HEISC Webinar

Phishing Programs: Chapter 1
Getting Your Campus Ready for a Phishing Awareness Campaign

Presented by the EDUCAUSE Cybersecurity Initiative

April 11, 2017 • 3–4 pm EDT

www.educause.edu/security
Today’s Speakers

Sandra Silk  
*Director of IT Security Education & Consulting*  
Harvard University

Eric Weakland  
*Director, Information Security*  
American University
Three Main Areas

1. Response capabilities
2. Customer call to action
3. Internal communication practices
Response Capabilities

• Where are gaps/inconsistencies in process across the full organization?
• Where are pain points for end users?
• Is spam within scope of reporting?
• Where are sticking points or gaps in triage?
• What service expectations are you setting with your community?
Gaps and Inconsistencies

- How many different teams are performing triage?
- Do they all use the same process and standards?
- Where are the delays in escalations?
Customer Pain Points → Abandonment

- This is spam or phishing
  - Will this harm our School?
    - Yes → Forward as attachment to phishing mailbox
  - No → Could others be harmed?
    - Yes → [Process]
    - No → [Process]

- What email do you use?
  - [Options]
    - Outlook for Windows
    - Outlook for Mac
    - Gmail
    - O365
    - Apple Mail
    - Other

- This is too complicated. Delete and move on.
Quick Poll #1

What types of messages do you ask users to report?

• University-specific phishing only
• Any phishing, but not spam
• Anything - phishing and spam
Set Service Level Expectations

Are you responding to each report?
- Is it an auto-response or custom?
- Will there be follow-up?

What level of effort goes into triage for:
- University-specific phishing?
- Other phishing?
- Spam?
Cut your response time

Where can you streamline triage?

- Automation
- APIs
- Take-down notices
- Hand-offs and tickets
• Primary goal: Detection or reporting?

• Simple sleuthing skills

• URL rewrites - Does it factor into your messaging?

• With power comes responsibility
  High value targets
  High value influencers in community
What’s your primary driver?

Focus on one goal – detection or reporting.
Simple Sleuthing Skills

Check with “source” of questionable message:

• Call
• Text
• Go to official website and login

When in doubt, assume it’s bogus
URL Rewrites

“Between the lines”

 Adds a layer of complexity to analysis:

- Ignore the domain name
- Interpret ASCII text

Is this a “critical path” skill?
Who has power?

High Value:

Targets

• Celebrity faculty members
• C-Suite
• Government appointments
• Scholars at risk

Gatekeepers / Influencers

• Executive Assistants
• Department Admins
• Faculty Assistants
Internal Communication Practices

• Why bother? Who benefits?

• Who should I be reaching out to on campus?

• Phish or Flop? Fifty Shades…

• When to cry “Phish!”
Quick Poll # 2

How are you dealing with third-party links in “official” university messaging? (Check all that apply)

- Use them “as is”
- Provide navigation instructions instead of links
- Use a central URL shortener (bit.ly type or internal hosted)
- CNAME (DNS) entries for click-through tracking
## Why bother? Who benefits?

<table>
<thead>
<tr>
<th>Neutralize Phish</th>
<th>Reduce Flops (Faux Pas)</th>
<th>Focus on Fine</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increase the security of institutional and individual information.</td>
<td>Improve the effectiveness of your broadcast email communications.</td>
<td>Preserve email channel as a means for important messaging.</td>
</tr>
</tbody>
</table>
Phish or Flop?

Fifty Shades of

Your email WON’T see you now....

- Unfamiliar sender
- Link to a “login page”
- Lack of text version
- Attachment
- Red text
- Many images
- Linking to multiple domains
- ALL CAPS
- Keywords on spam list
- Typos
- High “bounce” rate
- No unsubscribe link
When to Cry “Phish!”

- Know your culture
- Choose your battles
- Less is more, when it really counts
Suggested Resources

- Defeating Phishing and Spear-Phishing Tactics (*EDUCAUSE Review* guest blog)

- Annual Security Awareness Campaign (HEISC resources with customizable content)
  - February 2017: Learn What It Takes to Refuse the Phishing Bait
  - November 2016: Avoiding Ransomware Attacks
  - April 2016: Don’t Get Hooked

- **HEISC Information Security Guide**
Poll 1: What types of messages do you ask users to report?

- University-specific phishing only: 5%
- Any phishing, but not spam: 50%
- Anything - phishing and spam: 45%
Poll 2: How are you dealing with third-party links in "official" university messaging? (Check all that apply.)

- 23% Use them "as is"
- 7% Provide navigation instructions instead of links
- Use a central URL shortener (bit.ly type or internal hosted)
- CNAME (DNS) entries for click-through tracking
- Combination of any of the 4 options