THE SECURITY STANDARD™

Securing the Enterprise from a Dangerous Cyberworld

September 19-20, 2011 • Marriott Brooklyn Bridge, New York City

Produced by
CSO

Next-Gen Security Awareness: Educating the Spectrum -- from Digital Natives through Baby Boomers

Lee Parrish

CISO

Parsons

Lee Parrish – VP & CISO, Parsons Corp

Parsons, celebrating more than 65 years of growth in the engineering and construction industry, is a leader in many diversified markets with a focus on infrastructure, environmental, and defense/security. Parsons delivers design/design-build, program and construction management, professional services, and innovative alternative delivery solutions to federal, regional, and local government agencies worldwide, as well as to private industrial customers. For more about Parsons, please visit www.parsons.com.

The Evolution of Threats and Their Defenses

1. Malware	a. Anti-Virus (signature/behavioral)
2. Perimeter Attacks	a. Firewalls (packet filter/stateful/app)
	b. Intrusion Detection/Prevention
3. Data Destruction/Alteration/Loss	a. Encryption
	b. DLP
4. Social Engineering	a. New hire and annual training
	b. Job-specific training
	c. **Next Gen Awareness & Training**

Cerebral Configuration

- Training & awareness is a human issue, dealing with how people learn and retain information.
  - Repetition (annual vs. frequent)
  - Generational & role aspects to how we learn
  - Relevancy
  - Common theme
  - Changing behavior

Historical Model of Awareness

- New-hire training
- Annual refresher training
- InfoSec awareness posters
- Security trinkets
  - “What is the awareness ROI of a stress ball?”
- Policy
  - We expect employees to not open unsolicited attachments or click on links.

"People respect what you inspect, and not what you expect."

- Lou Gerstner (former CEO, IBM)

INTERNAL PHISHING CAMPAIGNS

Phishing Your Own Employees

- People tend to view the micro (individual) view rather than the macro (community) view.
- Increases awareness in a very personal way
  - Touching the stove rather than being told the stove is hot
- Occurs all within the safety of your own security program
  - No data was harmed in the exercise

Building the Program

- Build or Buy?
- Start small
- Target high value roles
  - Administrative Assistants
  - Finance
  - Public/Corporate Relations
- Create (or buy) the technical underpinnings

Cutting Bait

- Craft a spoofed email with a link to an internal site
- Use a call to action to entice user interaction
- Start with campaigns that are fairly easy (not simple) for the employee to catch
- Progress with added complexity in each campaign

The Lesson

- On the internal site:
  - – Explain to the user what just happened
  - – Visualize for them how they could have picked up it was a phishing email – be specific
  - – Thank them for helping to secure the network
- Overall, user feedback is positive

Catch & Release

- Capture actionable metrics that highlight:
  - # of users in the campaign
  - # of users who opened the email
  - # of users who clicked on the link
  - # of users who did not open the email
- Look for trends – are some Business Units more vulnerable than others? How do you address?

SOCIAL MEDIA

Think Before You Tweet

- Create an internal buffer page, activated when a user goes to a social media site
  - One per browser session rather than for each social media site
- Identify:
  - Potential dangers of social media
  - Responsibilities of the user to protect data
  - Links to social media policies (you have them, right?)
  - Click through agreement

Leveraging Social Media

- Use social media as a security awareness tool:
  - – Internal micro blogging tools to distribute security awareness messages
  - – Corporate Facebook and LinkedIn instances to convey public messages (staffing needs, etc.)

EMAIL EXTERNAL TAGGING/STAMPING

Origination Intelligence

- Places a stamp in the subject line that reads “External” for all inbound email from outside the company
- Accomplished through content filtering and transport rules in email solutions through white listing

Email Tag/Stamp

- Another layer of awareness for the user
- If an email requests the user to change network credentials but comes from an external email address – raises a red flag
- Some push-back due to sorting and searching email

Final Thoughts

- Next Generation Awareness is not a substitute for traditional training
  - We still need annual training, role based training, and awareness articles
- These newer types of programs are supplements to the traditional forms of awareness

Thank You!

lee.parrish@parsons.com