SANS Summit

London, GB
July 10, 2015
We would like all of your registration information please...

Spotting them is never this easy.
Why our role is Important!

Who We Are:

• 572 facilities in 500 cities and 50 states
• Internationally, business locations are in 70 nations and territories
• 112,000 Employees
• 30 million emails/day

We never forget who we’re working for™... and neither do the bad guys!

© 2015 Lockheed Martin Corporation
Email testing has Proven to Enhance Cyber Security Posture and Heighten Awareness both at WORK and at HOME!

© 2015 Lockheed Martin Corporation
Email Testing: Strategy & Concept

Corporate Wide Testing

Grade 1
- No Business Relevance
- No Perceived Trust
- Just Above SPAM
- Baseline & Monthly Testing

Grade 2
- Little Business Relevance
- Little Perceived Trust
- Possible Personal Relevance (risk)
- Generic Phishing
- Baseline & Monthly Testing

Grade 3U
- Industry Relevance
- Low – Moderate Trust
- Generic “Industry” Spear Phishing
- Baseline & Monthly Testing

Grade 3T
- Lockheed Martin Specific Relevance
- Lockheed Martin / Org Trust
- Spear Phishing
- Baseline & Monthly Testing

Grade 4
- Program Relevance
- Org / Personal Trust
- Advanced Spear Phishing
- Red / Blue Testing (only)

Program Specific Testing

Business (or Personal) Relevance

Modeled After Real APT Attack Emails Received by Lockheed Martin

© 2015 Lockheed Martin Corporation
Results Achieved at Lockheed Martin

- **Rate of Bad Actions** (employees clicking on links or attachments)

  Overall % improvement = 55.1%

  \[
  = \frac{(2009 \, B/L\% - 2015 \, YTD\%)}{2009 \, B/L}\%
  \]

- **Rate of Good Actions** (employees reporting suspicious emails to CIRT)

  Overall Improvement = 38X

  2015 YTD rate of CIRT Reporting is 38 times higher than it was during the 2009 Baseline test.

UAR = Undesired Action Rate (opening link or attachment)

© 2015 Lockheed Martin Corporation
Structuring Phishing Emails

- Modeled after real APT received by Lockheed
  - Ensure “sender” is not Lockheed Martin employee
  - Confirm invalid external email address

- Consider current events / trending
  - Personal in nature
  - Finance / Health related
  - Shipping (DHL / FedEx without branding)

- Structure training / awareness based on metrics / employee feedback
  - Baseline testing led to laser focus on NEO
  - Current trending leaning towards BEO

- Emails targeted for specific Lockheed Martin audiences
  - Internal conferences / Leader Development Program
  - Utilize historical data (F2F Info Sec course, Threat Briefs)
Progressive Training and Accountability

- **Training**
  - Identifying Red Flags
  - Short video
  - LMS course added to Learning Plan
  - Links to more detailed information

- **Accountability**
  - Employee notification
  - Leader engagement
  - Talking points / Takeaways

Progressive Training and Accountability Drives the Message Home!
You were notified last month that your employee, John Doe, had taken an undesired action on two consecutive e-mail tests. They were recently tested again and took another undesired action. You are now required to conduct a one-on-one discussion with this employee within one week to review this issue and confirm the completion of that discussion with a reply to this message.
I realize I have been targeted for suspicious e-mails and I have completed the course E-mail Awareness for Targeted Employees. I think this course was probably the most meaningful and valuable training I have received since working here. My awareness of suspicious e-mail messages has been improved with the content of this course.

Sent: Monday, June 23, 2014 2:02 PM
To: CIRT (RESOURCE)
Subject: RE: EXTERNAL: Action Required: Upgrade to Latest Acrobat Reader for Windows

CIRT,

I would just like to let you know that the awareness that LM has brought to the fraud e-mail has personally saved me $250. I received an fraudulent PayPal e-mail to my personal account that I would have fell for if it wasn’t for LMs awareness program. Please let your entire team know that I thank them for their efforts.

Thank you and have a great day,
Lessons Learned

• Think strategically how you will move forward
  - What is your “end state”
  - Consider Location/Role/Title/Level/Generation/Representation
  - Reporting process/staffing
  - Provide detailed educational material, FAQ’s and reporting process
  - Technology/Tool Mods (External Label, MS Labeling)

• Set the expectations – All Employee Memos
  - We will begin testing
  - We will start periodically testing
  - And support an accountability process “taking testing to the next level”
  - Imperative for future justification to employees who question the effort

• Process in place to handle Replies and Forwards

• Content/topic Consideration - Weather/Plant closings/Resumes/Health
When it Comes to Changing Culture…

What are our Challenges?
- Emerging technologies
- Process execution
- Acceptable level of risk

Next Steps to Address
- Researching alternative testing methodologies
- Role-based training based on level of risk
- Diverse training opportunities (e.g. interactive LMS)
- Continue strategizing with enterprise stakeholders
- Awareness Tools viewed on mobile devices (e.g. iBooks)
High Level Process Improvements

JIT Pages
- STOP on the JIT page
- Simplify the message
- “protecting Yourself and …”
- 

Email Notifications
- “Confirmation Required” from Employee
- Added generic 6 minute voice over
- Email to the manager/leader
  - “Action Required”
  - Discussion with the Employee w/response
  - Provide talking points / teachable moments
- Pilot Activity to reduce Repeats – May 2015
- Recognizing positive actions reinforces good behavior

Thanks Debbie! This is a really cool concept. It’s nice to be acknowledged for demonstrating awareness and resulting actions related to receiving unusual email communications. Please let your management know how meaningful this is to me (and others, I’m sure).
Discussion?

#SecAwareSummit

© 2015 Lockheed Martin Corporation