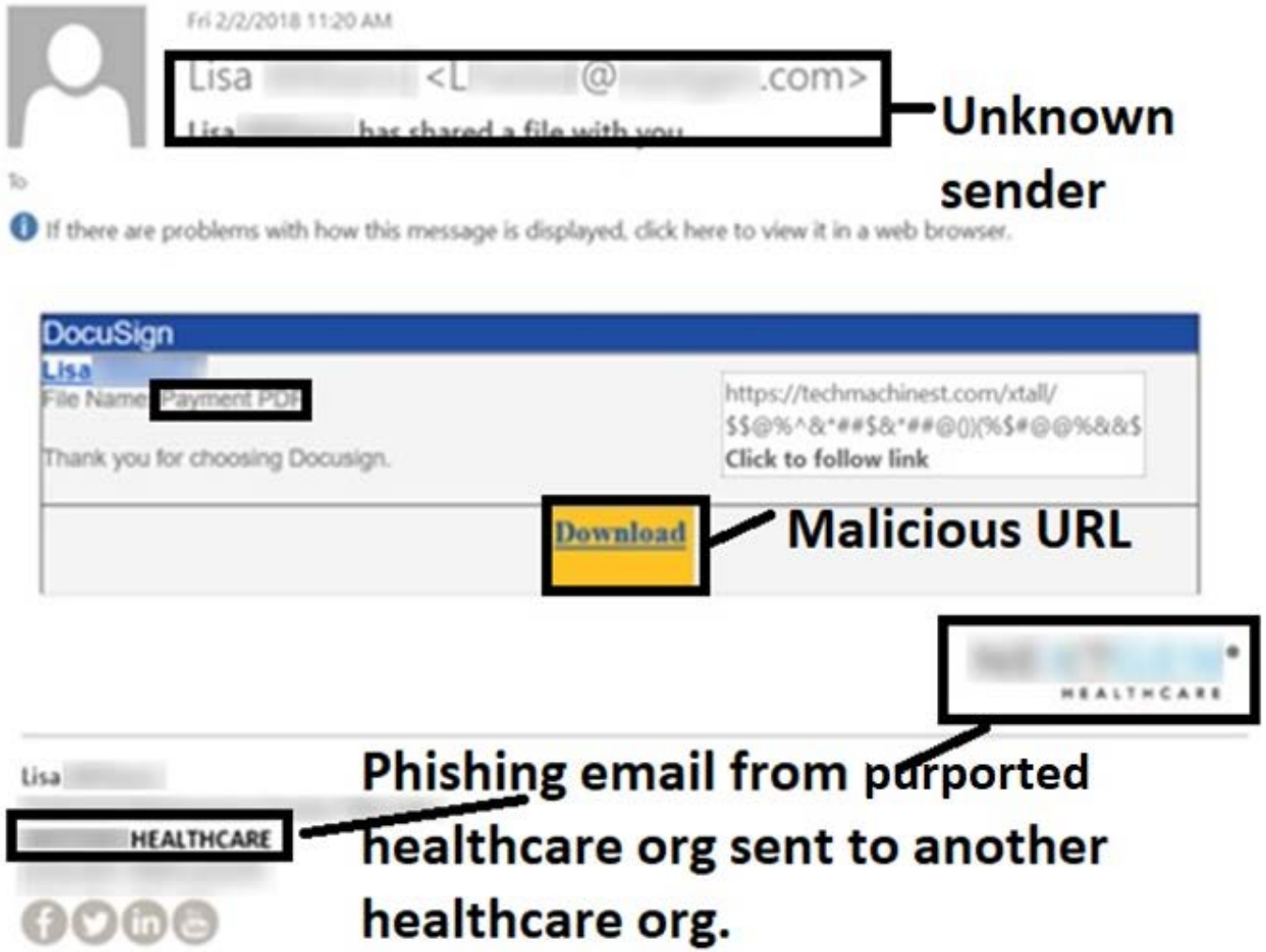
You can download the text file with the explanation of abuse by following the link
https://bit.ly/2jhnSC8 — Malicious link; real URL hidden

We also request that you send a response within 48 hours to us. This response should contain information about what you plan to do with it. — Urgency

Important notice:
When replying to us, leave the compliant ID "1757064939:90" unchanged in the subject. — Typo

Better Business Bureau
Abuse Department
Betty W Doyle

Spear-Phishing Example



Top Threat: Ransomware

- **Significant ransomware threat: Double extortion**
- **Phishing emails are generally the source of ransomware attacks.**
- **Ransomware operator: “If you don’t pay the ransom, we will leak your data.”**
- **No honor among thieves. Paying the ransom is no guarantee of safe return of data or that you won’t get extorted again.**
- **Consider engaging law enforcement, your insurance carrier (if you have cyber liability coverage through your insurance carrier), and legal counsel**
- **Tips: Do keep clean backups of data. Backup data on a regular basis. Determine if there is a reputable decryption tool for the ransomware infection.**

Top Threat: Credential Stealers

- **Phishing e-mails are often the source of credential stealing malware. The e-mail may appear to come from a trusted vendor or another trusted source.**
- **Credential stealing malware steal your credentials, generally via a fake landing page and/or keylogging software.**
- **Having a robust endpoint detection and response platform, web gateway, and e-mail gateway are recommended defenses.**
- **Tips: Do not reuse credentials. Do not use easy to guess credentials. Use multi-factor authentication whenever possible.**

Security Defenses

- Firewalls
- Endpoint detection and response platform (EDR)
- Multi-factor authentication
- Network gateways (all types of data: e-mail, web, etc.)
- Encryption at rest and in transit
- Patch management tools
- Data loss prevention software
- Incident response team and plan
- Business continuity and disaster recovery team and plan

Questions?

Lee Kim, JD, CISSP, CIPP/US, FHIMSS

Lee.Kim@himss.org

Resources

HIPAA

Phishing: Don’t be Phooled!

Top 10 routinely exploited vulnerabilities: Alert (AA20-133A)

Defending Against COVID-19 Cyber Scams

A Lifeline: Patient Safety & Cybersecurity

InfraGard Cyber Health Working Group

Stay Safe Online

Resources

HHS: Ransomware Fact Sheet

FBI: Ransomware Prevention and Resources for CISOs

The No More Ransom Project

MITRE ATT&CK Framework

Cyber Security Book of Knowledge