Largest Data Breaches

Source: Informationisbeautiful.net

© Copyright 2012-2013 PhishMe, Inc. All rights reserved.
Attacks Begin With Email-based Tactics

IN A SINGLE CAMPAIGN,

135,000 SPEAR PHISHING EMAILS SENT
80 COMPANIES TARGETED
28,000 IP ADDRESSES USED TO SEND EMAILS
20 “LEGITIMATE” WEB SITES HIJACKED TO HOST MALWARE

80 DAYS TO DISCOVER MALICIOUS BREACHES
91 PERCENT OF CYBERATTACKS THAT BEGIN WITH SPEAR PHISHING

$8,900,000 AVERAGE ANNUAL COST OF CYBER CRIME
$222 COST PER COMPROMISED RECORD
3.9X HIGHER COST OF CYBER CRIME IF UNDER PROTECTED

- Massive-scale phishing attacks loom as new threat, USA Today
- Ponemon Institute: 2012 Cost of Cyber Crime Study
- 2012 Verizon Data Breach Investigations Report
- Spear phishing the main email attachment threat, ComputerWorld UK

© Copyright 2012-2013 PhishMe, Inc. All rights reserved.
Evolution of a Phish

Account Information <bankofamerica@yahoo.com>

Warning: This message may not be from whom it claims to be. Beware of following any links in it or of providing the sender with any personal information.

We recently have determined that different computers have logged onto your Online Banking account, and multiple password failures were present before the logons. We now need you to re-confirm your account information to us.

If this is not completed by September 27, 2007, we will be forced to suspend your account indefinitely, as it may have been used for fraudulent purposes. We thank you for your cooperation in this manner.

To confirm your Online Banking record, please visit:
http://0xcb5c3a88/icons/www.bankofamerica

Thank you for your patience in this matter.

Bank of America Customer Service

Please do not reply to this e-mail as this e-mail address is not monitored.

© 2007 Bank of America Corporation

© Copyright 2012-2013 PhishMe, Inc. All rights reserved.
The **USER** is the Vulnerability

From a forensic expert at Verizon Business...

“China is overplayed – still an issue, but not nearly as big an issue as the standard Russian/Romanian organized crime stuff. APT is not real, IMHO. 95% of the “APT” cases we see start with a **Phishing** email. Not advanced at all.

Still the same hype – most media outlets pushing fear, uncertainty and doubt when in truth a little common sense and a modicum of security will prevent most breaches.”
We Need to Change the Way We Defend
Engage Humans in Your Security Program

Tier 1: Traditional Defenses
- Perimeter and network security controls
- Host and endpoint protection

Tier 2: User Awareness & Training
- Simulated phishing exercises, interactive education
- Improve awareness / Change security behavior

Tier 3: User Empowerment
- User attack identification and reporting
- Decrease time to incident detection and response
Tier 1: Stop What You Can

- Maximize usage of traditional security controls
  - Gateway email filtering
  - Gateway content filtering
  - Domain SPF
  - Host level filtering
  - Host level execution controls
Tier 2: Educate and Change User Behavior

- Adopt a continuous education program
- Maintain training focus on current threats
- Run simulated scenarios
- Provide integrated education in the context of the training exercise
- Report and measure users and the program’s overall performance
“Traditional approach doesn’t work”

Security awareness didn’t, because we were:

- Boring
- De-focused
- Compliance oriented
- Annual

We didn’t have metrics to prove otherwise!
Making It Work: Think “Marketing”
Making It Work: Immerse in the Experience
Making It Work: Real-time Feedback

Source: Fitbit.com

© Copyright 2012-2013 PhishMe, Inc. All rights reserved.
Education Must Be a PROGRAM

1. Choose a Theme:
   - Click-Only
   - Data Entry
   - Attachment-Based
   - Double Barrel
   - Benchmarking

2. Create Email:
   Upload your recipient list and create your email.

3. Choose Training:
   Choose from PhishMe provided training modules or redirect to your organization’s internal training.

4. Measure Results:
   Send the email, track the results, and measure your progress.

- Unlike typical security technologies we are ‘touching’ non-IT savvy employees
- Avoid those political landmines
- People don’t like to feel cheated
- The soft elements are more important than the simulation itself
Making It Work: It Needs to be Continuous

Users Caught by Phishing Exercise

- Test #1: 150 people caught out of 200 (75%)
- Test #2: 2,582 people caught out of 5,000 (52%)
- Test #3: 213 people caught out of 5,000 (4%)
- Test #4: 355 people caught out of 5,000 (7%)
- Test #5: New test population from 5,000 to 14,300
- Test #6: 3,930 people caught out of 14,300 (27%)
- Test #7: 3,168 people caught out of 14,300 (22%)

Benchmark (31%)

CALENDAR

Phishing Exercise Topics
- Test 1 – Feb 2012: Salary Survey Phishing
- Test 2 – May 2012: Salary Survey Phishing
- Test 3 – Oct 2012: Virus Outbreak Phishing
- Test 4 – Feb 2013: Social Media Phishing
- Test 5 – May 2013: Fake Fax Phishing
- Test 6 – Sep 2013: UPS Acknowledgement

Repeat Offenders ("Caught" more than twice)
- Test 4 – 251 repeat offenders from test 1-3
- Test 5 – 777 repeat offenders from test 1-4
- Test 6 – 900 repeat offenders from test 1-5

*Benchmark – Average response of (31%) against this phishing method for all customers of "phishme.com"
Lesson - Broad Exposure is Key

• Not just for “high value” targets
• Lesson from RSA compromise in 2011 –
  – Spear phishing targeted 4 mid-level employees
  – Attack succeeded...cost the company $66MM

• Teach everyone
  – Build the message appropriate to their level of experience
Tier 3: The User CAN be a Threat Detection Sensor

- Most people respond to emails within the first few hours of receiving them.
- If users are empowered to report, IR & SOC teams get relevant and timely threat intelligence.

“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
Users who learn to not fall for phishing attacks also learn to report them. *PhishMe’s Phish Reporter is a one-click button for users to send in near real-time threat data.*
Shrink the Detection Window to Seconds!

Customer deployed Phish Reporter on 60,000 email clients and ran a phishing simulation. The results:

At 6:01:15am, **a diligent user flagged the attack — 15 seconds before the first compromised user clicked** on the fraudulent link (6:01:30).

Over the next 75 seconds, the next six users correctly identified attack.
Customer ran campaigns for both attachment-based and click-only spear phishing scenarios.

45% of users fell for the first attachment-based campaign, followed up with immediate education.

Employees were more susceptible to attachment-based phishing attacks - an increase in education led to an immediate improvement to this scenario.

By focusing on attachment-based phishing attacks, the Customer addressed a specific pain point and effectively mitigated the threat of future attachment-based spear phishing attacks.
Case #2 – The Need for Continuous Education

Customer results 5/2011 to 6/2013

- Customer ran its first simulated spear phishing campaign in May 2011.
- During first year, significant improvements were realized as employees went through PhishMe’s educational process.
- From March 2012 and June 2013, the Customer did not run any phishing campaigns. The result: a significant spike in response rates.

The Conclusion: Organization must continuously educate users to effectively mitigate the threat of phishing attacks and significantly reduce susceptibility.
What We Have Learned After 5 Years

• Telling users about the program upfront is critical to its success and helps avoid ego battles.

• On average, **most organizations move from a 60% susceptibility to 10%**. AND employees report feeling empowered, reporting that they avoid phishing attacks on personal accounts.

• Every industry vertical needs a people-centric security strategy, inclusive of a phishing training program.

• Organizations can experience valuable side benefits.....
Customer Outcomes

- Decreased incidents caused by phishing
- Increased user reporting of phishes
- Decreased time: in both incident to report and incident to containment
- Improved internal communications
- Provided better metrics

Employees become part of the solution, instead of viewed as the problem.
Thank You