Smart Phone Security & Privacy:

What Should We Teach Our Users

…and How?

Norman M. Sadeh, Ph.D.

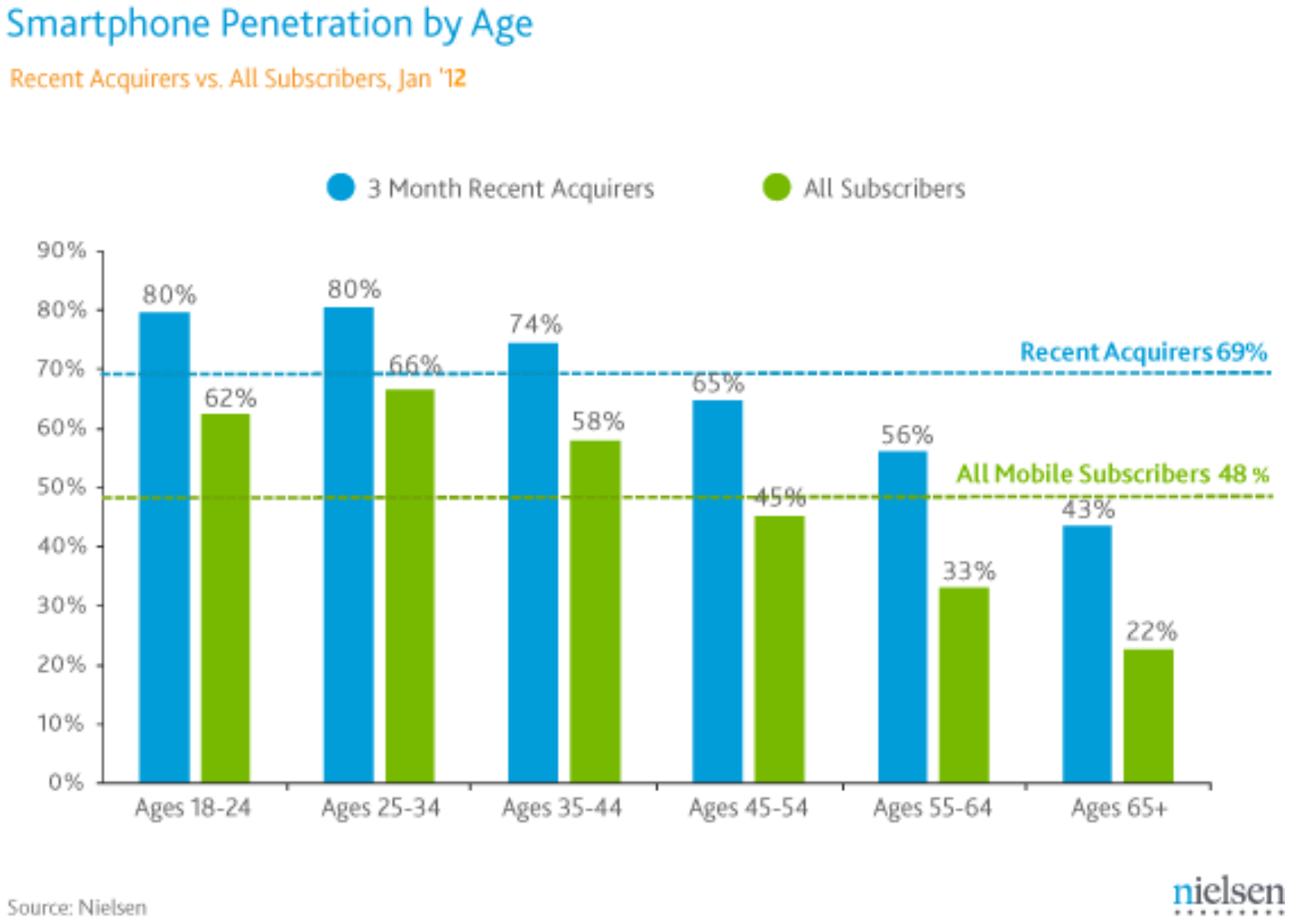
Professor, School of Computer Science
Director, Mobile Commerce Lab.
Carnegie Mellon University

Co-Founder & Chief Scientist
Wombat Security Technologies

mobile commerce lab

wombat™ security technologies

The Smart Phone Invasion



BYOD: The New Frontier

- 48% of employees will buy their own devices – *whether their organization approves that particular device or NOT!* (Forrester Research)
- Blur between work life & private life

- Unrealistic policies don't work – even if they look good
- "If you can't fight them, join them"
  - **…hopefully under your own terms…**

The Problem is that…

BYOD implies users who are:

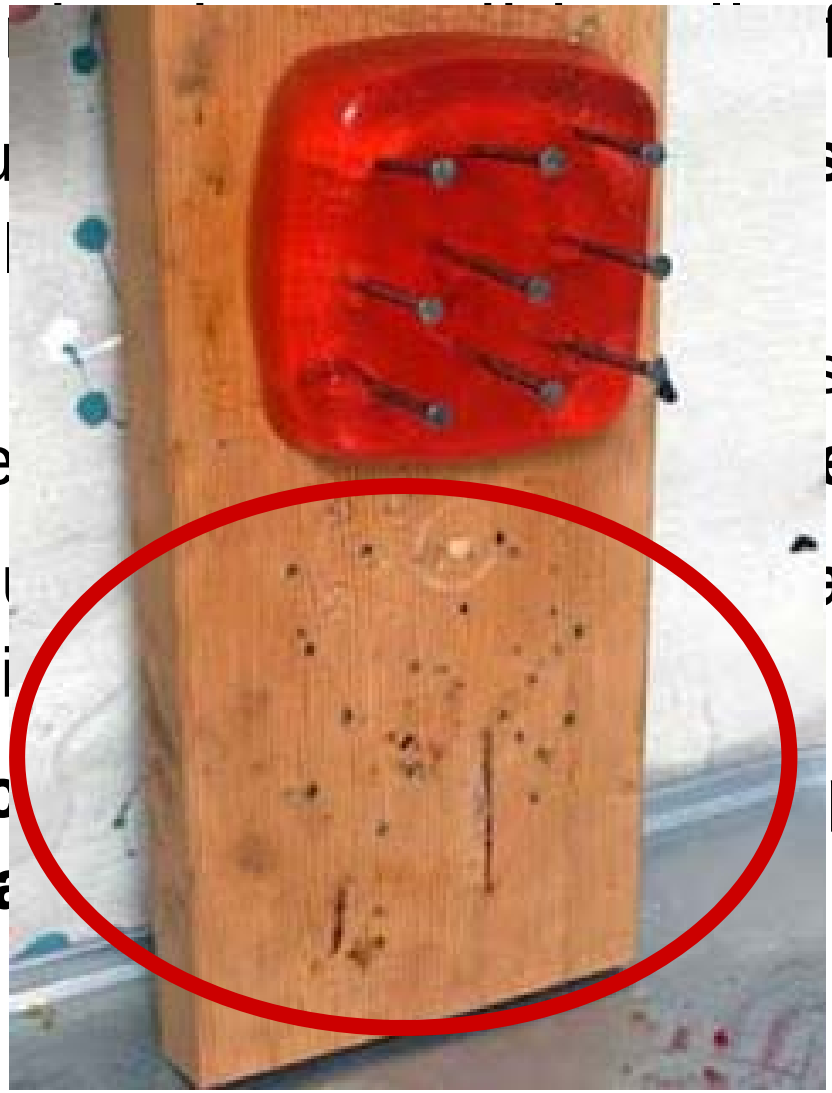
- responsible

Do we really have a choice?

Training has a Big Role to Play

...But trai failed

- Secu **sk**:
  empl d to learn
- Trad s and content
  have **elling**
- **Req** **ast** &
  conti
- **Prac** ps are **not**
  alwa

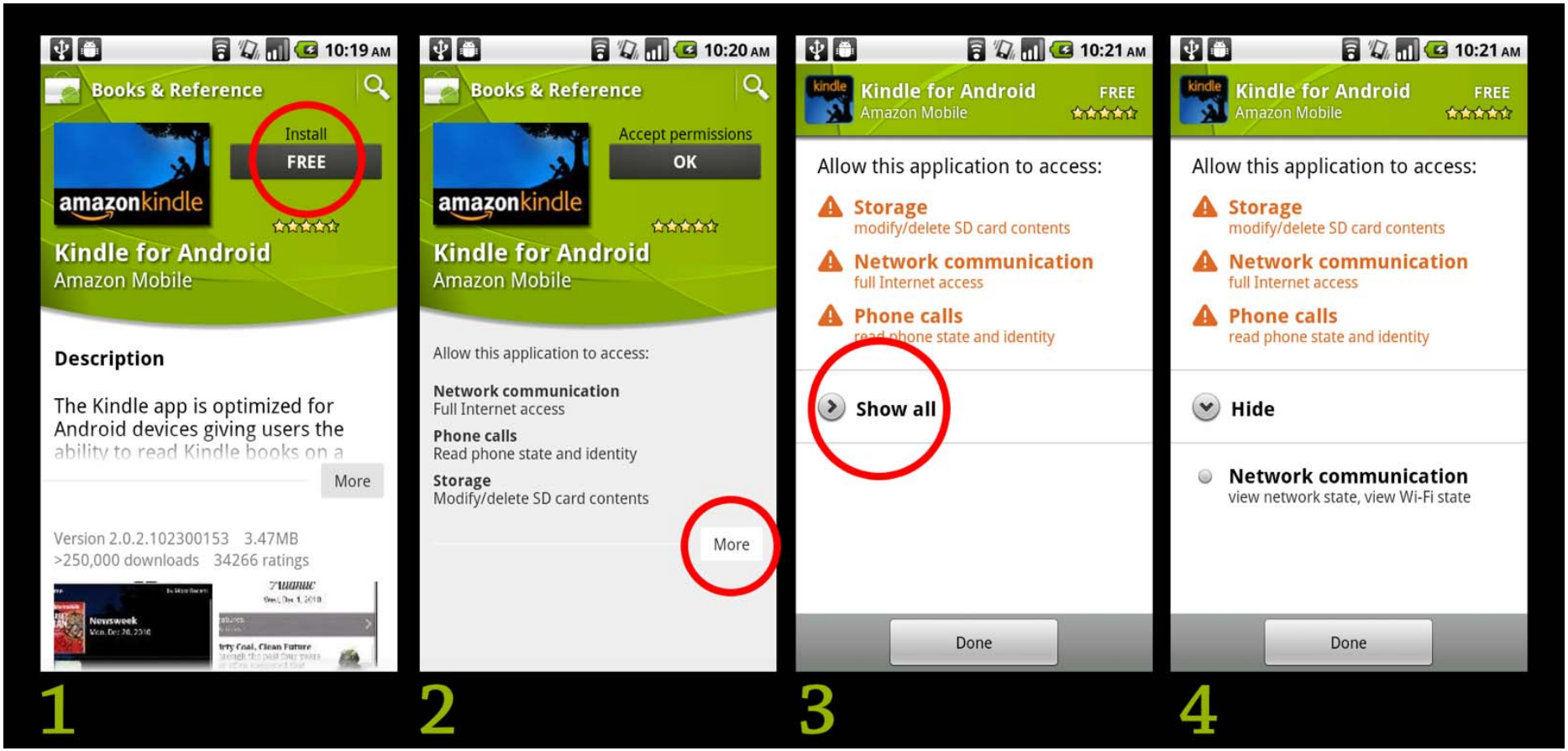


Mobile Security & Privacy Training

…at least as complex…

- Mediates a wide range of **scenarios**
- ….and obviously
- they are **mobile**
- devices…

Android Permissions:
An Example of the Challenges We Face



P. Gage Kelley, S. Consolvo, L. Cranor, J. Jung, N. Sadeh, D. Wetherall, "**A Conundrum of Permissions: Installing Applications on an Android Smartphone**", USEC2012.

What Are We Up Against?

- **Misconceptions**: Most users did not realize that apps were not vetted

Where Do We Start?

of apps, even though they don't understand the permissions

Understanding the Risks: The Big Gap

The more features your phone has
the more risks it carries:

Features	Risks
Calling	Eavesdropping Social Engineering
Location	Tracking
Bluetooth	Contact theft Phone or SMS hijacking
WiFi	Snooping Viruses and Trojan Horses
Emails	Phishing Impersonation
Apps	All of the above and more

Most people do not realize how sensitive their phones are

…and How Vulnerable They Are…

- Challenge them to take quizzes
- …or better: Motivate them via mock attacks
- **Nothing beats showing a user how vulnerable (s)he is**

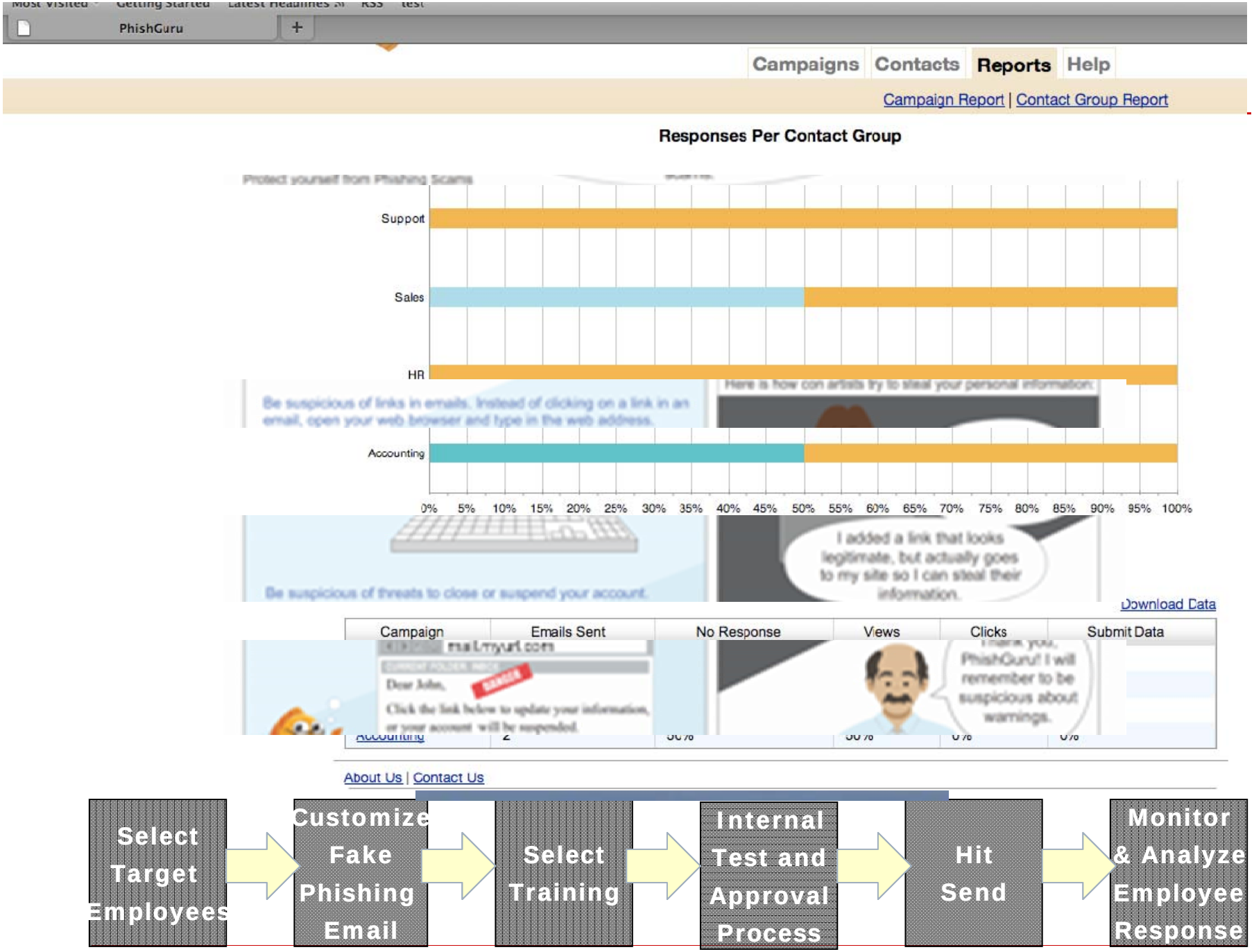
Phishing as An Example

- **Email phishing**: Much worse on mobile phones
  - Mobile users are first to arrive at phishing websites
  - Mobile users **3x more likely to submit credentials** than desktop users

Source: Trusteer, Jan. 2011 – similar

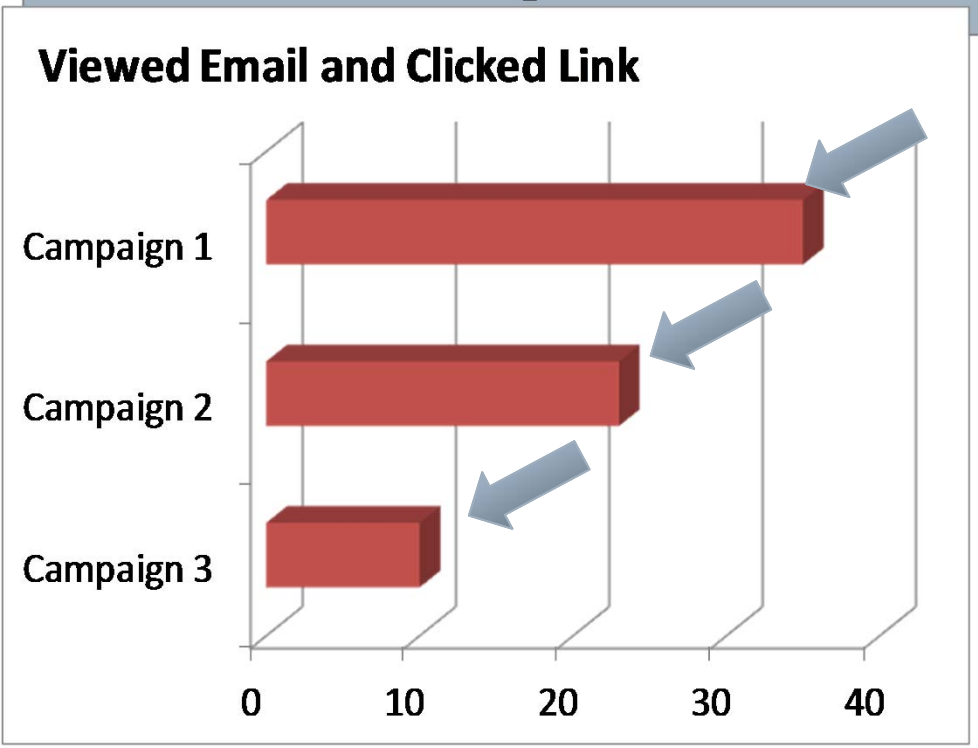
Training via Mock Attacks: PhishGuru

- Teach people **in the context** they would be attacked
- **If a person falls for simulated phish**, then pop up an intervention
- Unique "**teachable moment**"



This really works!

Reduces the chance of falling for an attack by more than 70% !



Actual Results

Starting with the Most Common Threats

- Millions of cell phones lost or stolen each year
- Majority of smart phone users still do not have PINs

rce for image: http://www.malaysianwireless.com/2011/09/advice-how-to-protect-your-smartphone/

Learning by Doing is Critical

Teach people to better appreciate the risks

Create mock situations

Force them to make decisions

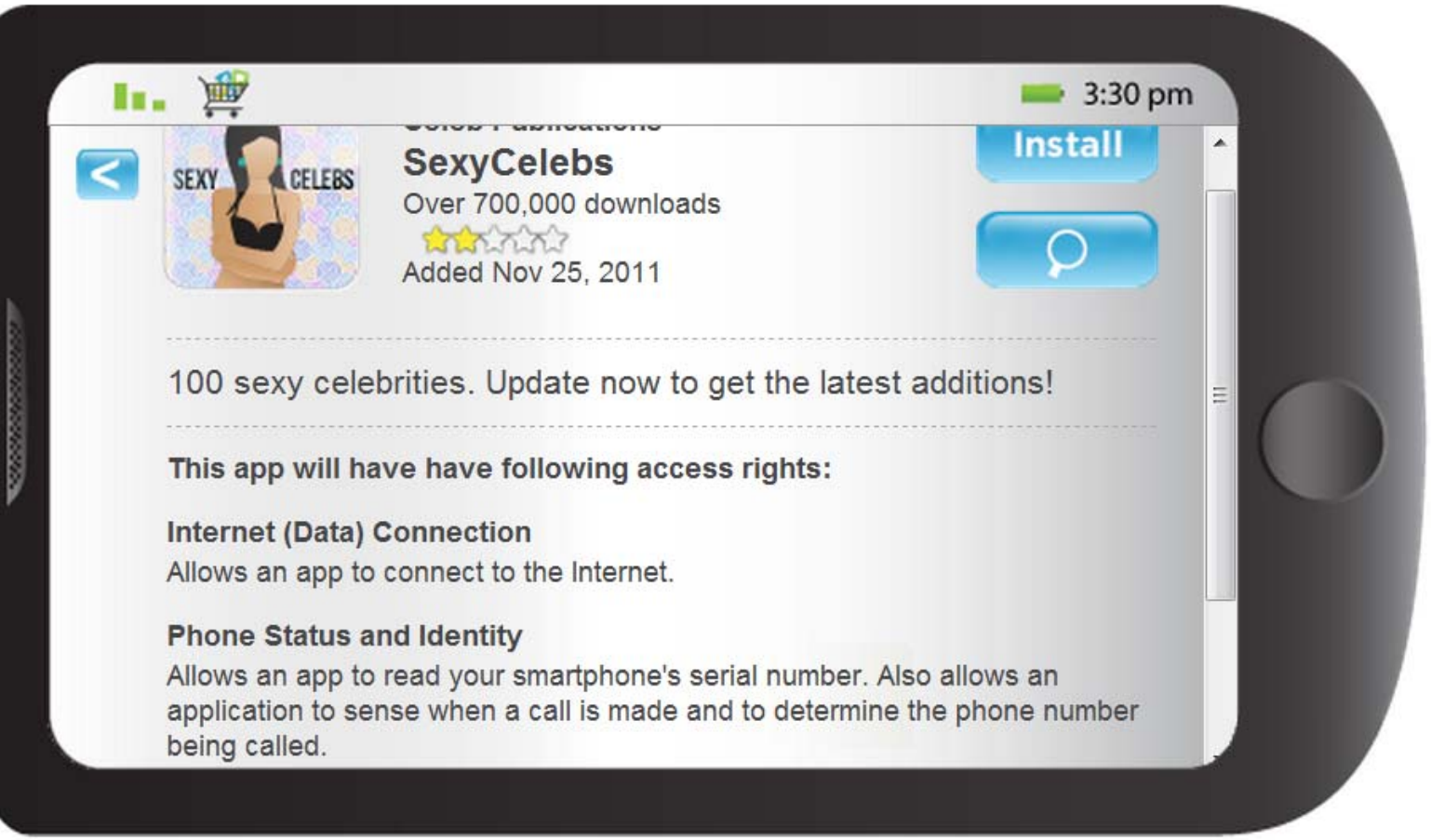
adually Move Towards More Complex Tasks

- Mobile Apps
- Location
- Social Networking

Mobile Apps

- **Challenge**: difficult to come up with full-proof rules
- Train people to be suspicious & look for possible red flags
- Emphasis on:
  - **Learning by doing**
  - **Feedback**
  - **Opportunities for reflection**

From Simple to Increasingly Realistic



Concluding Remarks

- BYOD trends make training critical
- Users have little awareness of the risks associated with smart phones
- Effective training requires adoption of learning science principles
  - Creating realistic scenarios – including mock attacks
  - Interactive training - Learning by doing
  - Start with most common risks
- Training has to be part of an employee's daily life – repetition & variations are critical

Q&A

http://mcom.cs.cmu.edu

http://wombatsecurity.com