Secrets to an Effective Phishing Program

https://securingthehuman.sans.org
@securethehuman
Security Awareness Maturity Model

- Non-existent
- Compliance Focused
- Promoting Awareness & Behavior Change
- Long-Term Sustainment & Culture Change
- Metrics Framework
Fogg Behavior Model

B = mat
behavior motivation ability trigger at same moment

High Motivation

Low Motivation

motivation

Action Line

triggers succeed here

triggers fail here

Hard to Do

ability

Easy to Do

For permissions, contact BJ Fogg

www.BehaviorModel.org

© 2007 BJ Fogg
Two Types of Metrics

• **Compliance Metrics**: Measure the deployment of your awareness program. Are you compliant?

• **Impact Metrics**: Measure the impact of your awareness program. Are you changing behavior?
Why Phishing?

- Phishing is a useful metrics for most organizations:
  - Measures a key human risk organizations care about
  - Simple, low cost and easy to repeat
  - Quantifiable measurements that are actionable
- 90% fall victim in the first hour
Key Points

• Biggest difference between technical and human metrics is that humans have feelings
• Announce your metrics program ahead of time, and then start slow and simple
• Do not embarrass people (no Viagra e-mails)
• Do not release names of those who fail. Only notify management of repeat offenders
• Focus on real-world risks, do not “trick” people
• Always make sure there are at least two ways to detect an assessment
Get Approval

• Before conducting any type of assessment, make sure you have appropriate approvals
• Can’t get approval? Try a test run against the blockers (such as HR and Legal)
• Make sure security team knows ahead of time. Let them know each time when you do it and whom to contact when things go wrong
Dear Customer,

We hope you enjoyed your recent flight! As a valued customer you are entitled to 10,000 bonus miles. This bonus offer will expire in 48 hours, so hurry!

Click Here to Claim Instantly

Frequent Flier Customer Relations
Enrollment Review Required

John Doe,

Governmental stipulations as outlined by the Affordable Care Act have caused us to make changes to this year’s Employee Benefit Plan. These changes may affect your current enrollment. Please click here to review and if necessary, update your information.

You may update any of, but not limited to, the following plans: Dental Plan, Group Term Life Insurance, Voluntary Group Term Life (VTTL), Accidental, Cancer, Critical Care Elite, Hospital Confinement, Group Short Term Disability, Voluntary Long Term Disability and Vision Plan.
Click Results

If a person falls victim to a phishing assessment, you have two general options:

• No feedback
• Immediate feedback that explains this was a test, what they did wrong, and how to protect themselves
Whoops...
You just got phished!

Fortunately this was an authorized training simulation, but if it had been a real phishing attempt, your online safety could have been compromised. Opening and reading email is fine, but clicking on malicious links or attachments could cause you harm.

**Common clues of a phishing attack**

- Messages that create a tremendous sense of urgency may be trying to rush you into making a mistake.
- If it sounds too good to be true, it probably is (no, you did not just win the lottery).
- Official organizations don’t usually send messages that are full of grammatical errors and spelling mistakes. They also don’t come from personal email addresses (such as @gmail.com, @yahoo.com, or @hotmail.com).
- Messages that open with “Dear Customer” or some other generic greeting should get close scrutiny.
- No legitimate organization should request highly sensitive information over email such as your credit card number or account password.
- The message comes from someone you know, but they just don’t sound quite right. Cyber attackers can send emails that look like they come from your boss, co-worker, or friend in order to gain your trust.
Follow-Up

• Send results of test to all employees 24 hours later
• Explain results and how they could have detected phishing e-mail and what to look for in the future. Include screen shot of phishing e-mail
• Include your monthly security awareness newsletter
Violations

1. First violation, employee is notified with additional or follow-on training
2. Second violation, employee is notified and manager is copied
3. Third violation, manager is required to have meeting with employee and report results to security
4. Fourth violation, employee reported to HR
Phishing Results

• First phish: 20 to 50% fall victim
• 12 months later: Low as 5%
• The more often the assessments, the more effective the impact
  • Quarterly: 20%
  • Monthly: 05%
• Over time, you will most likely have to increase difficulty of tests
Legal Issues

• Is it legal to use another organization’s brand in a phishing assessment?
• To be honest, no one fully knows. Ultimately, a decision your legal has to make
• You can create effective phishing e-mails that do not use another organization’s brand
Human Sensors

- Another valuable metric is how many reported the attack
- If you measure this, you have to first train people on how to report
- May need a policy on what to report:
  - Do not report when you know you have a phish, simply delete
  - Report if you don’t know (think APT)
  - Report if you fell victim
Phishing Summary

• Success is ultimately not about technology but about communication.
• Always keep emotion in mind and start slow.
• When done right, phishing can become a powerful and gamified form of both metrics and learning.
Resources

- Awareness roadmap / posters
- Monthly OUCH! awareness newsletter
- Video of the Month
- Summits, two day courses and webcasts

securinthehuman.sans.org
**DON’T GET HOOKED!**

**WHAT IS PHISHING?**
Phishing is a psychological attack used by cyber criminals to trick you into giving up information or taking an action. Phishing originally described email attacks that would steal your online username and password. However, the term has evolved and now refers to any attempt to obtain sensitive information using unsecured messaging.

These attacks begin with a criminal sending a message pretending to be from someone or something you know, such as a friend, your bank or a well-known store.

These messages then entice you into taking an action, such as clicking on a malicious link, opening an infected attachment, or responding to a scam. Cyber criminals craft these convincing-looking emails and send them to millions of people around the world. The criminals do not know who will fall victim, they simply know that the more emails they send out, the more people will have the opportunity to hack. In addition, cyber criminals are not limited to just email but will use other methods, such as instant messaging or social media posts.

**WHAT IS SPEAR PHISHING?**
The concept is the same as phishing, except that instead of sending random emails to millions of potential victims, cyber attackers send targeted messages to a very few select individuals. With spear phishing, the cyber attackers research their intended targets, such as by reading the intended victims’ LinkedIn or Facebook accounts or any messages they posted on public blogs or forums. Based on this research, the attackers then create a highly customized email that appears relevant to the intended targets. This way, the individuals are far more likely to fall victim.

**WHY SHOULD I CARE?**
You may not realize it, but you are a phishing target at work and at home. You and your devices are worth a tremendous amount of money to cyber criminals, and they will do whatever they can to hack them. YOU are the most effective way to detect and stop phishing. If you identify an email you think is a phishing attack, or you are concerned you may have fallen victim, contact your help desk or security team immediately. To learn more about phishing or the SANS Phishing The Human Phishing Testing Platform, please visit http://www.sans.org/secure/

**PHISHING INDICATORS**

**A.** Check the email addresses. If the email appears to come from a legitimate organization, but the "FROM" address is someone’s personal account, such as ajroberts@gmail.com or ajroberts@hotmail.com, this is most likely an attack. You should check any "CC" fields. Is the email being sent to people you do not know or do not work with?

**B.** Be suspicious of emails addressed to "Dear Customer" that use some other generic salutation. If a trusted organization has a need to contact you, they should know your name and information. Ask yourself, am I expecting an email from this company?

**C.** Be suspicious of grammar or spelling mistakes; most businesses proofread their messages carefully before sending them.

**D.** Be suspicious of any email that requires an "immediate action" or creates a sense of urgency. This is a common technique to rush people into making a mistake. Also, legitimate organizations will not ask you for your personal information.

**E.** Be careful with links, and only click on those that you are expecting. Also, hover your mouse over the link. This shows you the true destination of where you would go if you clicked on it. If the true destination is different than what is shown in the email, this is an indication of an attack.

**F.** Be suspicious of attachments. Only click on those you are expecting.

**G.** Be suspicious of any message that sounds too good to be true. No, you did not just win the lottery.

**H.** Just because you got an email from your friend does not mean they sent it. Your friend’s computer may have been infected or their account may be compromised. If you get a suspicious email from a trusted friend or colleague, call them on the phone.
Special Discount Program GOV / EDU

- Through 31 Jan State / Local governments and universities, colleges and K12s receive discount pricing on STH Training and Phishing.
  - GOV: sans.org/partnership/cis
  - EDU: sans.org/partnership/education

partnership@sans.org