Social Engineering
Protecting PHI through the Weakest Link

Paul Douglas, CISA, CCSFP
Social Engineering Techniques
Common Social Engineering Attack Techniques

Phishing

Emails intended to acquire sensitive information
Examples from my inbox…….

Chase Online <info@chasing.com>

Important: Update

To:

Retention Policy 1 Year Permanent Delete (1 year, 3 months) Expires 12/7/2016

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Chase system upgrade, You are required to complete the online security maintenance of your account currently made available. We have updated our system to serve you better.

PLEASE NOTE: This is a mandatory measure. In order to keep our service safe and secured we kindly advice that you update all your records with us correctly or your online account access will be deactivated within 12hrs.

We need to re-confirm your account information with us this should be completed as soon as possible. Please sign on using the link provided below.

Click here to Continue

* PLEASE NOTE: If the verification is successful you will be transferred to the Chase Bank Welcome Page and you can use your account as regular. DO NOT Make any changes to your account.
Common Social Engineering Attack Techniques

Spear Phishing

Targeted emails customized for you and potentially the organization

Example: Target Breach
Examples from my inbox…….

Good day. I have attached a business proposal that I believe will be of mutual benefit to both of us to this email. Please go through the attached proposal and let me know if you are interested in working with us on this project. After reading the proposal, you can email me back on: afsurkazeem@syretmail.com so that we can go over the details together. If for some reasons you are unable to view the attachment, kindly inform me so that I can so that I can resend the proposal in a different format or plain text.

Regards.

Afsur.
A lot of Phish in the Sea…..

23% OF RECIPIENTS NOW OPEN PHISHING MESSAGES AND 11% CLICK ON ATTACHMENTS.

50% NEARLY 50% OPEN E-MAILS AND CLICK ON PHISHING LINKS WITHIN THE FIRST HOUR.

* Verizon 2015 Data Breach Investigations Report
Common Social Engineering Attack Techniques

Physical Spoofing

Physical impersonation of an employee or vendor
Common Social Engineering Attack Techniques

Remote Spoofing

Impersonation of a device, employee, or vendor

Example: Windows Support Calls
Common Social Engineering Attack Techniques

**Baiting**

- Physical objects used (CDs, USBs) to “bait” employees
- Example: Iranian nuclear plant USB drop
“A Network of Human Sensors”

“One of the most effective ways you can minimize the phishing threat is through effective awareness and training. Not only can you reduce the number of people that fall victim to (potentially) less than 5%, you create a network of human sensors that are more effective at detecting phishing attacks than almost any technology.”

Lance Spitzner
Training Director for the SANS Securing The Human Program
Employee Information Security Training

1. Diagnose the readiness of your employees for a social engineering attack
2. Design custom IT security training to address gaps / improvement opportunities with your workforce
3. Monitor progress though periodic testing and follow-up activities
Employee Information Security Training

Social Engineering Success Rate

<table>
<thead>
<tr>
<th>Year</th>
<th>Social Engineering Success Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015</td>
<td>35%</td>
</tr>
<tr>
<td>2016</td>
<td>30%</td>
</tr>
<tr>
<td>2017</td>
<td>25%</td>
</tr>
<tr>
<td>2018</td>
<td>20%</td>
</tr>
<tr>
<td>2019</td>
<td>15%</td>
</tr>
</tbody>
</table>
Breach Statistics

Data Breach Summary:
• Data from September 2009-April 2015
• Breaches affecting 500 or more individuals: 1,190
• Involving a Business Associate: 272 (23%)
• Amount of individuals affected: 129,466,215

Data Source: www.hhs.gov
# Breach Statistics

<table>
<thead>
<tr>
<th>Data Breach Type</th>
<th>% of Breach Type by Occurrence</th>
<th>% of Individuals Affected</th>
<th>Sum of Individuals Affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hacking/IT Incident</td>
<td>10%</td>
<td>74%</td>
<td>95,575,317</td>
</tr>
<tr>
<td>Improper Disposal</td>
<td>4%</td>
<td>1%</td>
<td>764,514</td>
</tr>
<tr>
<td>Loss</td>
<td>10%</td>
<td>6%</td>
<td>7,514,208</td>
</tr>
<tr>
<td>Theft</td>
<td>54%</td>
<td>15%</td>
<td>20,362,698</td>
</tr>
<tr>
<td>Unauthorized Access/Disclosure</td>
<td>22%</td>
<td>4%</td>
<td>5,249,478</td>
</tr>
<tr>
<td><strong>Grand Total</strong></td>
<td><strong>100%</strong></td>
<td><strong>100%</strong></td>
<td><strong>129,466,215</strong></td>
</tr>
</tbody>
</table>
Impact of the Anthem, Inc. Data Breach

Patient Records Breached

Pre-Anthem: 49,466,215
Post Anthem: 129,466,215
Regulatory Impact – HIPAA Security Rule

Health Insurance Portability and Accountability Act (HIPAA) Security Rule

- §164.308(a)(1) Security Management Process
- §164.308(a)(5) Security Awareness and Training
- §164.308(a)(8) Technical / Non-Technical Evaluation
- §164.316(a) Policies and Procedures
Regulatory Impact – PCI DSS

Payment Card Industry Data Security Standard Version 3.0

Requirement 11.3.1 – 11.3.3 – Perform a Penetration Test and Exploit Vulnerabilities


Requirement began June 30, 2015
Paul Douglas, Consulting Manager
225.408.4421
pdouglas@pncpa.com
Connect with me on LinkedIn

- Founded in 1949
- #1 largest Louisiana accounting firm
- Top 100 professional services firm in US