Is security awareness a waste of time?

New York State Cyber Security Conference
June 5, 2013

Scott Gréaux
Vice President Product Management and Services, PhishMe, Inc.
“They are exploiting human vulnerabilities and human trust”

- “100% of all APT style attacks have been root cause of humans” – Brian Honan, Leader Ireland CSIRT quoting Mandiant
- “If you're being attacked by an intelligent human, your most useful defense is to also be an intelligent human.” – Bruce Schneier
- “The Ultimate Defense Against Advanced Persistent Threats ... [people]” – Jason Rader, RSA
- "Security is not a technology issue – it’s a people issue" – Steve Mansfield-Devine, ContraRISK
I used to promote this

- Security awareness week
- Common materials/theme
- Infosecurity.ge.com
- Various business programs with localized themes and content

Pre 2007

- Security Awareness week
- Common materials/theme
- Infosecurity.ge.com
- Various business programs with localized themes and content

2007

- Security Awareness week
- Common materials/theme
- Infosecurity.ge.com
- AUG
- Common materials
- Intranet articles
- Toolkit
- Working group
- 1st Larry animation
- Limited business participation in global theme

2009

- Security Awareness week
- Common materials/theme
- Infosecurity.ge.com
- I'm Aware theme
- Translations 22 languages
- Common materials
- Intranet articles
- Toolkit
- New posters
- Physical security integration
- Two new Larry animations
- Most businesses participate in common theme
- Security Awareness quiz

2010

- Security Awareness week
- Common materials/theme
- Infosecurity.ge.com
- Article classification; informational, behavioral change
- Formal measurement system
- Working group growth
- New content
- New posters
- Business awareness program plans
- Industry participation
- Template refresh
- Quarterly business "awareness" events
- In-line training expansion
- Executive training
- Full population phishing simulations
- Advanced threat briefings
More Is Not Better
2010 – 2013: what changed?

What I said in 2010

<table>
<thead>
<tr>
<th>Month</th>
<th>Article</th>
<th>Type</th>
<th>How I feel today</th>
</tr>
</thead>
<tbody>
<tr>
<td>February</td>
<td>File sharing applications</td>
<td>Informational</td>
<td>Get application control</td>
</tr>
<tr>
<td>March</td>
<td>Emergency contact information</td>
<td>Behavioral change</td>
<td>Wrong communication mode</td>
</tr>
<tr>
<td>April</td>
<td>Portable devices &amp; removable media</td>
<td>Behavioral change</td>
<td>GPO</td>
</tr>
<tr>
<td>May</td>
<td>Concern and incident reporting</td>
<td>Behavioral change</td>
<td>Hey, this is still valid!</td>
</tr>
<tr>
<td>June</td>
<td>Creating a strong password</td>
<td>Informational</td>
<td>Really?</td>
</tr>
<tr>
<td>July</td>
<td>Travel security</td>
<td>informational</td>
<td>What does this even mean?</td>
</tr>
<tr>
<td>August</td>
<td>Managing your online presence</td>
<td>Informational</td>
<td>DLP, proxy in the cloud</td>
</tr>
<tr>
<td>September</td>
<td>Workplace violence</td>
<td>Behavioral change</td>
<td>Wrong competency</td>
</tr>
<tr>
<td>November</td>
<td>Phishing</td>
<td>Behavioral change</td>
<td>Responsible for 91% of breaches</td>
</tr>
<tr>
<td>December</td>
<td>Wireless security</td>
<td>Informational</td>
<td>Personal engagement, I like it</td>
</tr>
</tbody>
</table>

I’ve learned that consumers of organizational IT services need to know two things
• What to look out for (phishing)
• How to report (even if they were susceptible)
Technology addresses most risks

1. Click **Start**, and then click **Run**.
2. In the **Open** box, type **regedit**, and then click **OK**.
3. Locate and then click the following registry key:
   
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\UsbStor

4. In the details pane, double-click **Start**.
5. In the **Value data** box, type 4, click **Hexadecimal** (if it is not already selected), and then click **OK**.
6. Exit Registry Editor.
There is one attack vector..
So what does all that mean?

• Awareness should be focused and targeted
• Behavioral change should be measurable
• Topics must be relevant (and up to date)
• Good awareness works, bad awareness confuses
HOW TO CHANGE BEHAVIOR

Understand your human risks
When to educate
What to measure
2012 Year in review

• 243 median number of days that attackers were present on a victim network before detection (M-Trends)
• 66% of breaches went undetected for months or more (DBIR)
• 63% of breaches are reported by third parties (M-Trends)
• Approx 70% of breaches were discovered by external parties (DBIR)
• Average cost of a data breach $5.5MM (Symantec/Ponemon)
• The attackers are targeting people, not computer systems. (Kevin Mandia)
Control cost by incident phase

- Compromise
- Exfiltration
- Propagation
- Persistence

With a thriving user reporting ecosystem
Spear phishing trends

• Sports and other local interest themes
• 200+ users targeted per attack
• Decline in attachments (still a risk but being used less)
• Click-only is the most popular spear phishing tactic
• Data entry (no malware, just ask for credentials)
• M&A data is valuable – threats establish their foothold in the acquisition target prior to the deal and wait
• Emails are short, similar to the email that got RSA
• Emails do not impersonate commercial enterprises (such as LinkedIn, Twitter, etc.)
Timing is everything

Immediate and actionable feedback
Relevant so it sticks
Measurable
Measure everything

<table>
<thead>
<tr>
<th>Operational Area</th>
<th>Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing reports</td>
<td>Number of known suspicious emails (sum of all identification methods)</td>
</tr>
<tr>
<td>Phishing reports</td>
<td>Number of suspicious emails reported by email users</td>
</tr>
<tr>
<td>Phishing reports</td>
<td>Net number of suspicious emails reported by users (count of reported emails that were actual phishing emails)</td>
</tr>
<tr>
<td>Phishing incidents</td>
<td>Number of incidents caused by phishing</td>
</tr>
<tr>
<td>Phishing incidents</td>
<td>Percentage of incidents that originate from phishing attacks</td>
</tr>
<tr>
<td>Phishing incidents</td>
<td>Number of user reported phishing incidents</td>
</tr>
<tr>
<td>Phishing incidents</td>
<td>Number of technical control detected phishing incidents</td>
</tr>
<tr>
<td>Phishing incidents</td>
<td>Percentage of user reported phishing incidents</td>
</tr>
<tr>
<td>Phishing response</td>
<td>Time from incident to report</td>
</tr>
<tr>
<td>Phishing response</td>
<td>Time from incident to detection</td>
</tr>
<tr>
<td>Phishing response</td>
<td>Time from incident report to containment</td>
</tr>
<tr>
<td>Phishing response</td>
<td>Time from incident detection to containment</td>
</tr>
</tbody>
</table>

Workforce learned desired behavior
Trend ID’d with specific attack type
Implemented remediation and maintenance plans

Measuring behavior change will help fine tune your program, show success and ID trends
Increase engagement

• IT consumers are part of the solution
• Reinforce a culture of situational awareness
• Repurpose success in other awareness efforts
• Solicit input and feedback
BENEFITS

Threat intelligence
Increase engagement and awareness
Leverage existing processes and people
The value of information

“One of the most valuable resources in detecting and responding to cyber-attacks is accurate and timely threat intelligence.”

*Kevin Mandia, CEO Mandiant, to Select Committee on Intelligence, February 14, 2013*
Human sensors

“Once again, end users represent the most effective means of detecting a breach internally”

Verizon 2012 Data Breach Investigation Report

What can we ask of email users?

• Report suspicious emails, all of them
• Avoid being compromised
• If you think you are a victim of phishing, report it
Timeline of phishing attacks

Most people respond to emails within the first few hours of receiving them – if they are trained to report we get relevant, near time threat intel.

Users who learn to not fall for phishing attacks also learn to report them.
Improve Email Communications

• Inconsistent email messaging goes away
• Phishy looking communications morph into a standard way of delivering mass business related emails.
Improved Technical Defenses

Defenses get reviewed and improved

- Reject spoofed emails from the internet
- SPF
- DLP
- Role based web access filters
- Sandboxing
Tap into existing IR framework
Improve incident response

• Users provide near-time threat data
• Response can start day 1
  – Redirect and capture C&C traffic
  – Remove same/similar emails from other inboxes
  – Block additional inbound/outbound
  – Increase monitoring at targeted entities
  – If a successful compromise containment may be limited