Phishing Simulation Programs

A Higher Education Information Security Council (HEISC) Resource

April 2016
What Is a Phishing Simulation Program?
A phishing simulation program (also commonly referred to as “self-phishing” or phishing assessment program) is a customizable awareness program used by information security professionals in higher education and private industry. This highly effective training program allows organizations to simulate phishing e-mails, help identify which end users are more susceptible to such targeted e-mail attacks, and engage in more focused training opportunities to help users recognize phishing attempts.¹

Who Might Use a Phishing Simulation Program, and Why?
It is inevitable that end users will be targeted by a phishing scam, which is usually part of a more sophisticated attack on an organization.² Recent examples where the attackers got their initial foothold through phishing include Target,³ Anthem,⁴ and various direct deposit scams.⁵ To address these constant phishing attempts, an institution can use a phishing simulation program to help train end users about malware and other current threats introduced via e-mail or online browsing. Each phishing campaign provides immediate feedback, as well as comprehensive analytics and reporting about employee behavioral responses, ultimately resulting in a more secure campus environment.

The Benefits of Using a Phishing Simulation Program
A phishing simulation program is one of the few information security training techniques that can be easily measured and provides data to gauge effectiveness. More campuses are following private industry and starting to deploy phishing campaigns. The benefits include:

1. Providing an established training process that can be implemented monthly, quarterly, or annually as part of a more mature information security awareness program.
2. Allowing for targeted education campaigns using unique scenarios or variables (e.g., attachments, embedded links, or requests for personal information) for high-risk end user groups (e.g., new employees; staff dealing with financial transactions or employee records; stewards handling highly sensitive data; IT staff with admin privileges).
3. Establishing a baseline for all end users and developing metrics that best suit the campus culture (e.g., click rates—how many click on the message and fall for the scam or report rates, how many report the potential phishing message).

¹ Phishing is a form of online fraud where an attacker poses as a legitimate company and tries to trick a victim into sharing login credentials or account information. Attackers often use e-mail to perpetuate this type of fraud.
⁵ See REN-ISAC, “Advisory: University Payroll Theft Scheme,” November 12, 2014 [PDF]; and “IRS Alerts Payroll and HR Professionals to Phishing Scheme Involving W-2s,” IRS, March 1, 2016.
4. Reducing the number of end users that fall for phishing messages.
5. Minimizing risk by training a broader population to be more aware of current phishing scams or threats and proactively report suspected phishing messages.
6. Identifying end users frequently taking “undesired actions” by falling for phishing e-mails and using that information to deliver targeted training where it is most needed, when it is needed.
7. Leveraging end-user responses and metrics to identify gaps in existing security awareness materials and tailor materials to fit the training needs of the institution.
8. Providing end users with real-time, tangible feedback.
9. Offering end users a sense of accountability (i.e., cybersecurity is everyone’s responsibility) and helping everyone be prepared for potential cyberattacks.

Risks to Consider When Using a Phishing Simulation Program
Institutions must also weigh the risks of a phishing simulation program.

1. What may be seen as positive reinforcement of desired behaviors on one campus may be seen as a disciplinary measure or monitoring of employees on another campus. Ensuring that you have institutional leadership support before launching a phishing simulation program is crucial. You can demonstrate that a phishing campaign is a positive, effective, nonpunitive training tool that provides the opportunity to seize “teachable moments.” Start with a small pilot group and allow participants to ask questions or state concerns before the program is more broadly deployed. Gaining support or approval of end users that were initially skeptical can lend credibility to the new program and help build trust across campus.
2. Once the program is launched, you can also avoid the appearance of undermining an end user’s privacy by informing the community ahead of time about the phishing campaign. Note that some campuses may use different strategies.
3. If you have limited IT or help desk staff, consider streamlining the procedures for reporting suspected phishing e-mails before launching the program. Following a phishing campaign, the help desk could see a large jump in end users reporting “phishy” messages.
4. Creating a recognition or ambassador program will engage tech-savvy end users who believe they do not require additional training about suspicious e-mails.

List of Phishing Simulation Technologies and Tools
Below is a list of popular phishing simulation programs or tools for your consideration. Depending on your institution’s financial and/or personnel resources, you might select a hosted commercial service or an open-source solution (costs will vary). Each institution should
evaluate which tool will work best for its unique purposes. Neither EDUCAUSE nor HEISC recommends the use of a particular tool; institutions should use these tools at their own risk.

- GoPhish (open source)
- KnowBe4: phishing security test
- PhishLine: social engineering simulations
- PhishMe (simulator)
- Simple Phishing Toolkit (open source)
- Wombat Security: ThreatSim simulated phishing assessments

Additional Resources
- EDUCAUSE Review guest blog, April 4, 2016: Phishing Your End Users
- SANS Securing The Human presentation: Building an Effective Phishing Program
- SANS Securing The Human resource: Phishing Planning Checklist (part of the downloadable Security Awareness Planning Kit)
- US-CERT Security Tip: Avoiding Social Engineering and Phishing Attacks

Sustain and Improve Your Information Security Program
The Higher Education Information Security Council (HEISC) supports higher education institutions as they improve information security governance, compliance, data protection, and privacy programs. The HEISC Information Security Guide, created by practitioners for practitioners, features toolkits, case studies, effective practices, and recommendations to help jumpstart campus information security initiatives. Don’t reinvent the wheel—get the guide at educause.edu/security.