~~Visualizations for Helping People Manage Home Networks~~

Usable Privacy and Security in the Home

Lorrie Cranor
Jason Hong
Ponnurangam Kumaraguru
Steve Sheng

Costs of Unusable Privacy & Security High

- People not updating software with patches
  –> Spyware, viruses, worms
- Too many passwords!!!
  –> Easy to guess
  –> Wasted time resetting
- Hard to configure systems
  –> WiFi boxes returned
  –> Misconfigured firewalls
  –> Sharing entire hard drive (oops!)
- Ubicomp sensing systems scare a lot of people
  –> Less potential adoption

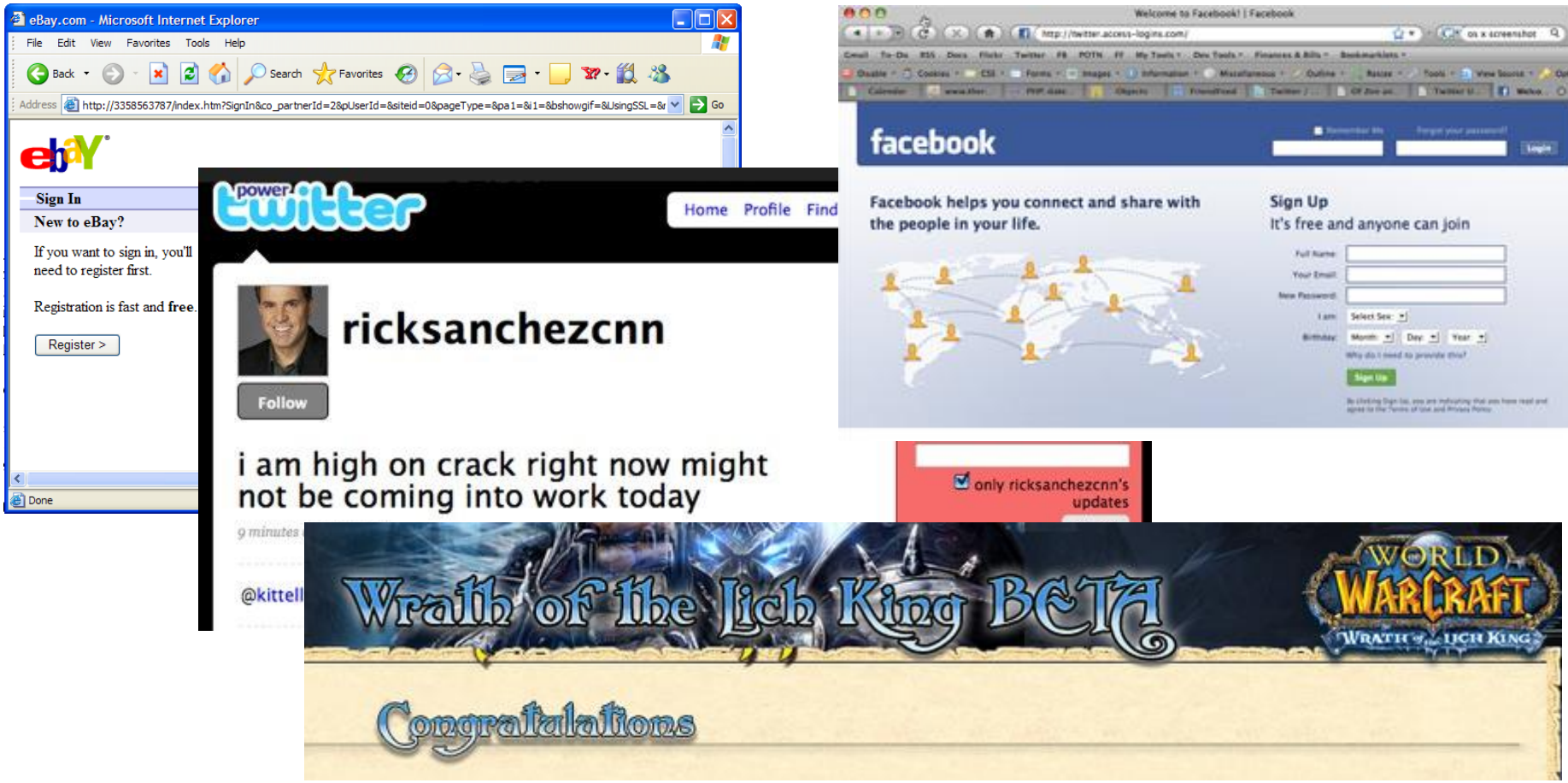
Usable Privacy and Security + Homes

- Symantec said that just over 711,000 new viruses were identified in 2008
- Vint Cerf estimated in 2007 a quarter of computers were part of a botnet

"You know, you can do this just as easily online."

- Ecosystem and business models for crime
  - Making problem of home networking even worse

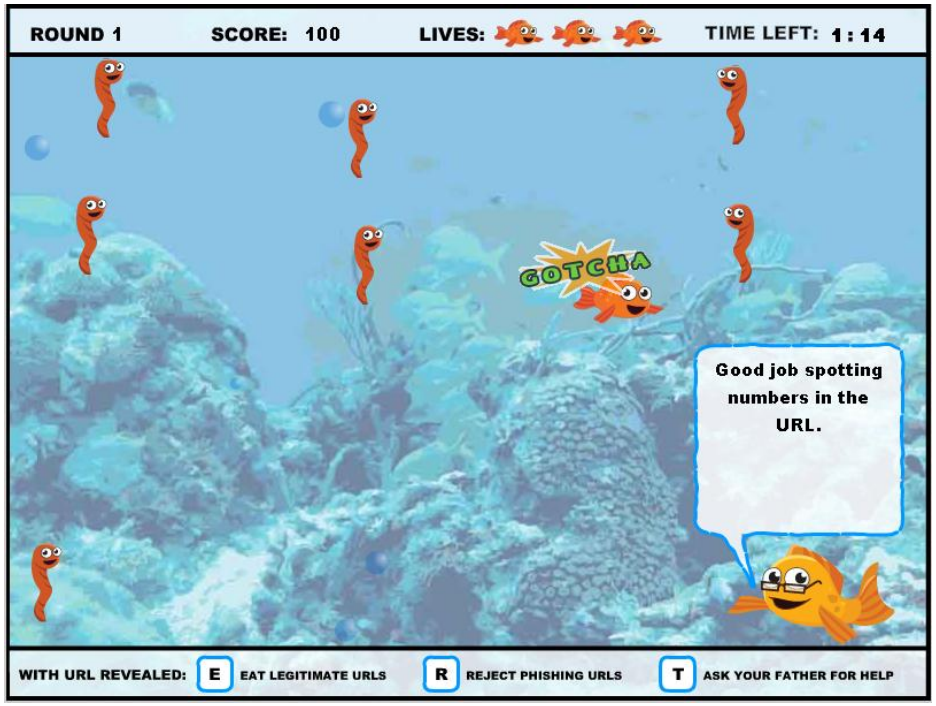
From Phishing to Home Networks

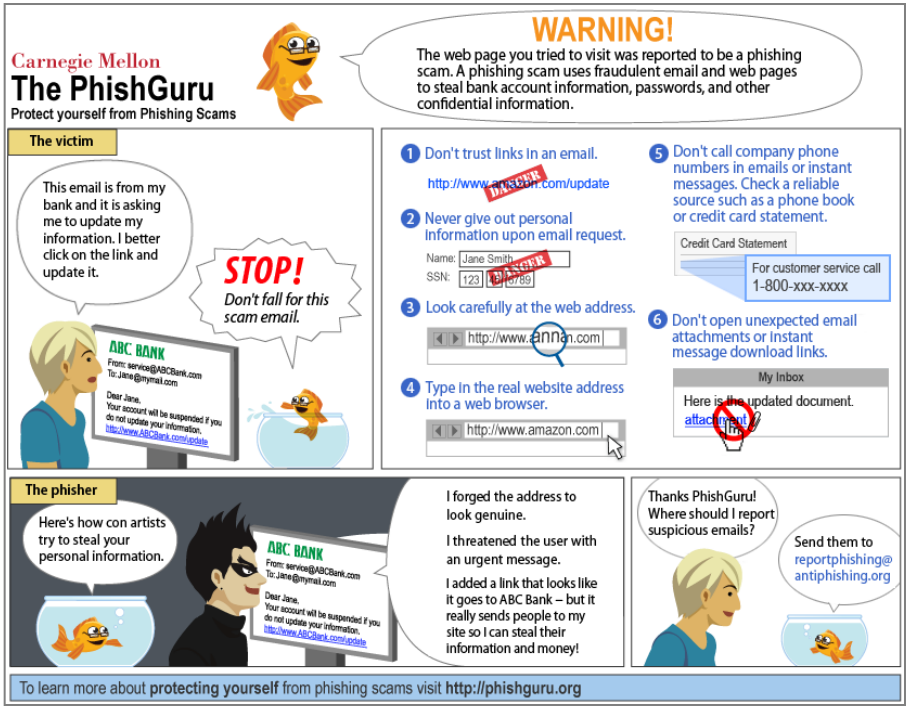


- Can we training people?
- Division of labor for home network security?

Training People

- Three general strategies for usable privacy + security
  - Make it invisible
  - Provide better interfaces (metaphors, models, interactions)
  - Train people





Training People

- Motivating people is possible if appropriate and perceived as useful
  - Through game or thru teachable moment
- Don’t just warn, give actionable items
- Provide basic conceptual model (threat model)
- Apply learning science principles

- But limitations of training too
  - Falling for phishing changed from 50% to 25%, but 25% still
  - Also, 18-21 demographic most likely to fall for attacks
  - How often do people need to be trained?

Division of Labor for Security

- Lots of stakeholders in phishing
  - Primary victims (end-users, banks, ecommerce sites)
  - Infrastructure providers (ISPs, browsers, email, registrars)
  - For-profit protectors (anti-virus)
  - Public protectors (law enforcement, volunteers, academics)
- Questions
  - What is the current state of things?
  - How to prevent future attacks?
  - What countermeasures?
  - How to align incentives?
- Interviewed 31 people among stakeholders

High-Level Findings

Online crime becoming more connected

- Professional criminals actively trying to subvert you and your network
  - “They are criminal organizations with business plans and contingency plans.”
  - “But the goal is to look for not only the traditional stuff but ways to monetize groups of users”
  - Crime is becoming linked: viruses, phishing, spam, etc
- Obvious links here to home network security

High-Level Findings

Stakeholder Capabilities and Incentives Misaligned

- Financial organizations bearing brunt of cost (lost funds, helpdesk, recovery costs)
  - But have little ability to detect or prevent these attacks
  - Primarily education campaigns, shutting down fake sites, 1.5 factor authentication
- Merchants often left holding the bag
  - No easy way to verify if credit card is fraudulent
  - Merchant gets charge back if transaction deemed fraudulent

High-Level Findings

Stakeholder Capabilities and Incentives Misaligned

- ISPs
  - Want to protect users' email
  - Don't want to be blacklisted for sending out spam / phish
  - One ISP estimated 10% of customers had malware
    - But still paying a monthly fee
    - Could quarantine, but customer service cost to reinstall OS high, but low benefit to ISP
    - At same time, end-users and ISPs creating negative externality on others due to lack of protection
  - ISPs are competitive market, and when cost is primary differentiating factor, quality suffers first

Privacy, Security, and Home Networking

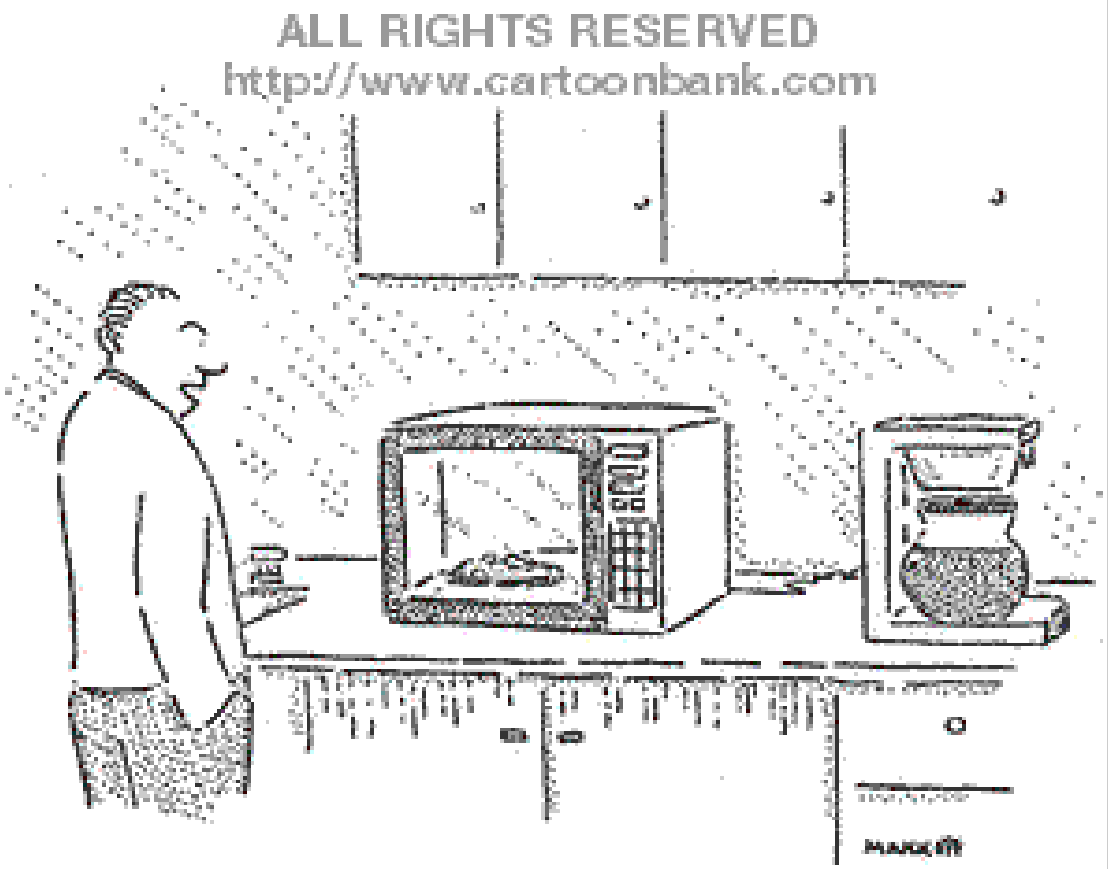
- Who is in best position? Who should bear the costs?
- How to have a unified, understandable experience?
  - Think volume control

- Software / hardware
  - Patches
  - Configuration
  - Viruses
  - Filters
- Data
  - Personal photos / videos
  - Media library
  - Files (taxes, mortgage)
  - Sensor data

- Stakeholders
  - End-users
  - Hardware manufacturers
  - ISPs
  - Application Developers
  - Services (e.g. Facebook)
  - Government
  - Law enforcement
  - Volunteers / Advocacy

Privacy, Security, and Home Networking

- What strategies to apply where?
  - Make it invisible (SSL, taking down fake sites, defaults)
  - Better interfaces
  - Train the end-users (mental models, common risks)
- Training / Knowledge / Helping each other
  - What do people know, and how did they learn it?
  - Understanding what the “norms” are and should be
    - Home networking not easily observable (in terms of what’s going on, and comparing myself to others)
    - Don’t know what others are doing, so don’t know if I am normal or not -> isitnormal.com
    - Web 2.0 approaches for helping people



"No, I don't want to play chess. I just want you to reheat the lasagna."