

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

Pre 2007

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

2008

- Security Awareness
- Common materials
- Security awareness
- AU
- Common
- Intranet
- Toolkits
- Working group
- 1st Latin
- Limited participation

2009

- Intranet
- Re-use
- Security pilot
- New posters
- Physical security integration
- Updated Information Security training course
- All planning
- Business Security
- Business Week project

2010

- Article on information 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

More Is Not Better



2010 – 2013: what changed?

What I said in 2010

Month	Article	Type
February	File sharing applications	Informational
March	Emergency contact information	Behavioral change
April	Portable devices & removable media	Behavioral change
May	Concern and incident reporting	Behavioral change
June	Creating a strong password	Informational
July	Travel security	informational
August	Managing your online presence	Informational
September	Workplace violence	Behavioral change
November	Phishing	Behavioral change
December	Wireless security	Informational

How I feel today

2013

Get application control

Wrong communication mode

GPO

Hey, this is still valid!

Really?

What does this even mean?

DLP, proxy in the cloud

Wrong competency

Responsible for 91% of breaches

Personal engagement, I like it

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

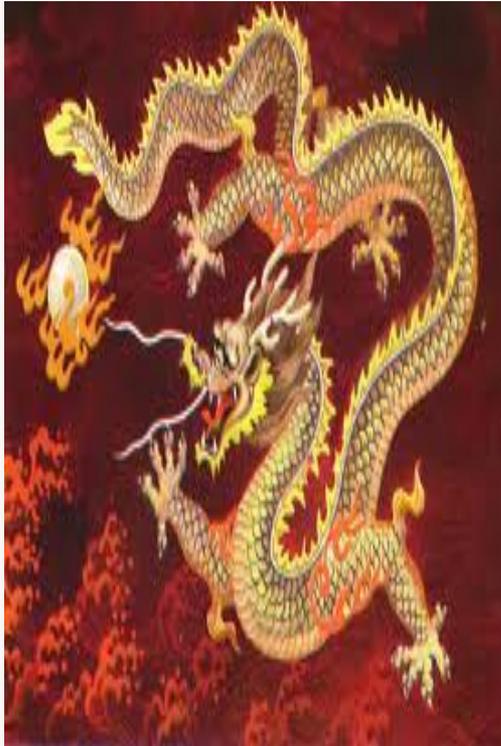
1. Click **Start**, and then click **Run**.
2. In the **Open** box, type **regedit**, and then click **OK**.
3. Locate and then click the following registry key:

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..



91% of cyberattacks begin with spear phishing email

Spear phishing makes use of information about a target to make attacks more specific and 'personal'

By Antony Savvas | [Computerworld UK](#) | Published: 15:21, 28 November 2012

+1 4 Like 20 Tweet 30

Some 91% of cyberattacks begin with a "spear phishing" email, according to research from security software firm Trend Micro.

Spear phishing is an increasingly common form of phishing that



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

Understand your human risks

When to educate

What to measure

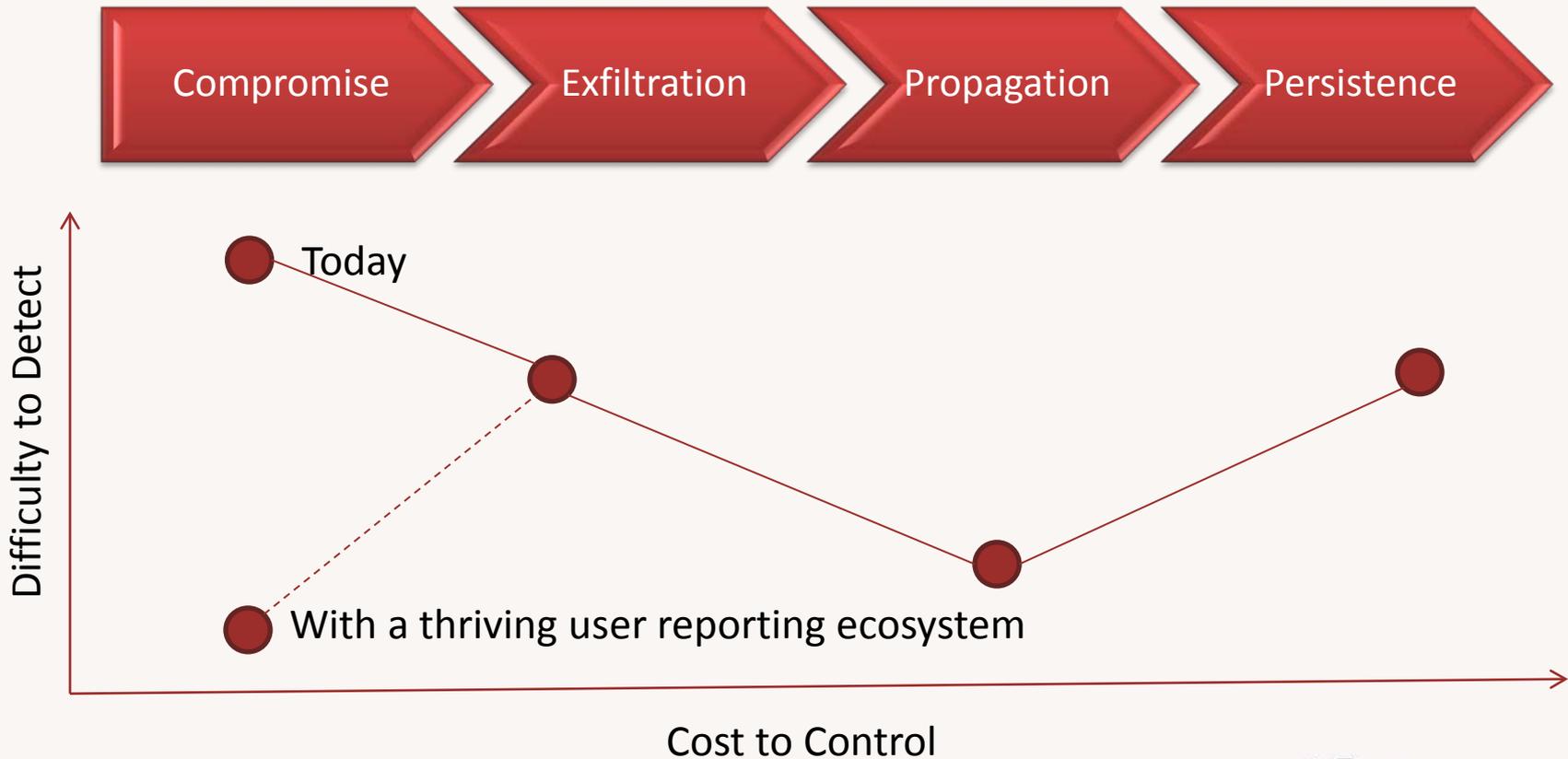
HOW TO CHANGE BEHAVIOR



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



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.)

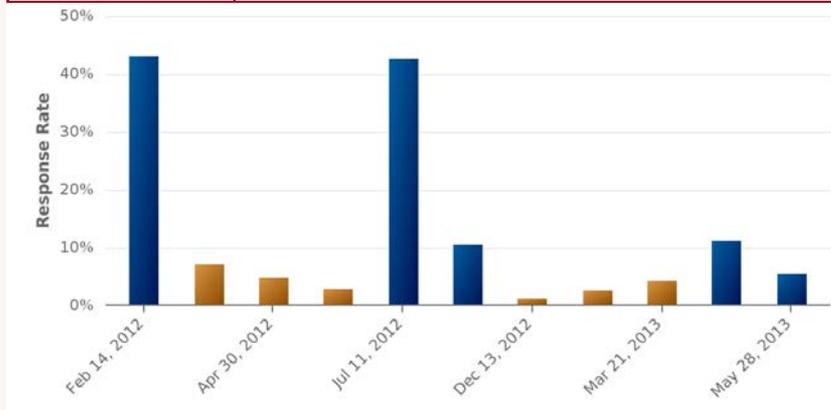
Timing is everything



Immediate and actionable feedback
Relevant so it sticks
Measurable

Measure everything

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



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

Threat intelligence

Increase engagement and awareness

Leverage existing processes and people

BENEFITS



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



U.S. Senate Select Committee on
INTELLIGENCE

Human sensors

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

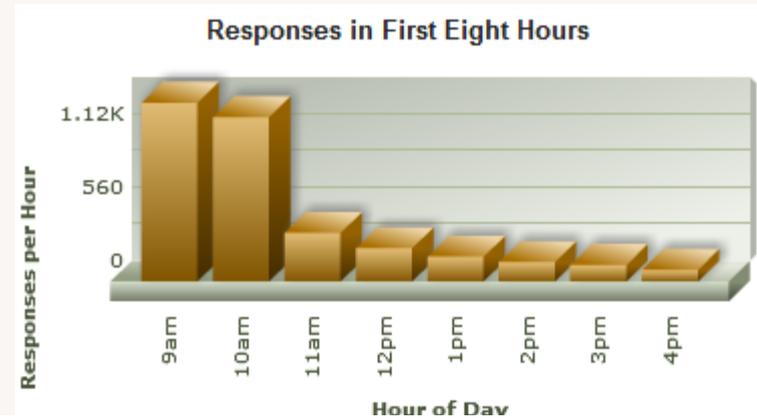
Verizon 2012 Data Breach Investigation Report

What can we ask of email users?

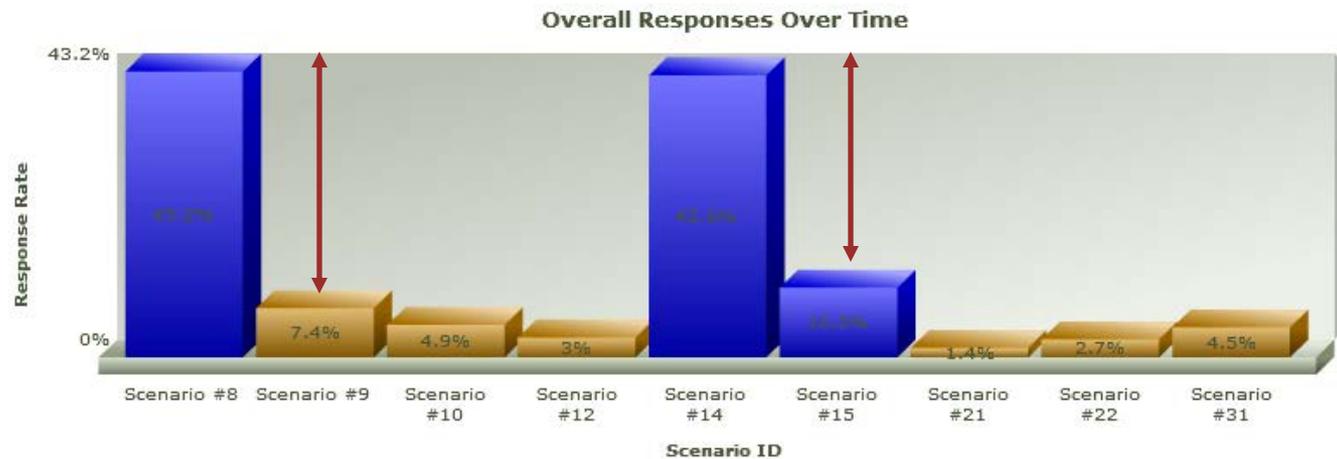
- Report suspicious emails, all of them
- Avoid being compromised
- If you think you are a victim of phishing, report it

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

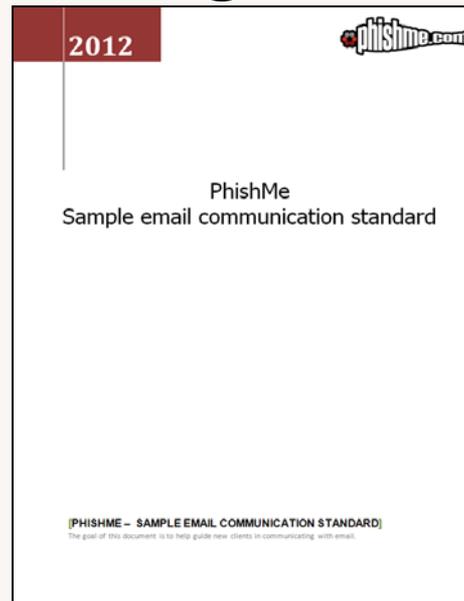


Users who learn to not fall for phishing attacks also learn to report them



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

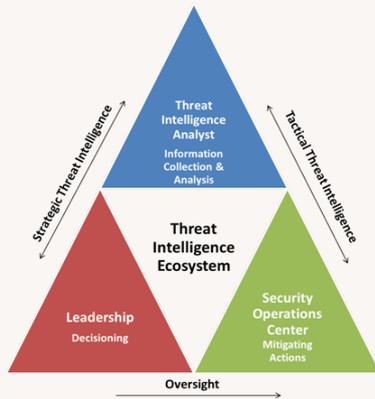
Defenses get reviewed and improved

- Reject spoofed emails from the internet
- SPF
- DLP
- Role based web access filters
- Sandboxing

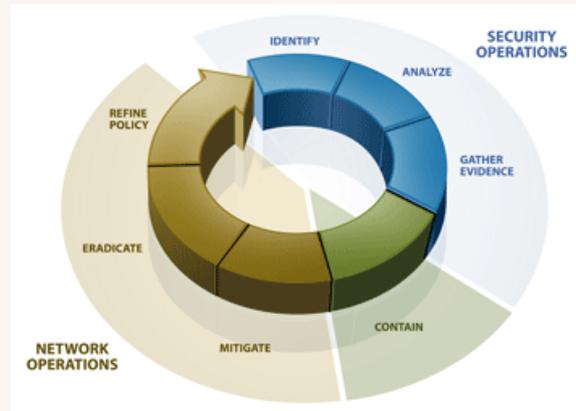


INCIDENT RESPONSE

Tap into existing IR framework



People



Process



Technology

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