A Phish Tale: Lessons Learned from a Successful Phishing Attack in a Managed Care Organization

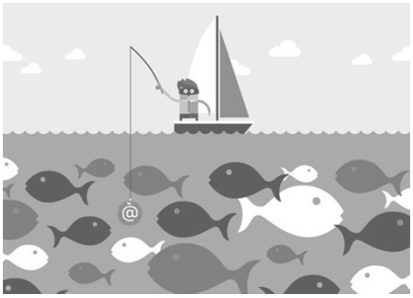
Jessica Vander Zanden, CHC - VP, Compliance and Audit, Network Health
Angela Keenan, CHC – Director, Privacy and Compliance, Network Health

Network Health - Background

- Founded in 1982, Network Health offers customized commercial and Medicare health plans to employers, individuals and families in more than 16 counties throughout northeast Wisconsin and beyond
- Network Health serves more than 165,000 members, including over 65,000 Medicare beneficiaries
- More information about Network Health is available at www.networkhealth.com, www.facebook.com/networkhealthwi and at www.twitter.com/networkhealthwi

Agenda

- Once Upon a Time – What Happened?
- Breach Requirements
- Security Controls
- Investigation Process
- Post Breach Actions
- Artifacts and Examples
- Lessons Learned



network health
networkhealth.com

3

Once Upon a Time

Once upon an August evening, came an email while some were sleeping.
Our prevention system tried stop it, but upon review the employee unblocked it.
The email's true sender was disguised as the recipient was like, "yup, I totally know this guy."
In that moment a link was clicked, the email recipient had been tricked.
A pop up seeking information became the subject of investigation.
The systematic measures had failed, and so begins Network Health's phish tale.

network health
networkhealth.com

4

Breach Requirements

- Risk Assessment
- Burden of Proof
- Individual Notices
- Substitute Notices
- Media Notices
- Notice to the Secretary
- Report to CMS

Security Controls

- Email Filtering Tool
- Security Awareness Efforts
- Penetration Testing
- Security Risk Assessment Process
- Third Party Security Reviews

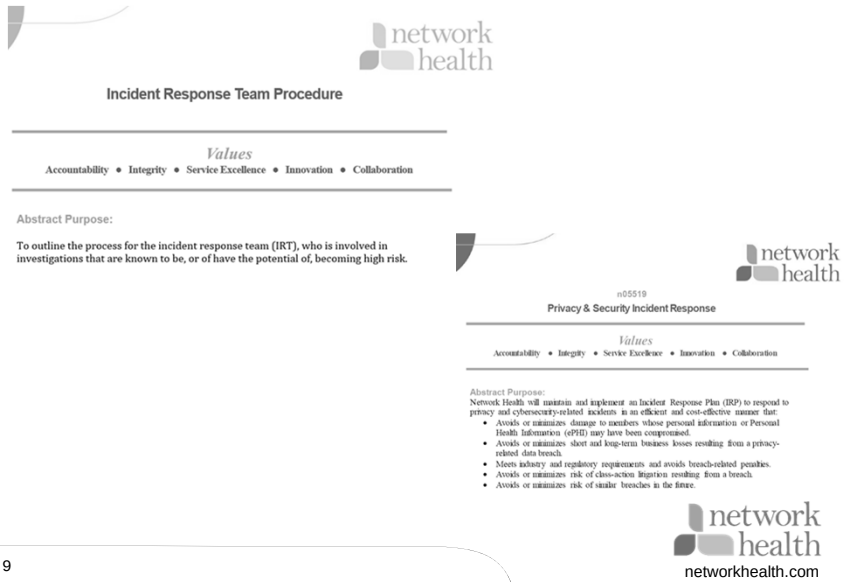
The Investigation Process

- Internal VS. External Resources
- Timeline
- Communications

Post Breach Actions

- Mass password reset
- Changes made to access allowances
- Messaging added on external emails
- Stronger PIN requirements implemented
- Messaging from general counsel sent

Artifacts and Examples



network health

Incident Response Team Procedure

Values

Accountability • Integrity • Service Excellence • Innovation • Collaboration

Abstract Purpose:

To outline the process for the incident response team (IRT), who is involved in investigations that are known to be, or of have the potential of, becoming high risk.

network health

n05519

Privacy & Security Incident Response

Values

Accountability • Integrity • Service Excellence • Innovation • Collaboration

Abstract Purpose:

Network Health will maintain and implement an Incident Response Plan (IRP) to respond to privacy and cybersecurity-related incidents in an efficient and cost-effective manner that:

- Avoids or minimizes damage to members whose personal information or Personal Health Information (ePHI) may have been compromised.
- Avoids or minimizes short and long-term business losses resulting from a privacy-related data breach.
- Meets industry and regulatory requirements and avoids breach-related penalties.
- Avoids or minimizes risk of class-action litigation resulting from a breach.
- Avoids or minimizes risk of similar breaches in the future.

network health

Artifacts and Examples

- If MIMECAST flags an email and puts it on hold, you need to review and always be cautious before releasing it.
  - If you are suspicious of an email:
    - **DO NOT** click on the links provided in the email.
    - **DO NOT** open any attachments in the email.
    - **DO NOT** provide personal information or financial data.
    - **DO** forward the email to the SPAMreporting@networkhealth.com and then delete it from your Inbox.
- If you receive an unexpected document in an email from a known sender, please CALL the sender to verify.
- **NEVER** send passwords to anyone in email.
- **NEVER** reuse your passwords across applications

1. Emails on mobile devices (Phones, IPADs, Tablets):
   If you receive Network Health emails on a mobile device, this change will impact you in the following ways:
   - If you currently have a 4 digit passcode, you will be asked to change it to 6 digit passcode. Additionally, simple passcodes like 123456 or 111111 will not be allowed. If you already have a 6 digit passcode, you don't need to take any action. If you have Touch ID (IOS) or fingerprint (Android) configured on your device, you can continue to use that feature to login. This change will be effective on Tuesday (9/5).

2. You will see a header and footer, as shown below, on incoming emails from external sources. As always please be careful with external emails.
   *** Attention: This email is from an external source. Use caution responding, opening attachments or clicking on links. ***

network health

Artifacts and Examples

Compliance Corner
September 2017

Phishing

It is important that we remain alert and aware of suspicious emails from outside parties. A common form of cyber-attacks is known as phishing.

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication. If you become suspicious of an email, here are a few reminders:

COMPLIANCE CORNER

DO NOT open any attachments in the email.

DO NOT click on the links provided in the email.

DO NOT provide personal information or financial data.

DO forward the email to the **SPAMreporting@networkhealth.com** and then delete it from your inbox as well as from your deleted emails.

If you receive an unexpected document in an email from a known sender, please **CALL** the sender to verify they sent it.

NEVER use Skype to transmit PHI.

AVOID including PHI in email whenever possible.

NEVER give out your usernames or passwords.

DO NOT reuse passwords for multiple applications.

Compliance posted a FAQ document on inNetwork with additional guidance. If you have questions, please contact compliance@networkhealth.com

network health
networkhealth.com

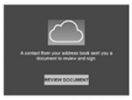
11

Artifacts and Examples

Tips to Recognize Phishing

- Look at the domain name in the email
- Hover over the link – **but do not click**

- Check for spelling mistakes
- Look for suspicious content
  - Is this an individual who normally sends you emails?
    Have you ever seen the type of link, document, etc they're asking you for?



Email and the Internet

It is easy to think of work email as being the same as email you might use at home. However, your work email contains much more sensitive information, and the risk of compromising your work email is much more severe than your home email account.

Keeping that in mind, always consider the following:

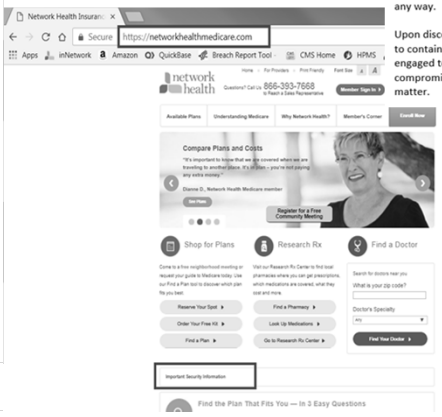
- Any email sent over the internet can be intercepted and read by others, including the Shared Services Operation (SSO) staff.
- Remember: Network Health owns all incoming and outgoing electronic communication, including email
- DO NOT send PHI, passwords, or other sensitive data via email *unless* it is in a secure format (i.e.; encrypted)

Email, IM and Other Electronic Transmissions Policy

network health
networkhealth.com

12

Artifacts and Examples



FOR IMMEDIATE RELEASE

Network Health Exposed to Sophisticated Email Phishing Attack

No financial information exposed; no evidence that exposed information misused in any way

MENASHA, WI – (Sept. 22, 2017) – In early August, two Network Health staff members were identified as the victims of a sophisticated email phishing attack by an unauthorized party which resulted in the potential exposure of their company emails. The emails did not contain any personal financial information and Network Health has no reason to believe that the exposed information was misused in any way.

Upon discovering the attack, Network Health took prompt action to secure the affected email accounts, to contain the impact and prevent further threats from the intruder. A forensic security expert was engaged to assess the attack and evaluate whether other areas of Network Health's network were compromised. In addition, federal law enforcement officials were notified and are investigating the matter.

Lessons Learned

- Establish a policy for maintaining emails
- Conduct knowledge checks of staff
- Incident Response Plan
- Concurrent Reporting to CMS
- Email screening tools

The End

With all of that our tale is done, and as you know, breaches are not much fun.
While we fell victim to a hacking curse, our situation could have been much, much worse.
Prevention, controls and education are key to ensure more phishing attacks are less likely.
We hope these lessons were helpful to you, in the event that you fall victim too.
These events are incredibly stressful – here's to all future attacks being unsuccessful!

Jessica Vander Zanden, CHC – jvanderz@networkhealth.com
Angela Keenan, CHC – akeenan@networkhealth.com