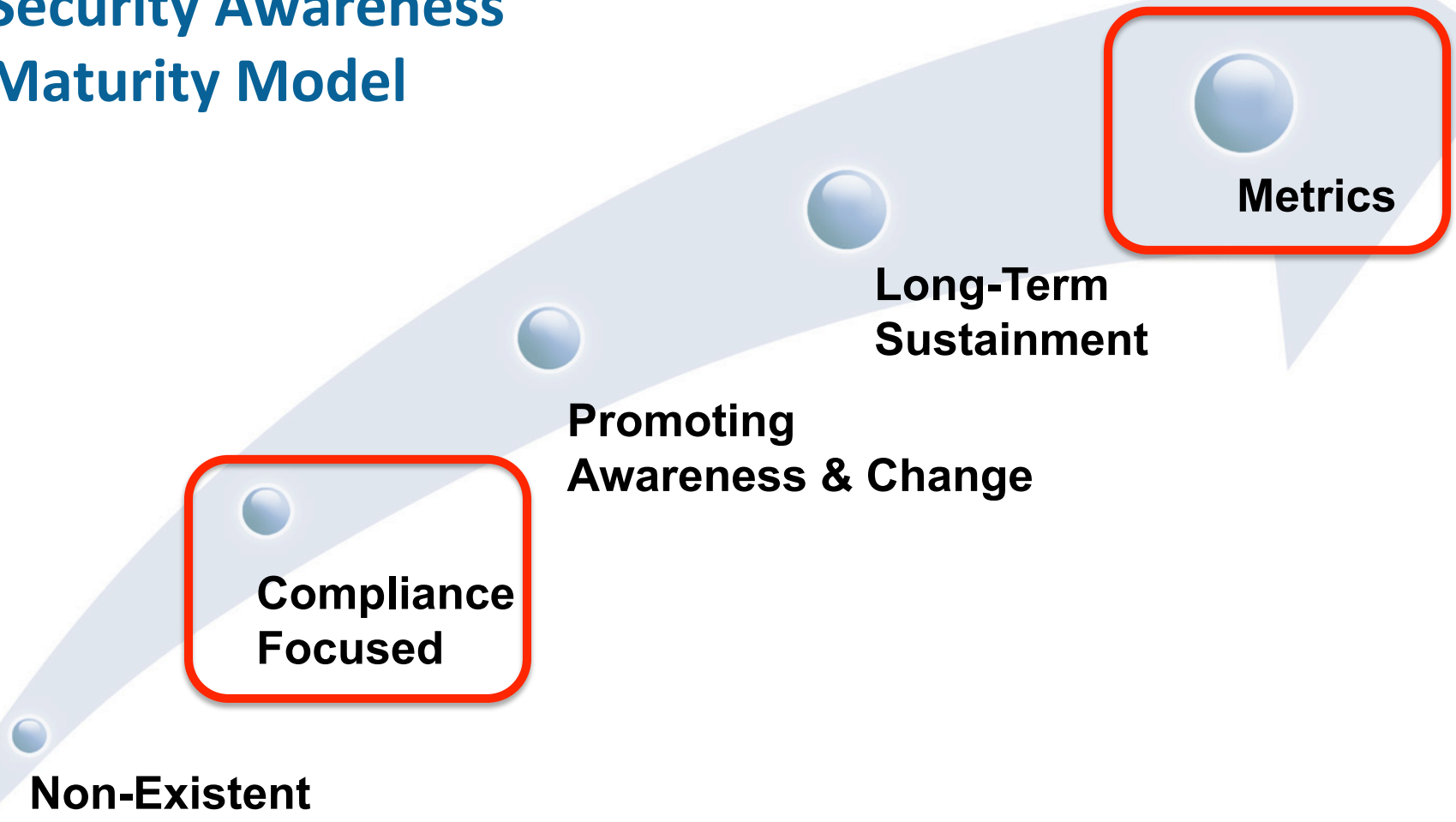
Building an Effective Phishing Program

www.securingthehuman.org
info@securingthehuman.org
@securethehuman

Security Awareness Maturity Model



Two Types of Awareness Metrics

- Metrics that measure the deployment of your awareness program - are you compliant?
- Metrics that measure the impact of your awareness program – are you changing behavior?

Why Phishing?

Recreate the very same attacks that the bad guys are launching. Excellent way to measure change in behavior

- Measures a high human risk
- Simple, low-cost and easy to repeat.
- Quantifiable measurements
- Actionable

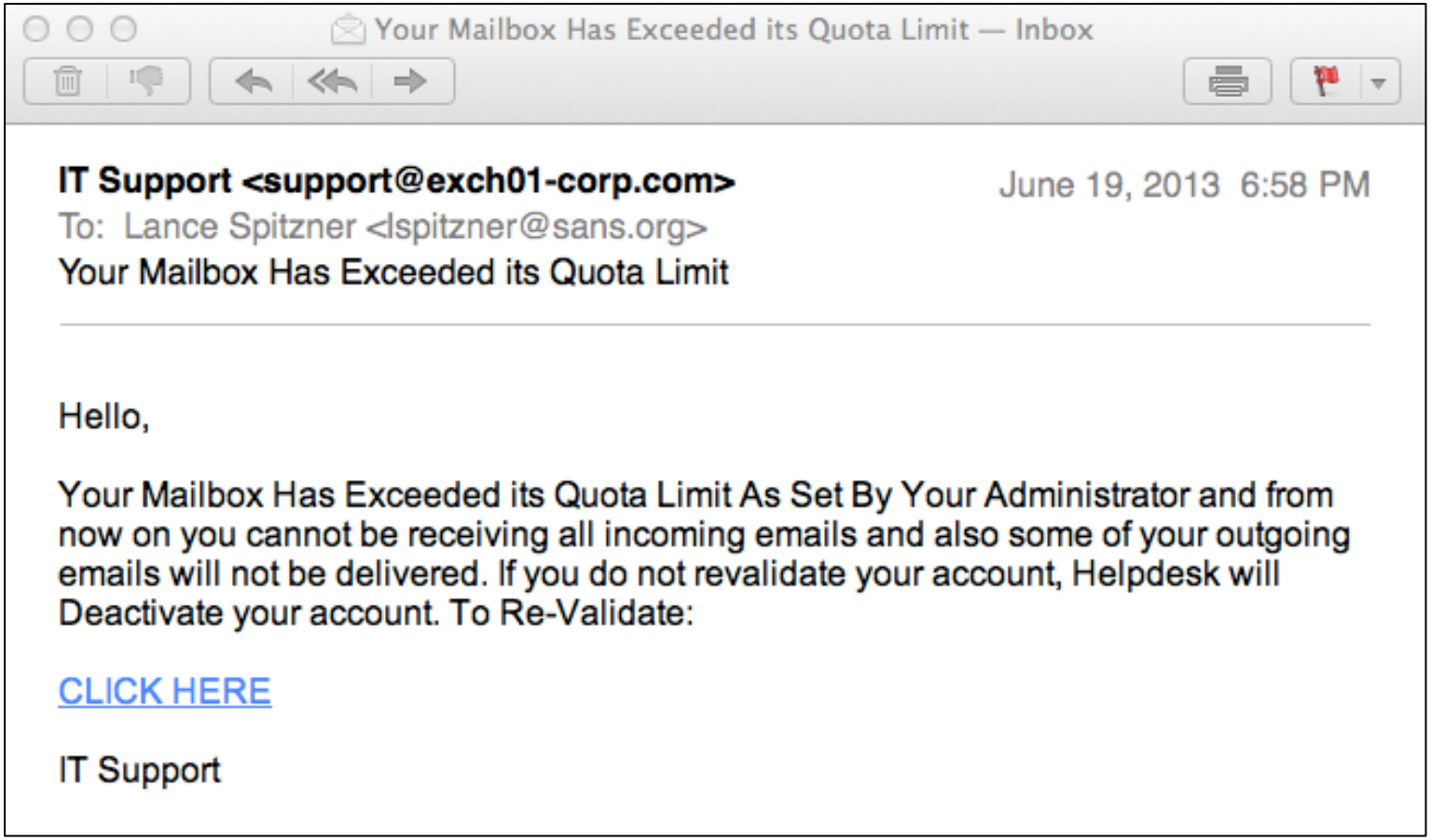
Key Points - 1

- Remember that while computers do not have feelings, people do. Emotion, not technology, is your biggest challenge
- Announce and explain your phishing program ahead of time
- Start your program with very simple phishing emails, then increase difficulty only after people are used to the program

Key Points - 2

- Ensure there are at least 2-3 ways people can detect the phish
- Do not embarrass people by releasing names of victims, nor should their names be reported to management. Only notify management of repeat offenders
- 90% of victims fail in the first two hours

Example


Your Mailbox Has Exceeded its Quota Limit — Inbox
IT Support <support@exch01-corp.com>
June 19, 2013 6:58 PM
To: Lance Spitzner <lspitzner@sans.org>
Your Mailbox Has Exceeded its Quota Limit
Hello,
Your Mailbox Has Exceeded its Quota Limit As Set By Your Administrator and from now on you cannot be receiving all incoming emails and also some of your outgoing emails will not be delivered. If you do not revalidate your account, Helpdesk will Deactivate your account. To Re-Validate:
CLICK HERE
IT Support

Click Results

If an end user falls victim to an email assessment, you have two general options:

- Error message/no feedback (Good for a baseline)
- Immediate feedback that explains this was a test, what they did wrong and how to protect themselves (Good for reinforcing key behaviors)

This was a test

You just fell victim to a phishing assessment. Our security team sent an email to all staff pretending to be a hacker, the email you just clicked on was part of that test. You and your computer is fine, however if this had been a real attack your computer would have most likely been compromised. A couple of points to keep in mind.

1. There is little risk in opening and reading email. However, opening attachments or clicking on links can be dangerous. If an email seems strange or suspicious, simply delete it. If you are not sure if an email is an attack, forward it to the security team.

2. The email was extremely generic in nature. Notice how it does not have your name but uses the introduction "Dear Customer" instead. The attack is designed to work against anyone.

3. Notice the poor grammar and spelling mistakes, this is another indicator the email is an attack.

4. Notice how the email comes from a @hotmail.com account, your bank would never use such an email address.

Follow-up

- Send results of test to all employees 24 – 48 hours later
- Explain results, how they could have detected phishing email and what to look for in the future. Include image of phishing email
- Include your monthly security awareness newsletter

Team,

As some of you may have noticed we had our monthly phishing assessment this week. As always the purpose of these assessments is to help you identify and protect yourself against common email based attacks. I've attached at the bottom of this email a screenshot of the scam that went out. If this had been a real attack, simply clicking on the attachment could have infected your computer. There were some very simple ways to determine that this was a scam.

1. The email was extremely generic in nature. Notice how it does not have your name but uses the introduction "Dear Customer" instead. The attack is designed to work against anyone. If your bank had sent you an email it would have used your name.

2. Notice the poor grammar and misspellings, this is another indicator the email is an attack.

3. Notice how the email comes from a @hotmail.com account, your bank would never use such an email address.

As for the assessment, only 13 people fell victim. Great job folks. Finally, be sure to download this month's security awareness newsletter "Social Engineering" from our internal company portal. As always, if you have any questions (or suggestions) about security please contact the help desk.

Thanks!

Violations

- First violation: employee is notified and given additional or follow-up training
- Second violation: employee is notified and manager is copied
- Third violation: manager is required to have meeting with employee and report results to security
- Fourth violation: employee reported to HR

The Impact

- First phish: 30-60% fall victim
- 6-12 months later: Low as 5%
- The more often the assessments, the more effective the impact:
  - Quarterly: 19%
  - Every other month: 12%
  - Monthly: 05%
- Over time, you will most likely have to increase difficulty of tests

Human Sensors

- Another valuable metric is how many reported the attack
- At some point, may need to develop a policy on what to report. One example:
  - 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

Summary

Phishing assessments are a powerful and simple way to measure (and reinforce) behavior change

www.securingthehuman.org/phishing

Free Resources

- Awareness Roadmap & Planning Kit
- Monthly OUCH! newsletter
- Awareness video of the month
- Awareness presentations & posters
- Free trial of full awareness library

www.securingthehuman.org/resources

www.sans.org/mgt433

DON'T GET HOOKED!

SANS SECURING THE HUMAN PHISHING

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 almost any message-based attack. These attacks begin with a cyber 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 they 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.

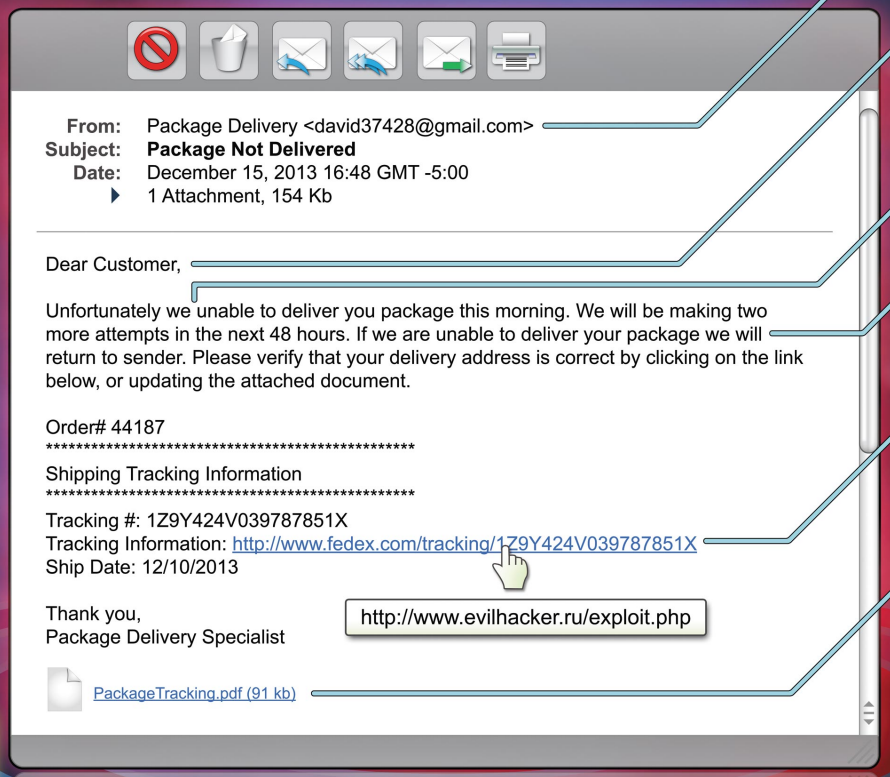
WHAT IS SPEAR PHISHING?

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.

This poster was developed as a community project. Contributors include: Cheryl Conley (Lockheed Martin), Tim Harwood (BP), Tonia Dudley (Honeywell), Ellen Powers (MITRE Corporation), Shanah Johnson (Reserve Bank of Atlanta) and Terri Chihota.

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 anything 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 to demo the SANS Securing The Human phishing testing platform, please visit http://www.securingthehuman.org/phishing.



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 @gmail.com or @hotmail.com, this is most likely an attack. Also, check the "TO" and "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" or that use some other generic salutation. If a trusted organization has a need to contact you, they should know your name and information. Also 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 "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 then 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.