Blunting the phisher’s spear: A risk-based approach for defining user training and awarding administrative privileges

Arun Vishwanath, Ph.D., MBA
Associate Professor
http://arunvishwanath.us
I study how hackers, cyber terrorists, hactivists enter networks...
I study...

- I study how hackers, cyber terrorists, hactivists enter and compromise networks

- The proverbial “people problem” of cyber security
Unintentional Insiders

Brute Force Hacking

DEFENDED

UNSECURED INTERACTION

Organizational Email Provider

External Email Provider

Spear phishing

VULNERABLE

HABITS

PERSONALITY

PERCEPTIONS

COGNITIVE PROCESSING

PSYCHOGRAPHICS

EMPLOYEE

UNINTENTIONAL INSIDER

External

Email Provider
Data breaches keep getting bigger...

Source: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
Spear phishing is the attack vector of choice.
Impacted every industry

- Information Technology
- Aerospace
- Public Administration
- Satellites and Telecommunications
- Scientific Research and Consulting
- Energy
- Transportation
- Construction and Manufacturing
- International Organizations
- Engineering Services
- High-tech Electronics
- Legal Services
- Media, Advertising and Entertainment
- Navigation
- Chemicals
- Financial Services
- Food and Agriculture
- Metals and Mining
- Healthcare
- Education

Industries Compromised by APT1
Perpetrated by State and Non-state Sponsors

YOU ARE THE WEAKEST LINK IN CYBERSPACE

SYRIAN ELECTRONIC ARMY

WE ARE ANONYMOUS
Approaches to dealing with the “people problem”

- Firewalls, antivirus; Whitelisting approaches

- EMET; Constrain access/admin privileges
How realistic is this...
Human factors approach: Cyber security training

1. “Phish” people simulations
2. Show them why they fell for it
3. Keep telling them to shape-up
4. Admiral Mike Rogers: “We should court-martial them!”
The PEOPLE PROBLEM

The Problem is NOT the People

It is in our UNDERSTANDING of PEOPLE

We Have developed a human factors model that explains how people think, act, behave online, and why.
Suspicion, Cognition, Automaticity Model (SCAM) (Vishwanath, Harrison, & Ng, 2016)
SCAM explains how users think:
Scrooge: I am a cognitive miser

I use cognitive shortcuts a.k.a Heuristics
Heuristics
Dear Anthem Client,

We wanted to make you aware of a data breach that may have affected your personal health information and credit card data. The data which was accessed may impact clients who made credit or debit card payments for healthcare or who got treatment during the year 2014.

Your trust is a top priority for Anthem, and we deeply regret the inconvenience this may cause. The privacy and protection of our client’s health care information is a matter we take very seriously and we are working diligently to resolve the incident.

To subscribe to a free year of credit card account protection please click on the link below and follow the instructions that will be required:

Click Here To Get Your Free Year Of Credit Card Protection
Dear [Redacted]

As you may have heard in media reports, Excellus BlueCross BlueShield (Excellus) publicly disclosed that it was the victim of a cyber attack. Excellus notified Anthem about this incident on September 9, 2015, the same day Excellus notified the media. You are receiving the attached letter from Excellus because Excellus has determined that your information may have been impacted by the cyber attack.

We would like to help explain Anthem’s relationship with Excellus and why your data may have been in Excellus’s systems. First, Anthem is neither owned nor operated by Excellus. Excellus is a separate company with which Anthem works to administer certain programs for health plans.
SCAM explains what users believe:
Cyber Risk Beliefs

WHAT IS SAFER:

- PDF vs. Word Document
- OSX vs. Windows
- iOS vs. Android
- Chrome vs. Safari
- Google Fiber vs. Free wi-fi
- Browser based email access vs. using an email client
SCAM explains the role of habits and devices
Habits

- Ritualistically checking email
- Texting while talking, walking, driving
- Entering login, password, authentication credentials
Smartphones, smart watches... not so smart people

Thanks Apple and Google!
Beware of

Cute Duckling Scam
Victimization, Suspicion, Cognition, Automaticity Model (SCAM) (Vishwanath, Harrison, & Ng, 2014)
Leveraging the understanding of people
Develop a Cyber Risk Index (CRI)

- An empirical data driven approach

- Uses a short, 40 question self-report survey

- Can be done within existing “red-team” simulations

- Like credit rating, it can we aggregated across division, organizations, sectors

© Arun Vishwanath
Deciding who gets trained and how:

- Cyber risk beliefs
  - Faulty
    - Yes → Belief Change
    - No
  - Poor
    - Yes → Better Heuristics
    - No
  - Inadequate
    - Yes → Education
    - No
  - Bad
    - Yes → Habit Change
    - No

Heuristics

Systematic processing

Habits

© Arun Vishwanath
Deciding who gets access:

- Current system of providing access is based on organizational role and status
- Use CRI to identify individual risk levels and changes in risk behavior overtime
- This becomes a quantitative score of INDIVIDUAL CYBER HYGIENE
References to published research and writings:

Selected Academic Research


Selected pieces in CNN


Contact Information

Arun Vishwanath, Ph.D., MBA
Email: avishy001@gmail.com
Web: http://arunvishwanath.us
Mobile: 716.508.0192