Turning Your Employees into Human Firewalls

Elevating Your Cybersecurity

Jason Stefanski

Director of Information Technology | GeoEngineers, Inc.

GBA GEOPROFESSIONAL BUSINESS ASSOCIATION

Outline

- Cybersecurity: Definitions & Data Points
- Technology Tools
- Digging in: Social Engineering & Phishing
- The Costs of Inaction
- What to do? Going beyond technology
- Our story
- Recap
- Q&A

GBA GEOPROFESSIONAL BUSINESS ASSOCIATION

Cybersecurity - Definition

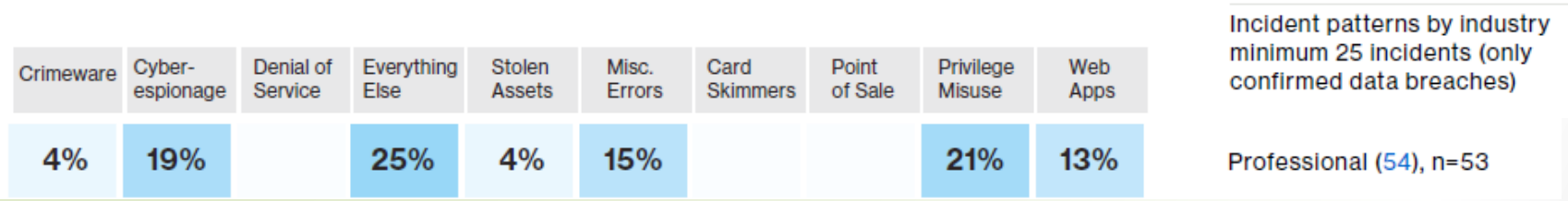
The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this

GBA GEOPROFESSIONAL BUSINESS ASSOCIATION

verizon

2016 Data Breach Investigations Report

89% of breaches had a financial or espionage motive.



Crimeware	Cyber-espionage	Denial of Service	Everything Else	Stolen Assets	Misc. Errors	Card Skimmers	Point of Sale	Privilege Misuse	Web Apps
4%	19%		25%	4%	15%			21%	13%

Incident patterns by industry minimum 25 incidents (only confirmed data breaches)

Professional (54), n=53

54 Professional, Scientific, and Technical Services[T]

Sources:

[1]2016 Verizon Data Breach Investigations Report

[T]2012 NAICS Definition

GEOPROFESSIONAL BUSINESS ASSOCIATION

Cybersecurity
Standard Technology Tools

- Antivirus/Antimalware/Antispam
- Firewalls
- IDS/IPS (Intrusion Detection/Prevention)
- Patching (Microsoft & 3rd party)
- Backups (and testing them!)

- Bonus points:
  - Security information & event management (SIEM)

GBA GEOPROFESSIONAL BUSINESS ASSOCIATION

“Amateurs hack systems, professionals hack people.”

- Bruce Schneier

American cryptographer, computer security and privacy specialist, and writer

GBA GEOPROFESSIONAL BUSINESS ASSOCIATION

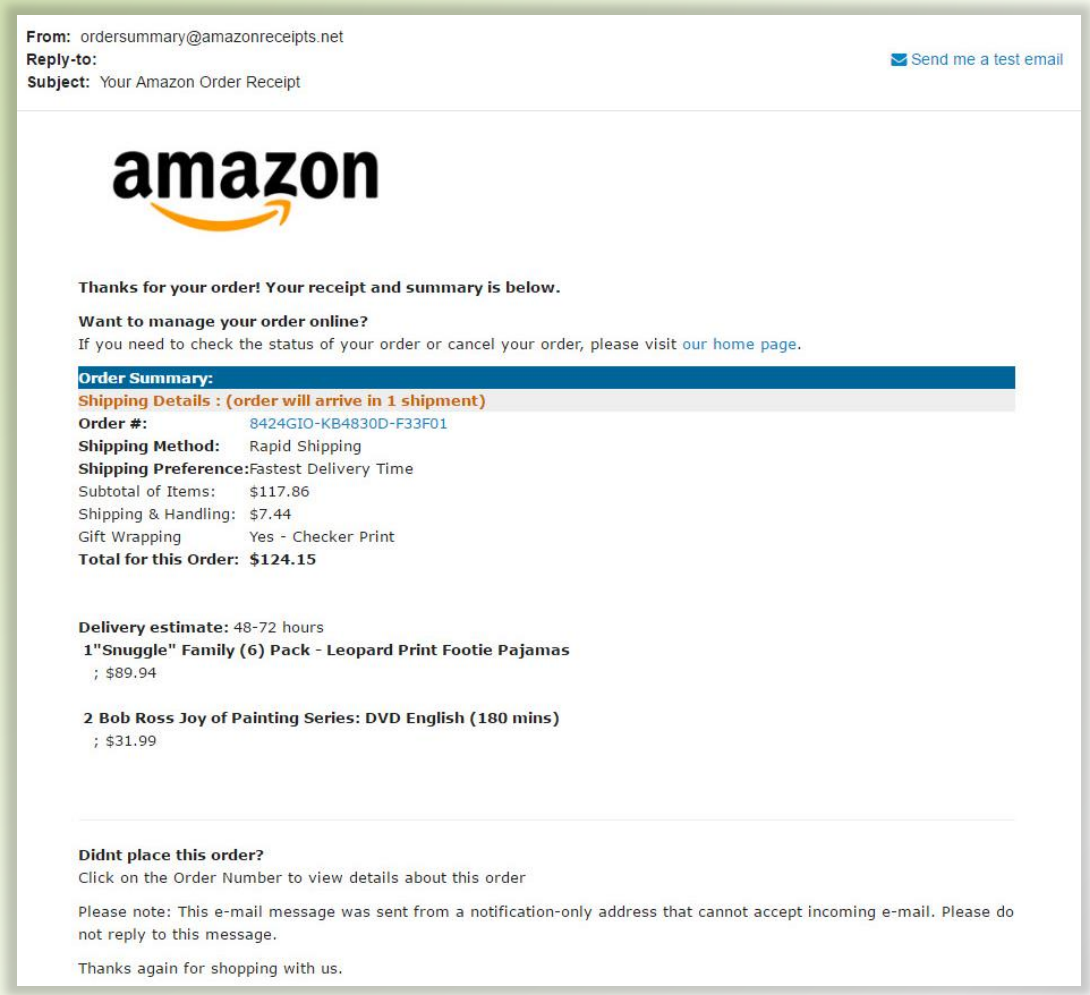
Social Engineering

Psychological manipulation of people into performing actions or divulging confidential information.

- Baiting
- Tailgating
- Phishing / Whaling

GBA GEOPROFESSIONAL BUSINESS ASSOCIATION

Sample Phishing Email



From: ordersummary@amazonreceipts.net
Reply-to:
Subject: Your Amazon Order Receipt

Send me a test email

amazon

Thanks for your order! Your receipt and summary is below.

Want to manage your order online?
If you need to check the status of your order or cancel your order, please visit our home page.

Order Summary:
Shipping Details : (order will arrive in 1 shipment)

Order #:	8424GIO-KB4830D-F33F01
Shipping Method:	Rapid Shipping
Shipping Preference:	Fastest Delivery Time
Subtotal of Items:	$117.86
Shipping & Handling:	$7.44
Gift Wrapping	Yes - Checker Print
Total for this Order:	**$124.15**

Delivery estimate: 48-72 hours
1"Snuggle" Family (6) Pack - Leopard Print Footie Pajamas
; $89.94

2 Bob Ross Joy of Painting Series: DVD English (180 mins)
; $31.99

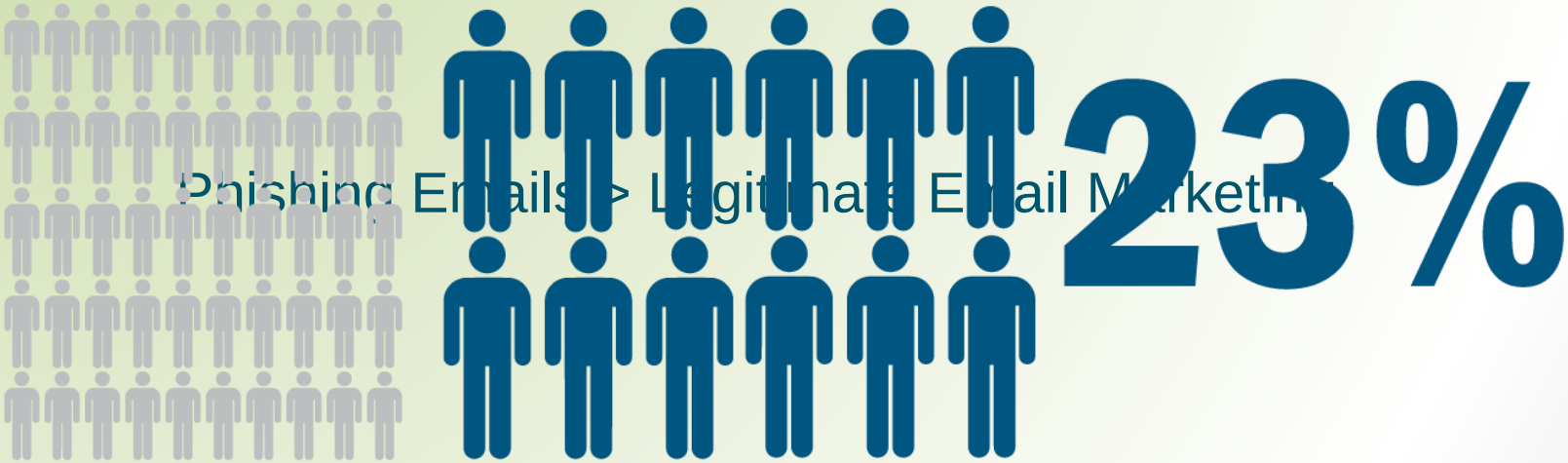
Didnt place this order?
Click on the Order Number to view details about this order

Please note: This e-mail message was sent from a notification-only address that cannot accept incoming e-mail. Please do not reply to this message.

Thanks again for shopping with us.

GBA GEOPROFESSIONAL BUSINESS ASSOCIATION

Shooting Phish in a Barrel



Phishing Emails > Legitimate Email Marketing

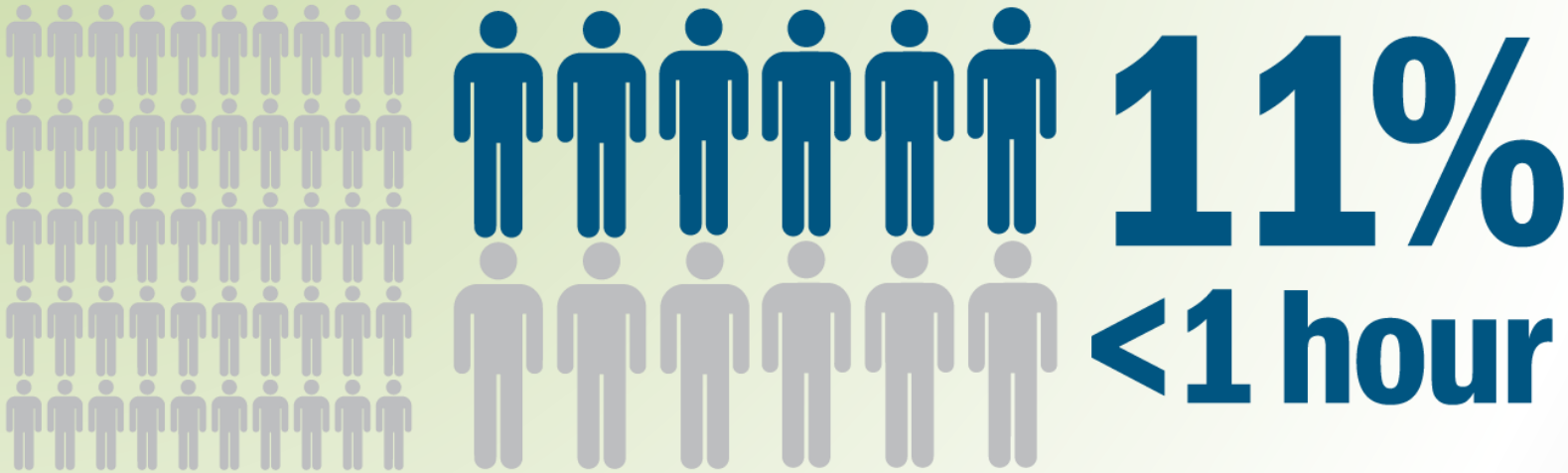
Sources:

[2] *Calyptix Security Blog*

[3] *2015 Verizon Data Breach Investigations Report (DBIR)*

GEOPROFESSIONAL BUSINESS ASSOCIATION

Shooting Phish in a Barrel

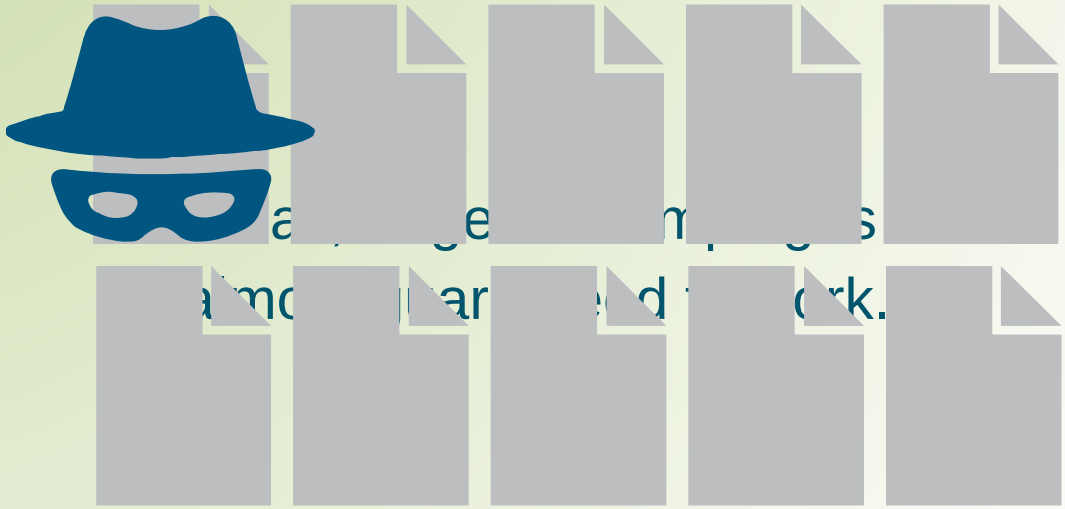


Sources:

[2] *Calyptix Security Blog*

[3] *2015 Verizon Data Breach Investigations Report (DBIR)*

GBA GEOPROFESSIONAL BUSINESS ASSOCIATION



Sources:

[2] *Calyptix Security Blog*

[3] *2015 Verizon Data Breach Investigations Report (DBIR)*

GEOPROFESSIONAL BUSINESS ASSOCIATION

Cybersecurity - Beyond Technology

So. . .why haven't user education and behavior training been used?

- "Scared" of the results or don't think there's a problem
- Don't think it will work or help
- People won't do it or will forget their training
- "Costs" too much (non-billable time)

GBA GEOPROFESSIONAL BUSINESS ASSOCIATION

Cost of Inaction (Expense/Internal)

- The average large company (1,000+ employees) spends $3.7M/year dealing with phishing attacks[4]
    1. Productivity losses ($1.8M)
    2. Cost of usernames/passwords not contained ($1.0M)
    3. Cost to contain usernames/passwords ($382K)
    4. Cost of malware (viruses) not contained ($338K)
    5. Cost to contain malware (viruses) ($208K)
- Spear phishing incident average cost is $1.6M[5]
- Insurance may not cover you![6]

Sources:

[4] *The Cost of Phishing & Value of Employee Training (Ponemon Institute)*

[5] InfoSecurity Magazine

[6] *Phishing for Insurance Coverage (Lexology)*

GBA GEOPROFESSIONAL BUSINESS ASSOCIATION

Cost of Inaction (Revenue/Clients)

- **Federal clients** requiring compliance with NIST (National Institute of Standards and Technology)
  - Minimum requirements for federal information systems
  - These controls include **Security Awareness Training**.[7]
- GBA's Spring "Crystal Ball" workshop
  - Real-world example: Target breach

Source:

[7] NIST 800-53 Rev 4, AT-2: Security Awareness Training

GEOPROFESSIONAL BUSINESS ASSOCIATION

What to do?

- Technology
  - Block, filter, and alert on phishing emails at the gateway
  - Segment the network
  - Antivirus
  - File server storage – restore, but keep forensic evidence
- Technology + People
  - Improve detection and response capabilities
- PEOPLE
  - Launch an engaging and thorough security awareness program

GBA GEOPROFESSIONAL BUSINESS ASSOCIATION

Security Awareness Program – our story

- Bank fraud - true story!

GEOPROFESSIONAL BUSINESS ASSOCIATION

Bank Fraud

From: Jenny Block <jennyb@gmail.network.com>
Reply-to:
Subject: double charged
statement.doc

Send me a test email

Hi , I am emailing you directly because I haven't received any reply from your Accounting department, regarding my problem. My credit card has been charged twice by geoengineers.com.

Please refund one of the charges. I am attaching my card statement as evidence.

Sincerely,

Jenny Block

GEOPROFESSIONAL BUSINESS ASSOCIATION

Security Awareness Program – our story

- Bank fraud - true story!
- Baseline Testing – how bad is it? (www.knowbe4.com)

GEOPROFESSIONAL BUSINESS ASSOCIATION

Baseline Testing

From: IT@geoengineers.com
Reply-to:
Subject: Change of Password Required Immediately

Send me a test email

We suspect a security breach happened earlier this week. In order to prevent further damage, we need everyone to change their password immediately.

Please click here to do that:

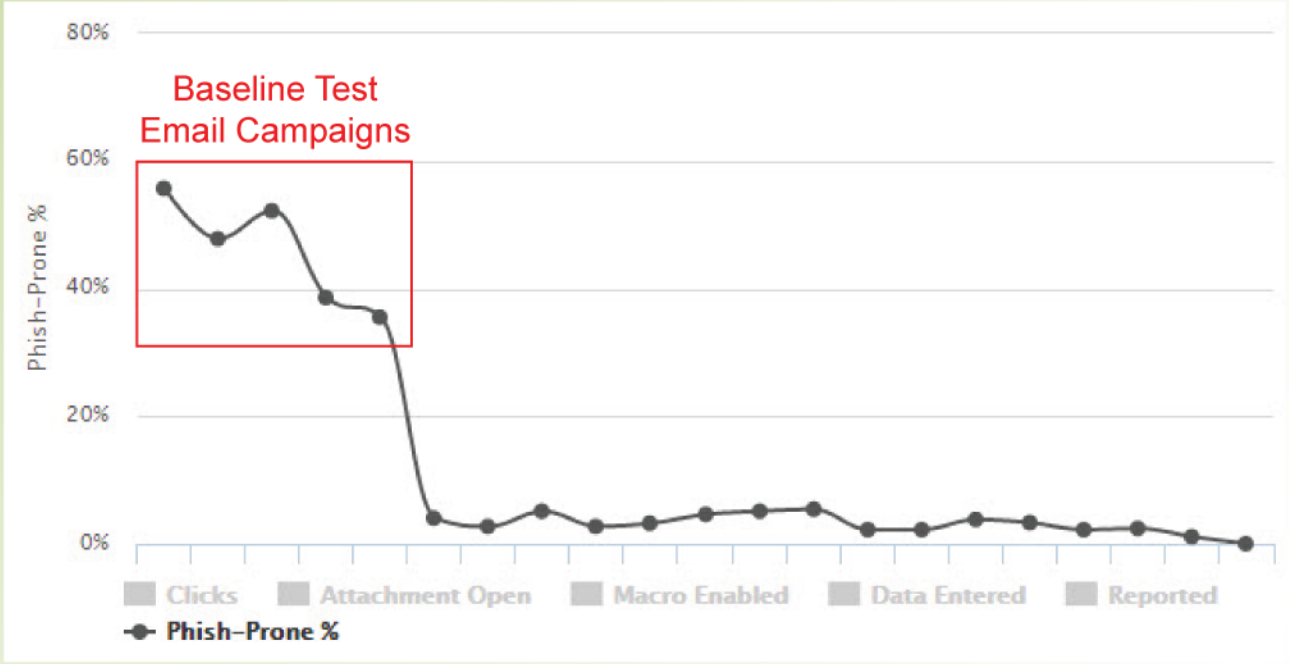
Change Password

Please do this right away. Thanks!

Sincerely,
IT

GBA GEOPROFESSIONAL BUSINESS ASSOCIATION

GeoEngineers' Phishing Click Rates, from the beginning (18 months)



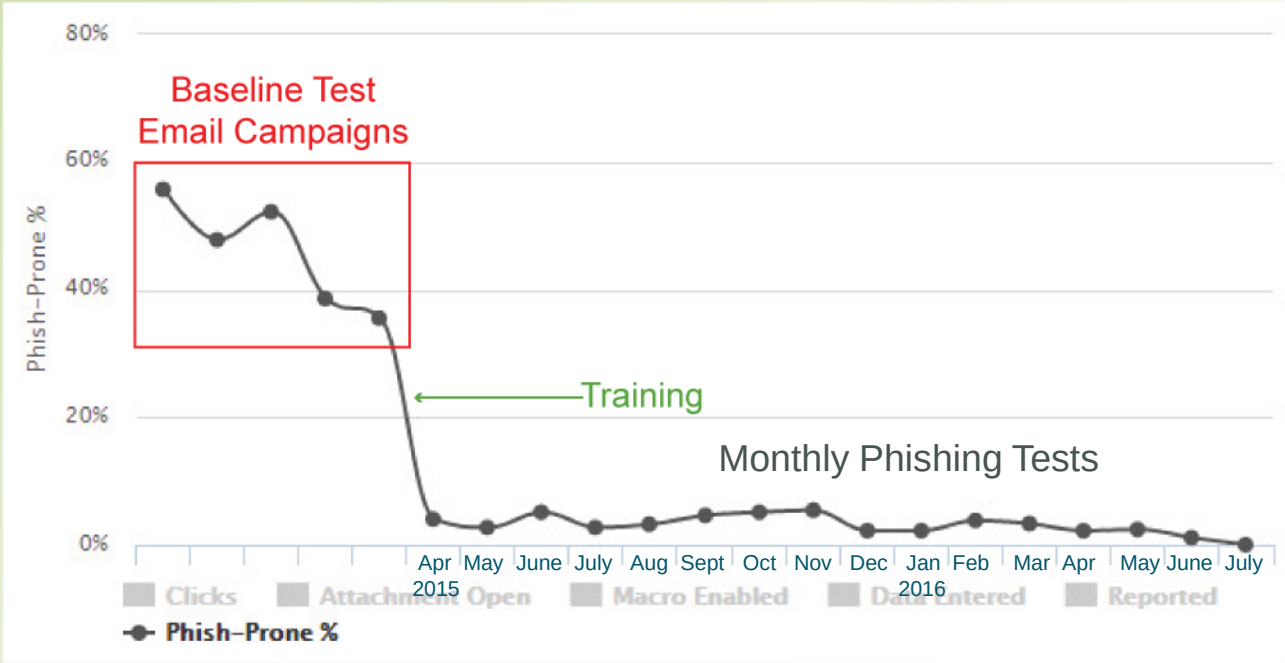
GEOPROFESSIONAL BUSINESS ASSOCIATION

Security Awareness Program – our story

- Bank fraud - true story!
- Baseline Testing – how bad is it? (www.knowbe4.com)
- Annual Training (mandatory 1 hr.)
  - Online video with Kevin Mitnick
  - Real life examples
  - Applicable to work *and* home
- Ongoing monthly tests (“phishing derbies”)
  - Random emails to everyone (different subjects)
  - Tracking metrics

GBA GEOPROFESSIONAL BUSINESS ASSOCIATION

GeoEngineers' Phishing Click Rates, from the beginning (18 months)

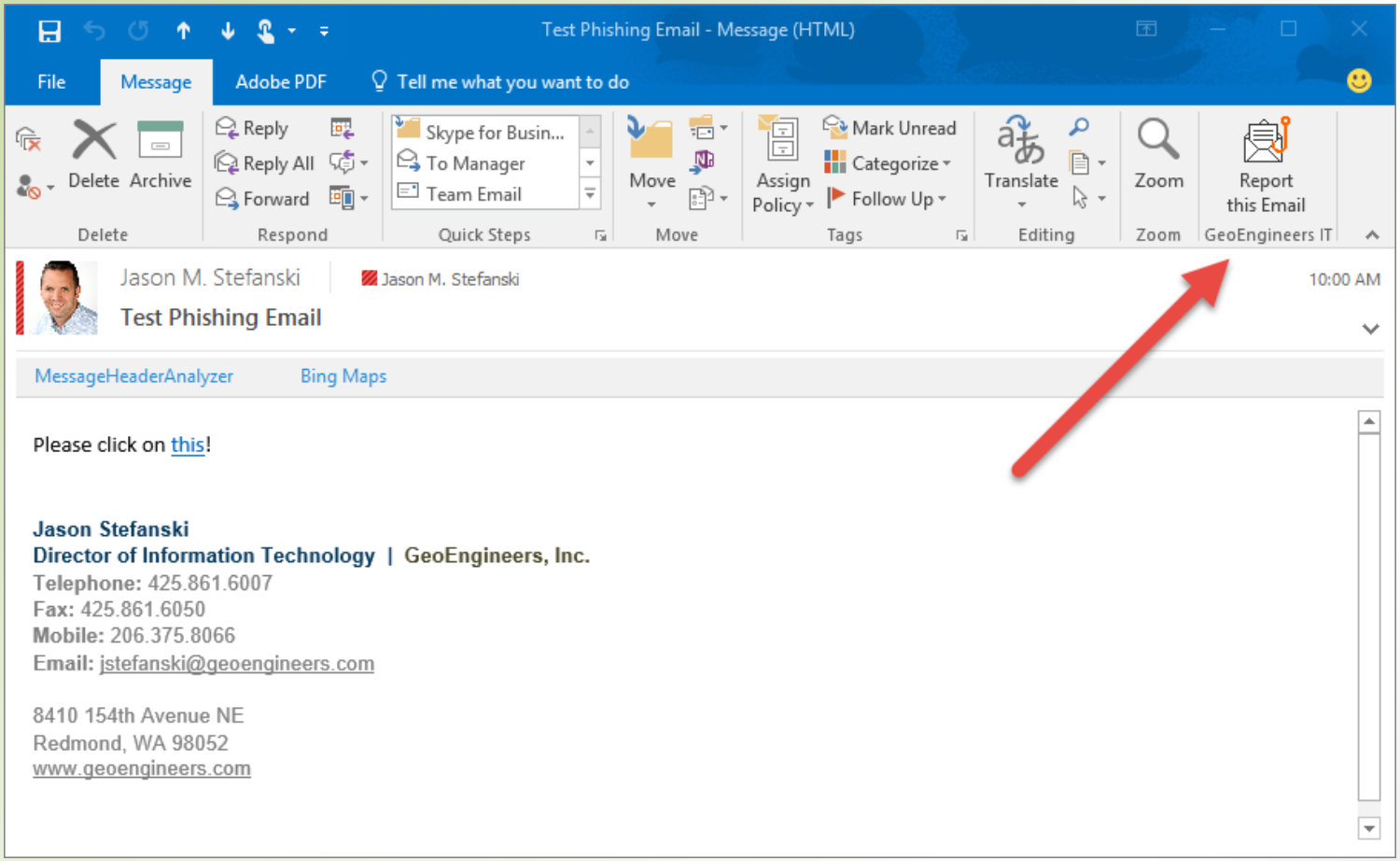


GEOPROFESSIONAL BUSINESS ASSOCIATION

Security Awareness Program – our story

- Bank fraud - true story!
- Baseline Testing – how bad is it? (www.knowbe4.com)
- Annual Training (mandatory 1 hr.)
  - Online video with Kevin Mitnick
  - Real life examples
  - Applicable to work *and* home
- Ongoing monthly tests (“phishing derbies”)
  - Random emails to everyone (different subjects)
  - Tracking metrics
- Reporting suspicious emails to IT
  - Engaging. Employees can do something about it!

GBA GEOPROFESSIONAL BUSINESS ASSOCIATION



GEOPROFESSIONAL BUSINESS ASSOCIATION

Security Awareness Program – our story

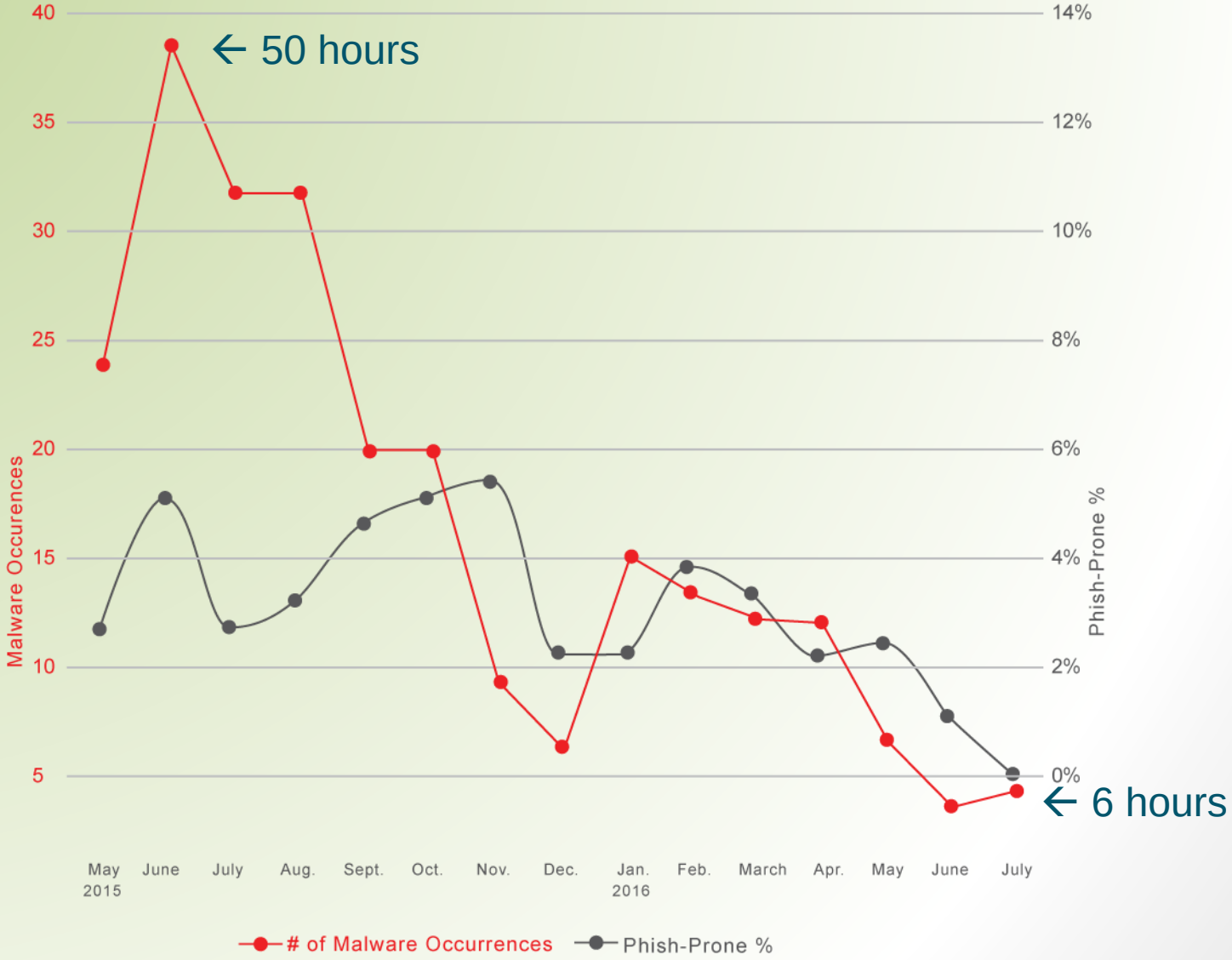
OK, we're done, right?

No. Repeat!

- Annual Training
  - 1 hour vs. 25 minutes
- Ongoing monthly tests ("phishing derbies")
  - Random emails to everyone (different subjects)
  - Tracking metrics
- Reporting suspicious emails to IT

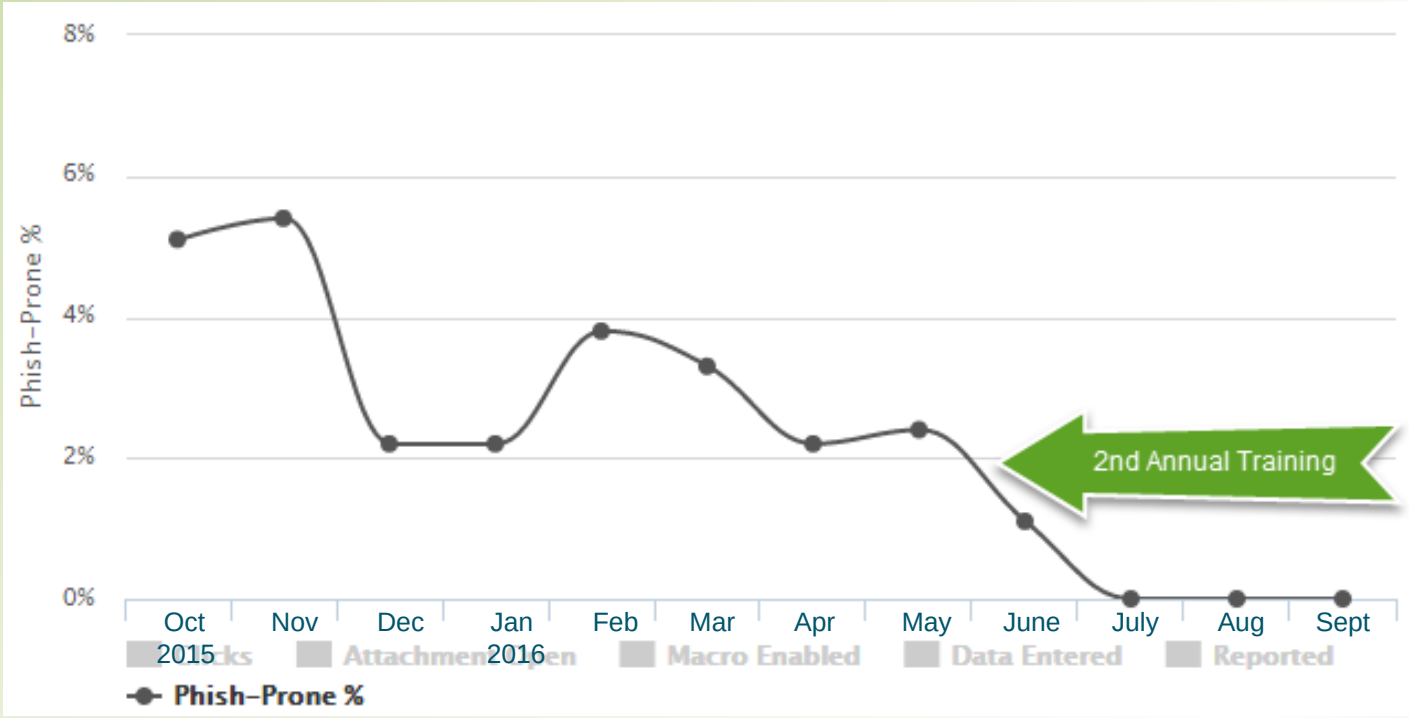
GBA GEOPROFESSIONAL BUSINESS ASSOCIATION

The result? Number of virus infections are WAY down…



GEOPROFESSIONAL BUSINESS ASSOCIATION

GeoEngineers' Phishing Click Rates, last 12 months



GEOPROFESSIONAL BUSINESS ASSOCIATION

Recap

- Technology Tools as a foundation
- Going beyond technology to create your own “human firewall”
  - Baseline testing
  - Cyclical process of…
    - Training
    - Monthly phishing derbies
    - Measure results
    - Provide opportunity for feedback
- Hitting “0” does not end the cycle!
  - We are human. We forget, aren’t consistent, and are not perfect.

GBA GEOPROFESSIONAL BUSINESS ASSOCIATION

Turning Your Employees into Human Firewalls

Elevating Your Cybersecurity

Q&A

Jason Stefanski

Director of Information Technology | GeoEngineers, Inc.

jstefanski@geoengineers.com

GBA GEOPROFESSIONAL BUSINESS ASSOCIATION

Cited Sources

[1] 2016 Verizon Data Breach Investigations Report (DBIR):

- http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf

[T] 2012 NAICS Definition:

- https://www.census.gov/cgi-bin/sssd/naics/naicsrch?chfart_code=54&search=2012%20NAICS%20Search

[2] Calyptix Security Blog:

- http://www.calyptix.com/research-2/verizon-data-breach-report-2015-top-10-charts-and-summary/

[3] 2015 Verizon Data Breach Investigations Report (DBIR):

- http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report_2015_en_xg.pdf

[4] The Cost of Phishing & Value of Employee Training (Ponemon Institute):

- https://info.wombatsecurity.com/hubfs/Ponemon_Institute_Cost_of_Phishing.pdf

[5] InfoSecurity Magazine

- http://www.infosecurity-magazine.com/news/spear-phishing-incident-average/

[6] Phishing for Insurance Coverage (Lexology)

- http://www.lexology.com/library/detail.aspx?g=5a05de35-3a83-4b27-b5bc-cf66076c7049

[7] NIST 800-53 Rev 4, AT-2: Security Awareness Training

- https://web.nvd.nist.gov/view/800-53/Rev4/control?controlName=AT-2

Other Sources

- NIST 800-53 Rev 4 (full standard):
  - http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
- WServerNews, Issue #1,000:
  - http://www.wservernews.com/newsletters/archives/issue-1000-12576.html

GBA GEOPROFESSIONAL BUSINESS ASSOCIATION