

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

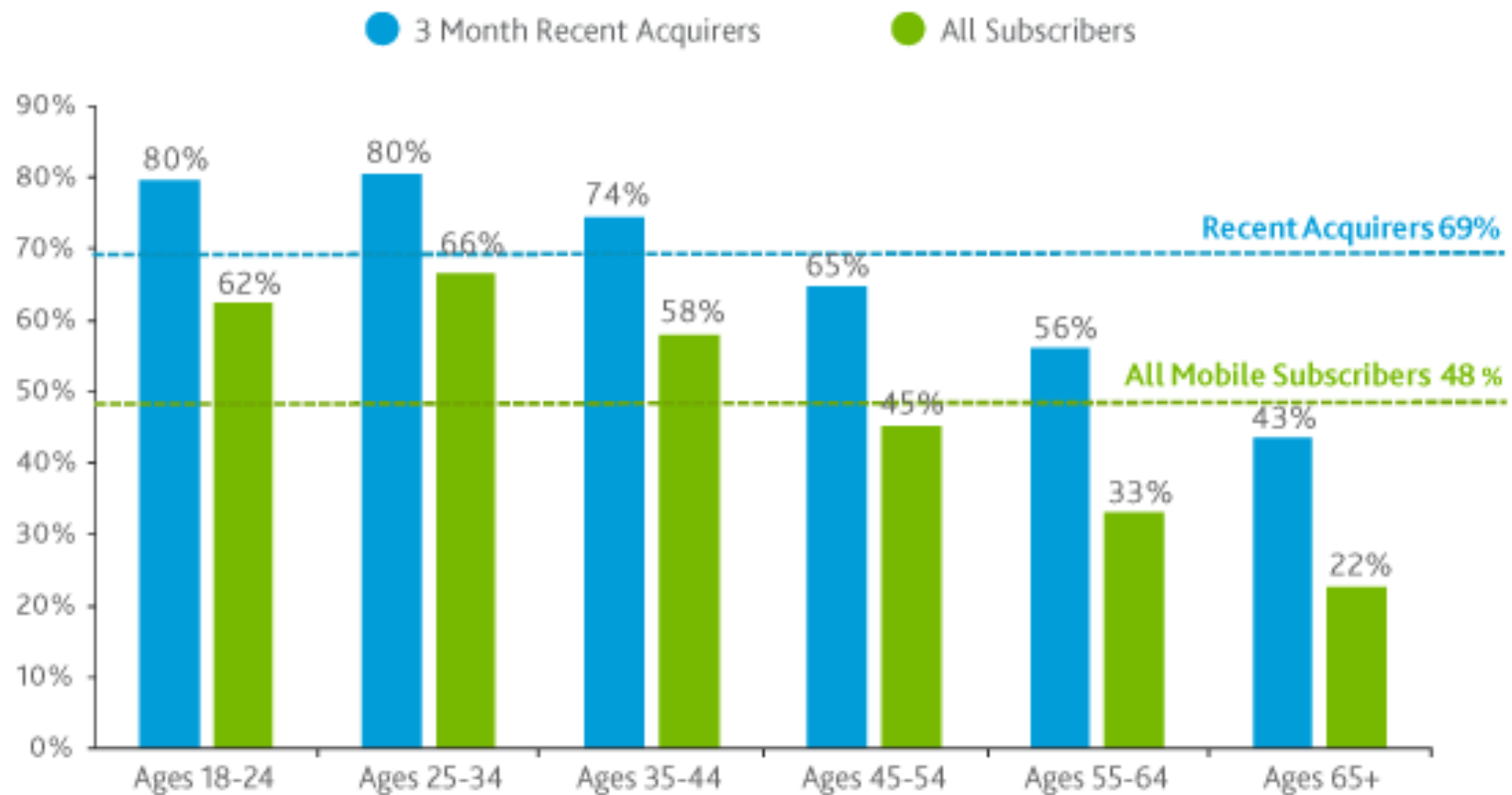
Co-Founder & Chief Scientist
Wombat Security Technologies



The Smart Phone Invasion

Smartphone Penetration by Age

Recent Acquirers vs. All Subscribers, Jan '12



Source: Nielsen

nielsen

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:

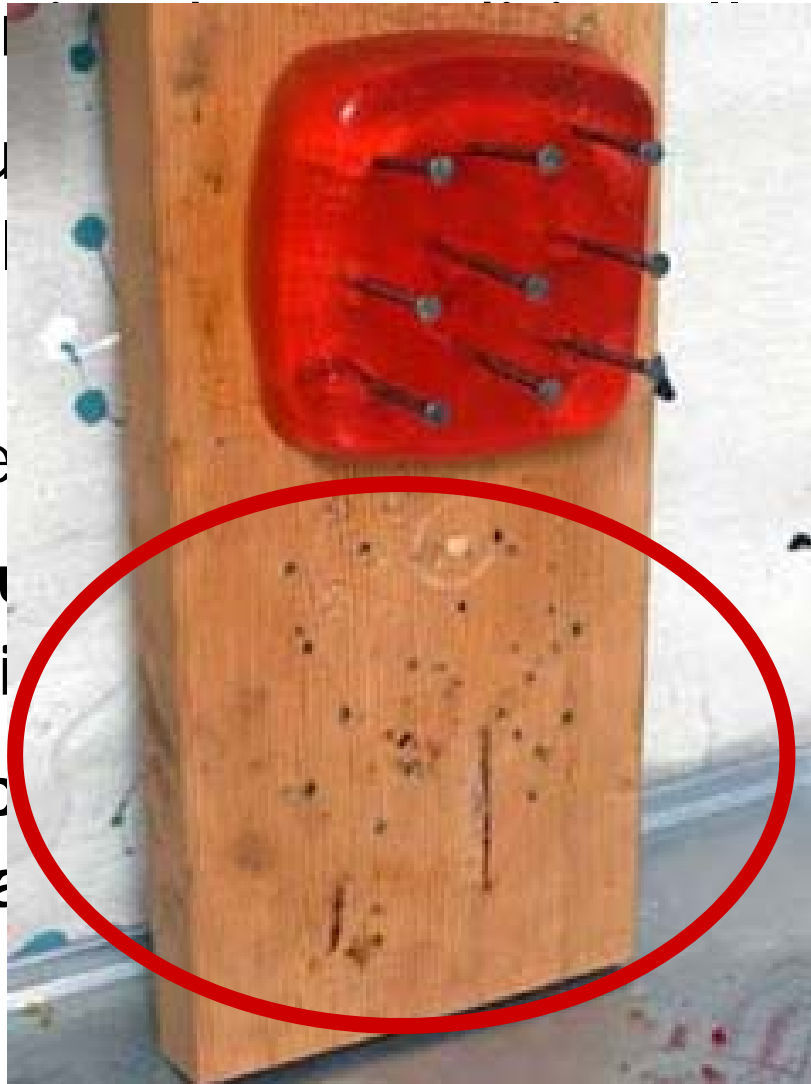
■ responsible

Do we really
have a choice?

Training has a Big Role to Play

...But training

- Security
- empl
- Trad
- have
- **Req**
- conti
- **Prac**
- **alwa**



failed

sk:

d to learn

s and content

elling

ast &

ps are **not**

Mobile Security & Privacy Training

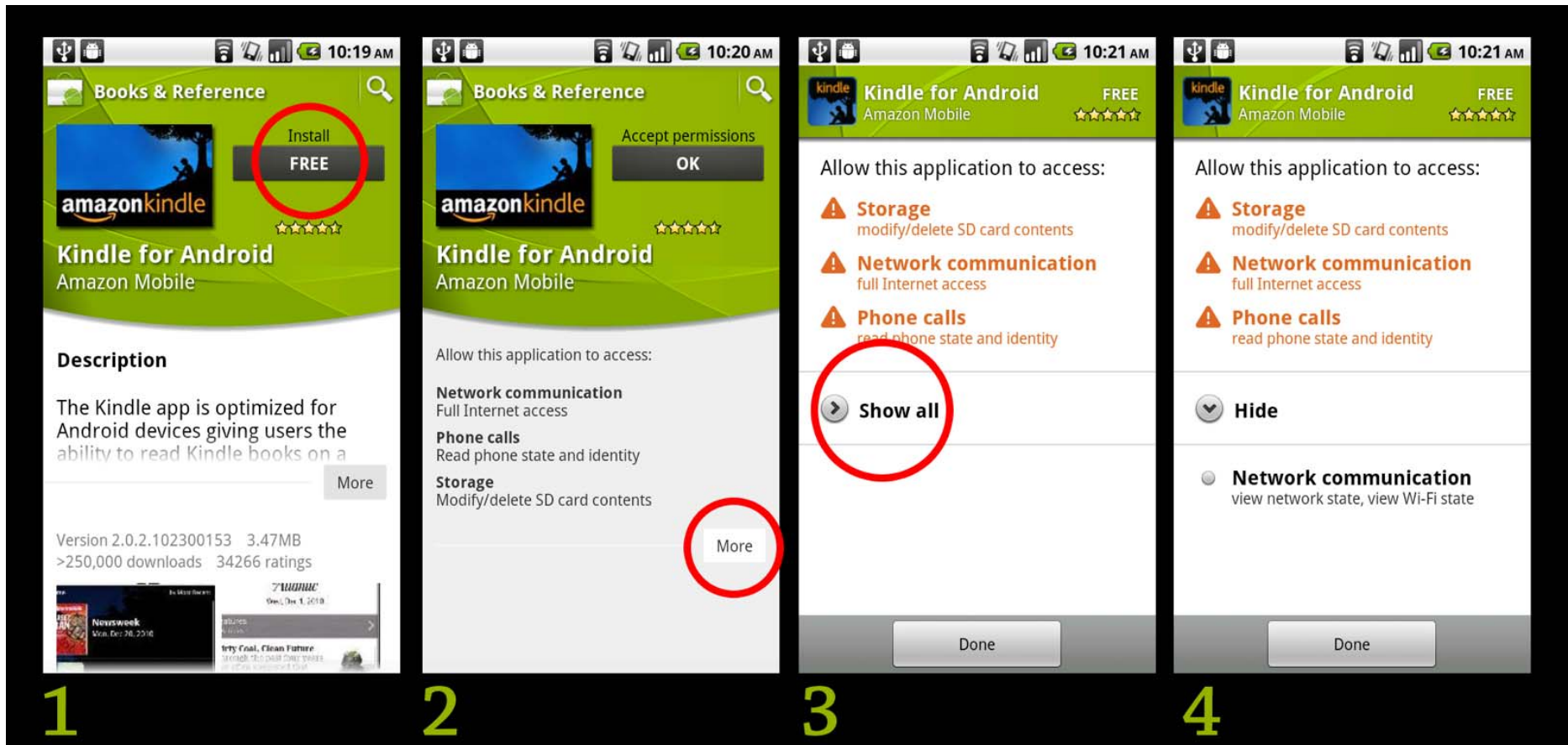
...at least as complex...

- 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

Smartphones carry a lot of *sensitive information on them!*

names>>addresses>>emails
email addresses>>phone numbers
confidential business information
calendar events>>documents
personal information >>texts
downloaded documents>>
apps>>financial information



© Wombat Security Technologies, 2011-2012

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

Features	Risks
 Calling	<ul style="list-style-type: none">EavesdroppingSocial Engineering
 Location	<ul style="list-style-type: none">Tracking
 Bluetooth	<ul style="list-style-type: none">Contact theftPhone or SMS hijacking
 WiFi	<ul style="list-style-type: none">SnoopingViruses and Trojan Horses
 Emails	<ul style="list-style-type: none">PhishingImpersonation
 Apps	<ul style="list-style-type: none">All of the above and more

© Wombat Security Technologies, 2011-2012

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

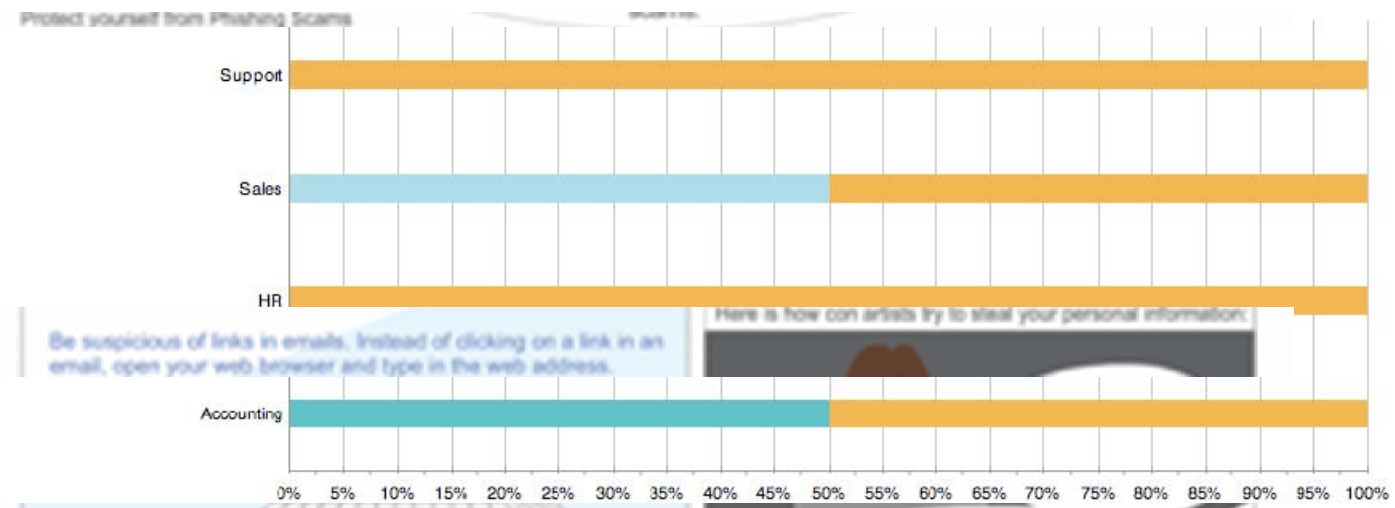
- **Email phishing:** Much worse on mobile phones
 - Mobile users are first to arrive at phishing websites
 - Mobile users **3x more likely to submit credentials** than desktop users

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”**

Responses Per Contact Group



Be suspicious of links in emails. Instead of clicking on a link in an email, open your web browser and type in the web address.

Here is how con artists try to steal your personal information.

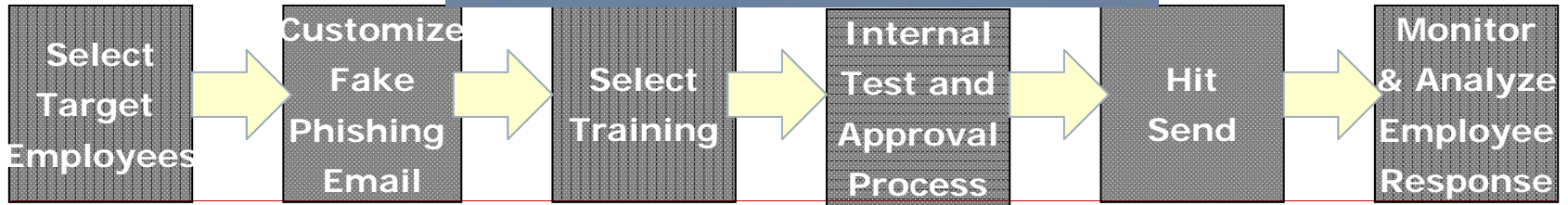
Be suspicious of threats to close or suspend your account.

I added a link that looks legitimate, but actually goes to my site so I can steal their information.

I thank you, PhishGuru! I will remember to be suspicious about warnings.

[Download Data](#)

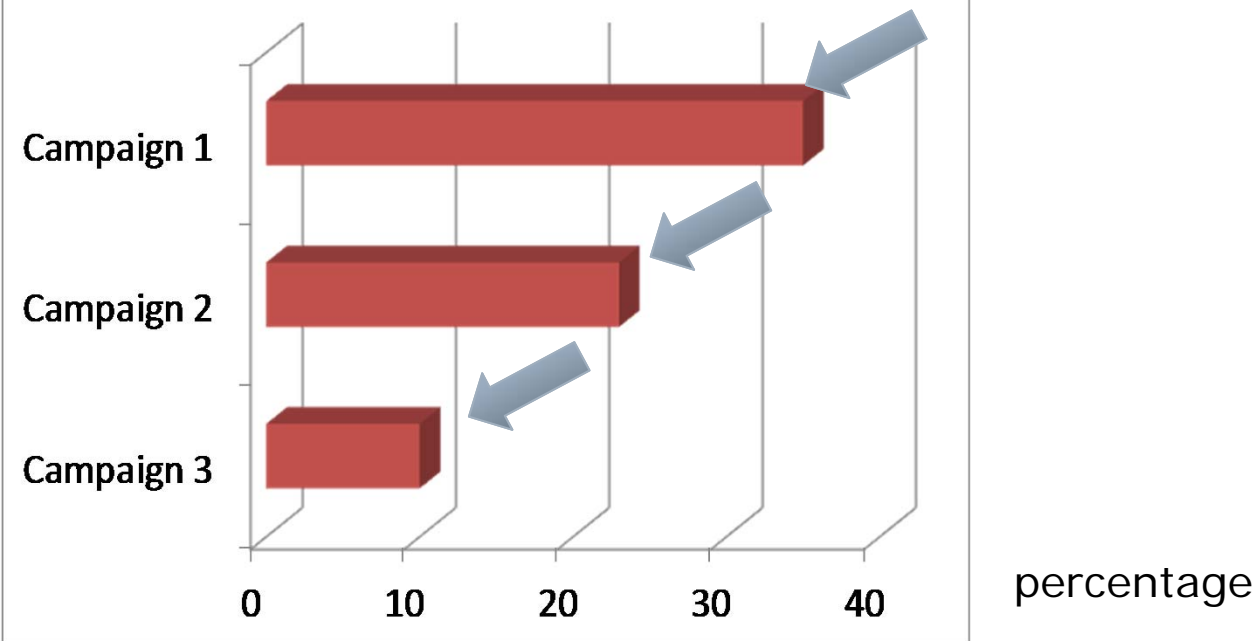
Campaign	Emails Sent	No Response	Views	Clicks	Submit Data
Accounting	2	0/70	0/70	0/70	0/70



This really works!

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

Viewed Email and Clicked Link



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

Learning by Doing is Critical



Smartphone Security

Lesson 2 - Communication

Communication Safety

2/5

Feature



Call



Text



Social



Bluetooth

Determine how risky the displayed activity is:

! *David is on the subway...*

"This project for VisionTech is so far behind, it's unbelievable. ...Yeah, there's no way it will be done in time to get paid this fiscal year."

Low Risk

High Risk

Click the arrow buttons to move through the tips. View all tips to move on.



© Wombat Security Technologies, 2011-2012

Teach people to better appreciate the risks

Create mock situations

Force them to make decisions

Don't do this with formal training

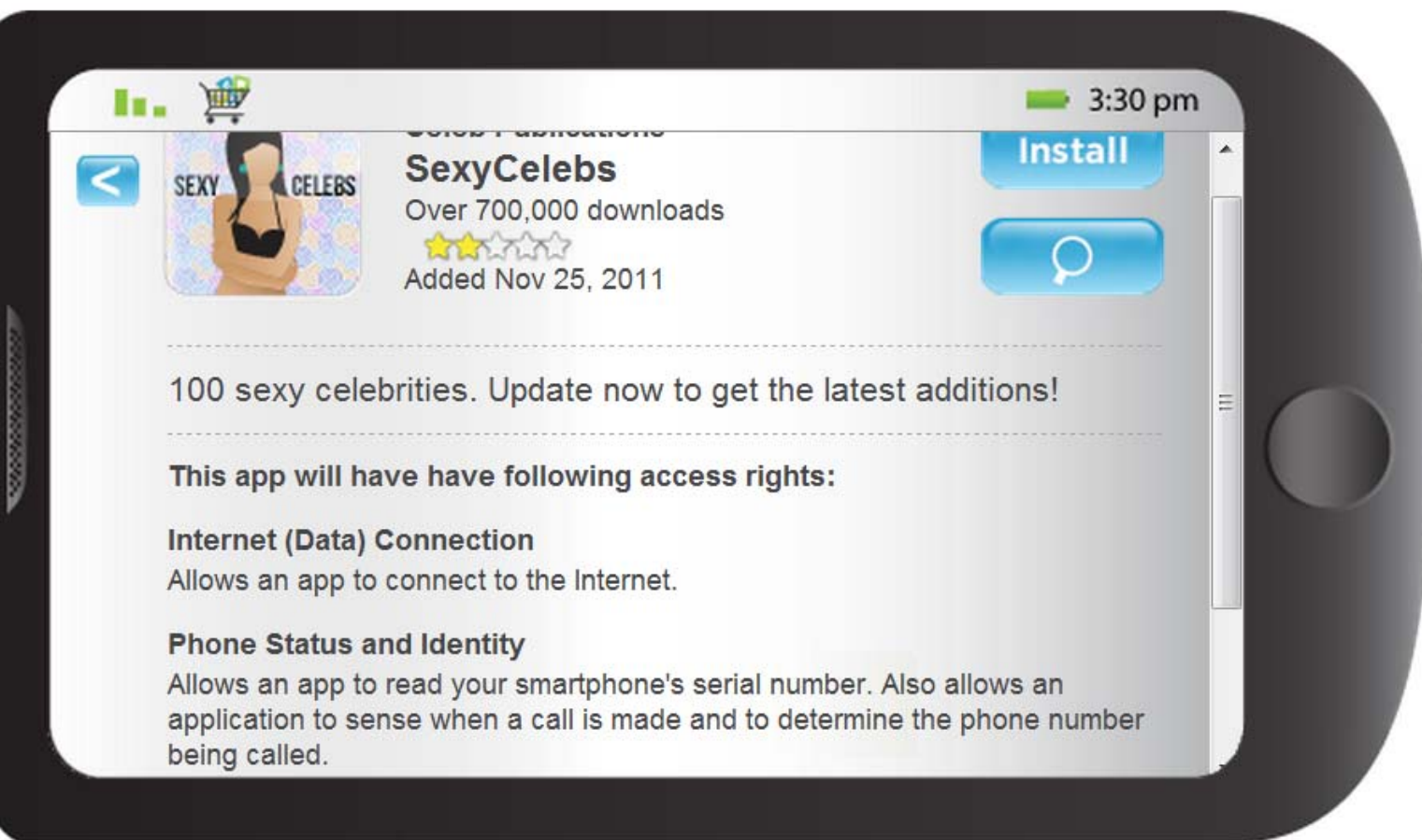
Gradually Move Towards More Complex Tasks

- 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>



wombatTM
security technologies

<http://wombatsecurity.com>