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.

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.
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

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 have the potential of becoming high-risk.

Privacy & Security Incident Response

Values
Accountability • Integrity • Service Excellence • Innovation • Collaboration

Abstract Purpose:
Network Health will maintain an incident response (IRT) to respond to privacy and security-related incidents in a timely and consistent manner for all stakeholders. Incident response activities will be conducted in a manner that is consistent with the following:
- Ensuring the safety and security of data and systems.
- Minimizing the impact of incidents on business operations.
- Complying with all relevant laws and regulations.

Artifacts and Examples

- If Outlook 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 not forward the email to the Helpdesk@networkhealth.com and then delete it from your inbox.
- If you receive an unexpected document as an email from a known sender, please CALL the sender to verify.
- NEVER send passwords to anyone in email.
- NEVER reuse 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 password, you will be asked to change it to 6-digit password. Additionally, simple passwords like 123456 or 111111 will not be allowed. If you already have a 6-digit password, 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 1/5/22.

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. ***

networkhealth.com
Artifacts and Examples

Compliance Corner
September 2017

Phishing

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, financial data) often by establishing a trustworthy entity in an electronic communication. If you become suspicious of a message, here are a few reminders:

- **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 IT Helpdesk (ITHelpdesk@networkhealth.com) and then delete it from your inbox as well as from your deleted emails.

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

**NEVER** use Skype to transmit PHI.

**AVOID** including PHI in email wherever possible.

**NEVER** give out your taxonomy or password.

**DO NOT** open passwords for multiple applications.

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

---

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 for?

Email and the Internet

It’s 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 covers 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, NH and Other Electronic Transmissions Policy
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