HEISC Webinar

Too Legit to Quit: How to Avoid Making Legitimate Campus Messages Look Phishy

Presented by the EDUCAUSE Cybersecurity Program
February 21, 2018 • 3–4 pm EST

www.educause.edu/security

UNCOMMON THINKING FOR THE COMMON GOOD
**Poll Question #1**

How are you dealing with third party links in “official” university messaging?

<table>
<thead>
<tr>
<th>Option</th>
<th>Percentage</th>
<th>Votes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use them as is</td>
<td>83.9%</td>
<td>68</td>
</tr>
<tr>
<td>Provide navigation instructions instead of links</td>
<td>32.1%</td>
<td>26</td>
</tr>
<tr>
<td>Use a central URL shortener (e.g., bit.ly or internal hosted)</td>
<td>22.2%</td>
<td>18</td>
</tr>
<tr>
<td>CNAME (DNS) entries for click-through tracking</td>
<td>1.23%</td>
<td>1</td>
</tr>
</tbody>
</table>

*Uncommon Thinking for the Common Good*
Today’s Speakers

Petr Brym
Assistant CISO
University of California, Davis

Patricia Clay
Director of Information Technology
DeSales University

Ed Hudson
Interim CISO
California State University, Office of the Chancellor
Introduction

- The phishing attack challenge
  - Increasing sophistication & success
  - Persistence
- Educating end users is not enough
- What else can we do?
- Which approaches work for you?
Navigation Instructions vs. Link

- **Links are good**
  - Easy to navigate
  - Reader knows what to do

- **Links are bad**
  - Too easy to click on without vetting
  - Readers are busy and in a hurry
  - Trains users to click! Ready to phish!

- Navigation skills provide long-term benefit
- Navigation skills are easier to teach to repeat audience with established websites
Example of Navigation Instructions

- Go to MyDSU [university portal]
- Select “Menu”
- Select “Policies and Procedures”
- Navigate to the “XYZ” policy link

- Go to MyDSU
- In the Applications section, choose Housing@DSU
- Do the xyz action
Send Clean Message

- Lessons learned from detour signs
  - Simple
  - Recognizable
  - Focused

- Readers are like drivers
  - In a hurry
  - Limited time to make a decision
  - Have to process the unexpected
What Would You Do?
Is Less More?

- How much time does the average recipient have to analyze each e-mail message?
- What percent of e-mail messages have links or attachments?
- One person’s 1.5 days
  - 51 emails with no links
  - 81 emails with links
- What’s your client’s experience?
What Would You Do?

Subject: Urgent message from campus security

Good morning, this is an alert from the campus Information Security Team. These alerts are released when unexpected or urgent situations arise that require your immediate attention.

The campus experienced an unprecedented amount of phishing and vishing attacks during the past 24 hours. The campus Information Security Team wants you to be safe. Please log in at https://xy9eb.moc or browse www.ourcampus.edu to view important details regarding today’s events and how to remain safe.

Warning: Legitimate e-mail messages are easily imitated and abused for malicious intent. We will never ask you for sensitive information by e-mail. Never click on links in unexpected messages. Before clicking on links, hover over them to see where they really lead. To confirm whether this is a legitimate e-mail, call the help desk at 800-84X-7394.
Register Messages

- Establish a known site
- Include public and authenticated options
- Publish messages on the site
- Reference the site in the email

Effective for repeat audiences
Less effective for one-time audiences

Example from UC Davis…
Example of Message Registration

The Following Messages Were Distributed To the Campus Community in abbreviated format. View the full message by selecting the corresponding subject and date stamp.

Subject: Campus Holidays, Date 1/5/2018
Subject: Phishing Alert, Date 1/18/2018
Subject: Guest Speakers, Date 2/1/2018
DMARC

- Identifies legitimate messages
- Helpful with obvious threats
  - Ransomware, phishing and spam
- With a bit of preparation, can be effective for both repeated and one time message
- Makes it easier to identify if other are spoofing your domain
- Adoption rate is critical
- Can reject legitimately spoofed emails (EDUCAUSE listserv)
Poll Question #2

Do you employ any of these strategies?

Poll #2: Do you employ any of these strategies? (select all that apply)

- An official site to look up known phishing attempts: 42.3% (36)
- DMARC: 24.7% (21)
- Digitally signed messages: 15.2% (13)
- Phishing simulation: 54.1% (46)
- Other options? Add your comments in the chat!: 16.4% (14)
Digitally Signed Messages

- Highly effective
- High learning curve
- High Integrity/Non-Repudiation
Phishing Simulation Tools

- Potentially core component of a phishing education
- Can be effective, but it can also blow up
- Need to plan ahead and secure executive support
- Better as part of planned campaign
- Pre-determine consequences and outcomes
- But could benefit both repeated and one-time messages

**Examples:** PhishMe, Gophish, KnowBe4, SANS
Poll Question #3

Do you believe phishing simulation is effective?

Poll #3: Do you believe phishing simulation is effective?

- Yes, but we do not have buy-in to do it (16.8%, 14)
- Yes, but only with consequences (2.41%, 2)
- Yes, but only with training associated (71.0%, 59)
- No, it erodes confidence (9.64%, 8)
- No, it does not help people learn about real phishing attempts (0%, 0)
Phishing Simulation

- **Warn in advance?**
  We announced the phishing campaign

- **Consequences?**
  DeSales locked accounts for users who did not complete training in 3 business days

- **Complainers?**
  Some of our complainers became champions

---

#CyberAware – Be Aware, Phishing is coming

October 4, 2017 by hillj

DeSales Community –

As a part of our NCSAM #CyberAware activities, the Information Technology Department will be sending out simulated phishing messages. Can you spot the phish? If you find one, please report it to helpdesk@desales.edu and we will get back to you. As ever, keep these tips in mind:
Poll Question #4

Do you have any PSAs that you use at your institution?

Poll #4: Do you have any PSAs that you use at your institution? (select all that apply)

- Yes, we have produced our own: 57.6% (49)
- Yes, we have student produced PSAs: 8.24% (7)
- Yes, we employ resources from Stop. Think. Connect. or other government resources: 44.7% (38)
- Yes, we use publicly available resources: 30.5% (26)
- Not yet, but we are currently exploring or developing resources: 7.06% (6)
- No, we do not: 16.4% (14)

UNCOMMON THINKING FOR THE COMMON GOOD

EDUCAUSE
Resources

- UCOP Systemwide Guidance – Prevent Emails from Looking Phishy: [https://security.ucop.edu/guides/create-less-phishy-emails.html](https://security.ucop.edu/guides/create-less-phishy-emails.html)
- PSA Video from DeSales University Student: [https://www.youtube.com/watch?v=BfDKBXr6PVY](https://www.youtube.com/watch?v=BfDKBXr6PVY)
- Campus Security Awareness Campaign, 2018 materials: [https://www.educause.edu/securityawareness](https://www.educause.edu/securityawareness)