Rethinking the Front Lines

or...

Hacking the Enterprise
Social Engineering Your Company’s Culture
Culture Hacking for fun and profit
Streetlight Effect
Problem

- Look at the headlines (um, Twitter timeline!)
- Lost laptops
- Bad passwords
- Password reuse
- We tend to focus on the glamorous attacks
- We’re so tools focused we forget the humans
- Security professionals have given up. Sometimes silently, sometimes explicitly
The Debate

• Wait, there’s a debate?
• Bruce Schneier’s article
  • Analogies to exercise, infectious diseases, driving, washing hands
• Dave Aitel’s article
• RSA panel “debate”
• Us vs. Them attitude
What’s in a name?

- What is “security awareness training”?
- My friend’s awesome training experience
- What are the goals?
- Nirvana fallacy
- Shift the balance. Small changes can really add up.
Habits
Bruce Schneier: “If we security engineers do our job right, then users will get their awareness training informally and organically from their colleagues and friends.”
Culture
Twitter Culture

• More new people than old people
• Growing out of the good culture; microcultures
• Keeping the good stuff
• Twitter Core Values
  • “Grow our business in a way that makes us proud”
  • “Innovate through experimentation”
More debates?!

- Culture Eats Strategy For Lunch by Shawn Parr in FastCompany
- Culture is a balanced blend of human psychology, attitudes, actions, and beliefs that combined create either pleasure or pain, serious momentum or miserable stagnation. A strong culture flourishes with a clear set of values and norms that actively guide the way a company operates.
Other views

• Reply by Venkatesh Rao on his blog

• But the lesson here isn’t that “culture eats strategy for lunch.” The lesson is that culture is what allows you to double down on a successful strategy. You still need the noncultural parts of strategy to create an opening. You will not be able to double down on all openings.

• Not hard to find other opinions on the matter
Being Rigorous

- Is training never effective? Or does the material suck? (Or maybe the trainer??)
- How are we measuring effectiveness? (Is anyone *really* measuring?)
- Can we measure culture? Or what would be a good proxy?
Goals

• Find a population to study
• Determine what to study
• Build feedback loop
Choosing the Population

- Lots of work going on, too much to manage all at once
- Segment by department? Geography? Something else?
New Hires

- We selected new hires for a few reasons:
  - They have to show up for their first day of work. I have a captive audience.
  - They are eager and impressionable. They are more likely to do what I say on that day than before they get caught up in their hectic work.
  - Over time they will represent a cross section of the company
  - We can track them during their entire company career
Who Presents?

• Does it matter?
• I do (when I’m not presenting at conferences)
• Signals to new hires that this is important, and I’m willing to make the time to do it
• How to measure the value?
Password Nightmares

- Thank goodness they’ll all be gone soon!
- Requirements and enforcements
- Good passwords: Not just a problem for regular users. Security pros too.
#prostyle Strategies

- Common
  - Hard to remember string, modified by something in the site I’m visiting
  - reused “low-value” password
- Not as common
  - xkcd passphrases
  - password managers
Password Managers

- Passwords may be going away, but a bunch are still around
- Create, use, manage strong passwords
- What do users really do? Not what security teams hope, assume they do.
- Does anyone teach users to use one? (not Tell)
- It took me a while to get into the swing of using one
Phishing Strategy

- Common phishing strategy:
  - phish employees
  - wait
  - phish them again
  - hope the numbers get smaller
- Anti-bodies!
- Can we do better?
Goals

• Cross correlate: Lost assets, password manager, phishability, and other factors

• Baseline data

• Study subjects over time, not just between two phishing campaigns

• Run multiple campaigns

• Get feedback loops going besides just phishing

• Weave in culture of security
Feedback Loops
Suspicious Events

- Phishing alert mailing list
- We try to answer them all (reward)
- We track:
  - suspicious but harmless
  - real attacks
  - spam
  - training (us)
Office Hours

- Come talk about anything (even non-security topics)
- Ask “dumb” questions (that aren’t so dumb after all)
- Building rapport
- Confessions
Some Results
Password Vault Usage
Password Vault - Early in program
Password Vault - Later in program
Password Vault - Some burnout in the first few weeks after they start, but if they survive, they become long term users.
Password Vault - hot spots

The graph shows the average usage over time for different departments:

- **Average Usage - Dept A**
- **Average Usage - Dept B**
- **Average Usage - Dept C**
- **Average Usage - ALL**

The x-axis represents time in intervals, and the y-axis represents usage percentage from 100% to 20%. The graph indicates a decreasing trend in usage over time for all departments, with slight variations among them.
Password Vault - Low adoption rate for Dept C

Lesson: Work to find out what’s happening in the field. Uptick is us identifying and doing a breakout training.
Phishing
Phishing Campaigns
Phishing - ID hot spots

We take the raw numbers, by department, who engaged with the campaign:

And we learn which departments are most likely to click on phishy links:
Phishing - ID hot spots

We take the raw numbers, by department, who gave up credentials:

And we learn which departments are most likely to give up credentials:
Phishing - Gender Differences
Feedback

We encourage our employees to report phishing attempts, and we track our response rate.
NHO Training Evolution

- Require users to change their passwords during the training session, using a password manager
- People loved it if they stuck with it
- Solicit information from the new hires about their knowledge of social engineering attacks, phishing, etc.
- More interactive
- Audience management
Areas for more research

- Blink response
- Measuring effectiveness of social engineering video
- More gamification
- Personal/team security scores
- Measuring by other factors like years in industry, first language, other cultural differences.
Lessons

• Track what changed in the NHO classes, slides
• Be careful of telling just one Story based on the Data
• Be prepared to be surprised, and sometimes confused
• Focusing on humans/culture isn’t just for pen testing
Conclusion

- Some successes, a lot of new questions
- Focus on building Culture, not Training
- Measure, change, repeat. It works!
- Never give up on users. It’s never a lost cause until you believe it is.
Look for the problems where they are, not where the light is.
Thank You!

@boblord