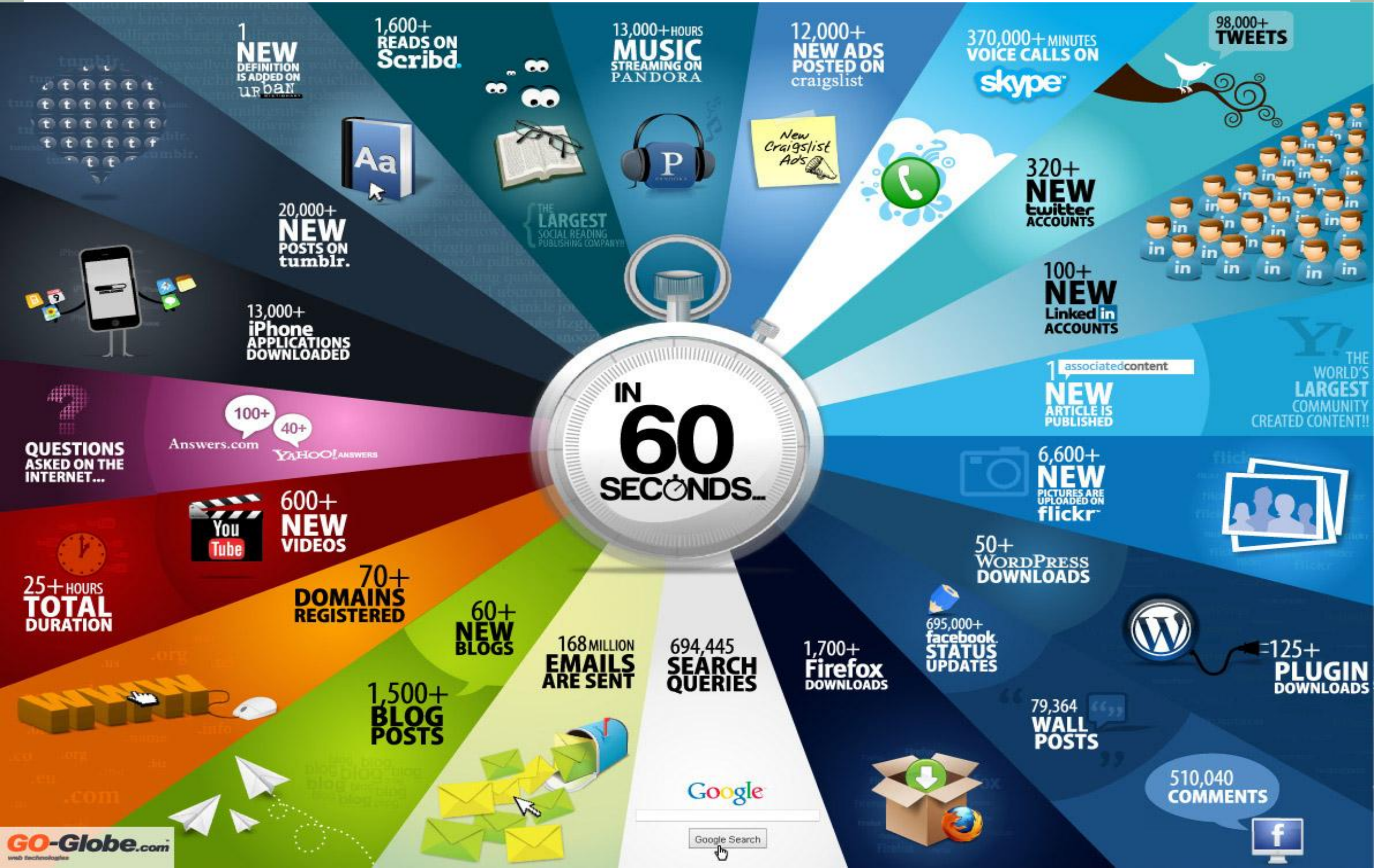
Security From 30,000 Feet: The Benefits of Multi-disciplinary Research

Shari Lawrence Pfleeger

I3P Research Director

March 2012

Most Systems Are Complex

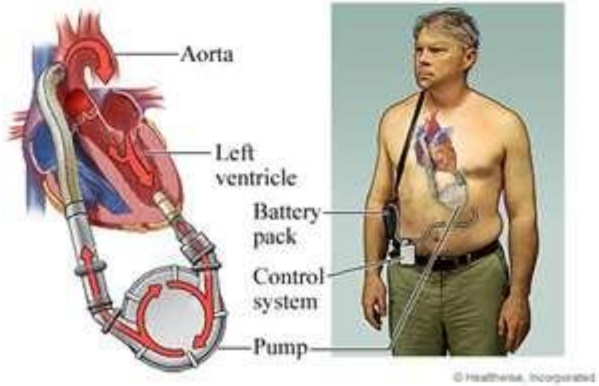


1 NEW DEFINITION IS ADDED ON urban
1,600+ READS ON Scribd.
13,000+ HOURS MUSIC STREAMING ON PANDORA
12,000+ NEW ADS POSTED ON craigslist
370,000+ MINUTES VOICE CALLS ON skype
98,000+ TWEETS
New Craigslist Ads
THE LARGEST SOCIAL READING PUBLISHING COMPANY!!
20,000+ NEW POSTS ON tumblr.
320+ NEW twitter ACCOUNTS
13,000+ iPhone APPLICATIONS DOWNLOADED
100+ NEW Linked in ACCOUNTS
IN 60 SECONDS...
1 associatedcontent NEW ARTICLE IS PUBLISHED
THE WORLD'S LARGEST COMMUNITY CREATED CONTENT!!
QUESTIONS ASKED ON THE INTERNET...
100+ Answers.com
40+ YAHOO! ANSWERS
6,600+ NEW PICTURES ARE UPLOADED ON flickr
You Tube
600+ NEW VIDEOS
25+ HOURS TOTAL DURATION
70+ DOMAINS REGISTERED
50+ WordPress DOWNLOADS
60+ NEW BLOGS
168 MILLION EMAILS ARE SENT
694,445 SEARCH QUERIES
1,700+ Firefox DOWNLOADS
695,000+ facebook STATUS UPDATES
125+ PLUGIN DOWNLOADS
1,500+ BLOG POSTS
79,364 WALL POSTS
510,040 COMMENTS
Google
Google Search
GO-Globe.com

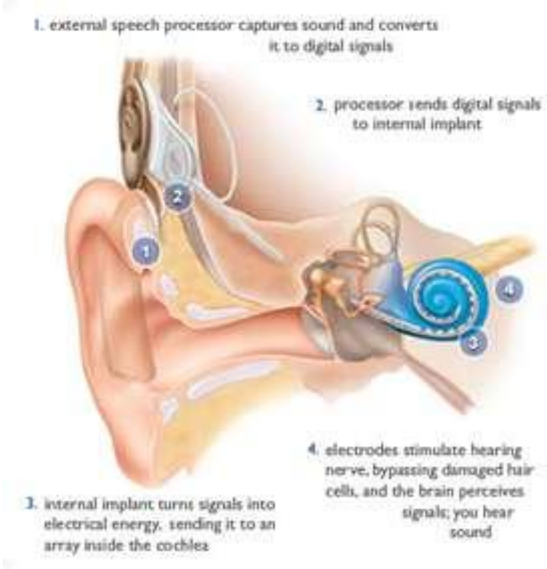
And Software Content is Growing

An automobile now has much more software in it than a Boeing 777!

Not to Mention Medical Devices …



© Healthwise, Incorporated


1. external speech processor captures sound and converts it to digital signals

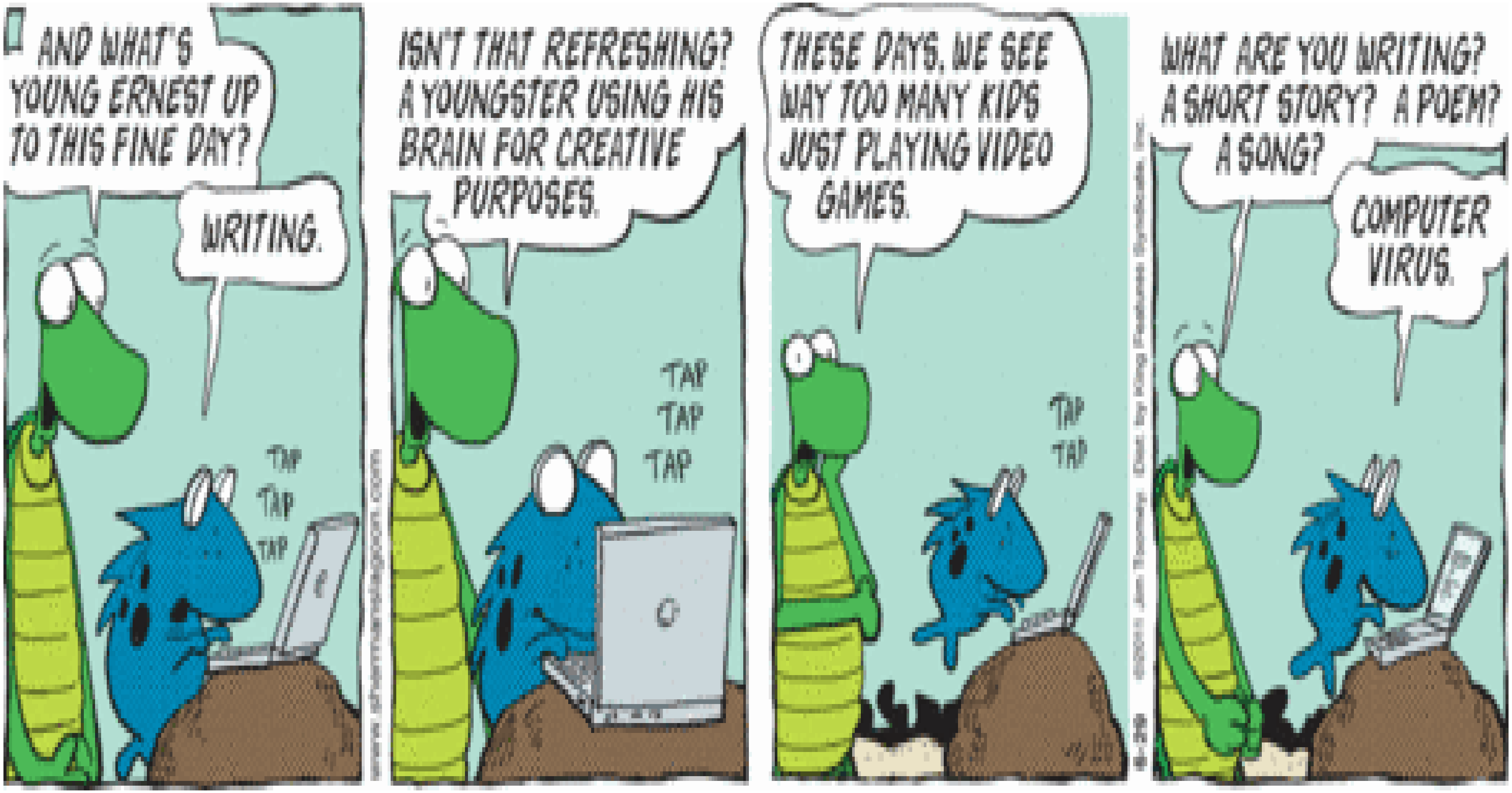
2. processor sends digital signals to internal implant

3. internal implant turns signals into electrical energy, sending it to an array inside the cochlea

4. electrodes stimulate hearing nerve, bypassing damaged hair cells, and the brain perceives signals; you hear sound

But We Do Not Always Design Well

And What Are People Doing on Our Networks?


AND WHAT'S YOUNG ERNEST UP TO THIS FINE DAY?
WRITING.
TAP TAP TAP
ISN'T THAT REFRESHING? A YOUNGSTER USING HIS BRAIN FOR CREATIVE PURPOSES.
TAP TAP TAP
THESE DAYS, WE SEE WAY TOO MANY KIDS JUST PLAYING VIDEO GAMES.
TAP TAP
WHAT ARE YOU WRITING? A SHORT STORY? A POEM? A SONG?
COMPUTER VIRUS.

Example: Car-hacking

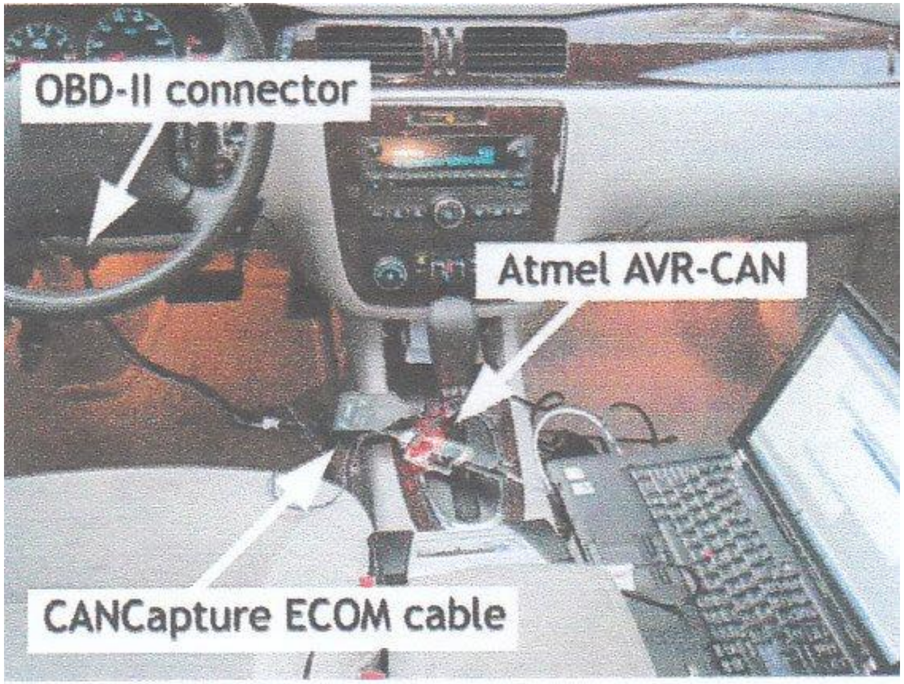
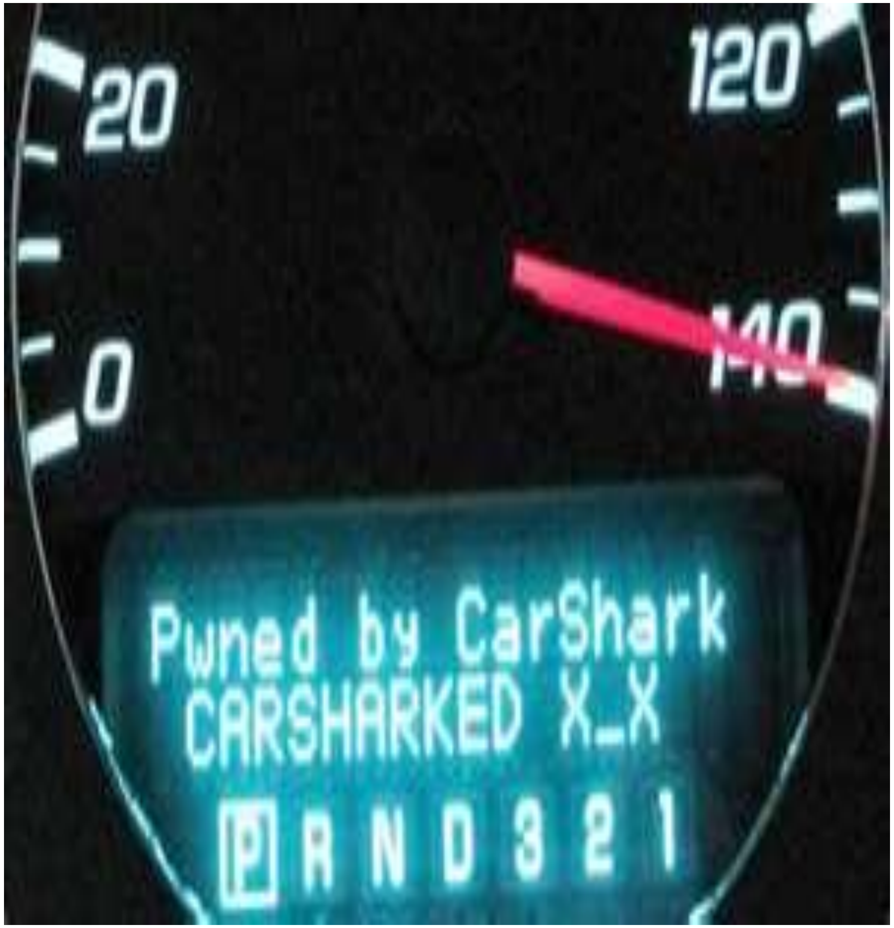


Figure 2. Example experimental setup. The laptop is running our custom CARSHARK CAN network analyzer and attack tool. The laptop is connected to the car's OBD-II port.



The View from Above

It’s not just technology. It’s

- Economics
- Psychology and sociology
- Business needs
- Legal constraints
- Ethical considerations
- And more

Examples

- Usability
- Insider Threat
- Cognition and incentives

- Application: Spear phishing

Usability

Consider basic functionality:

And Think About Context of Use

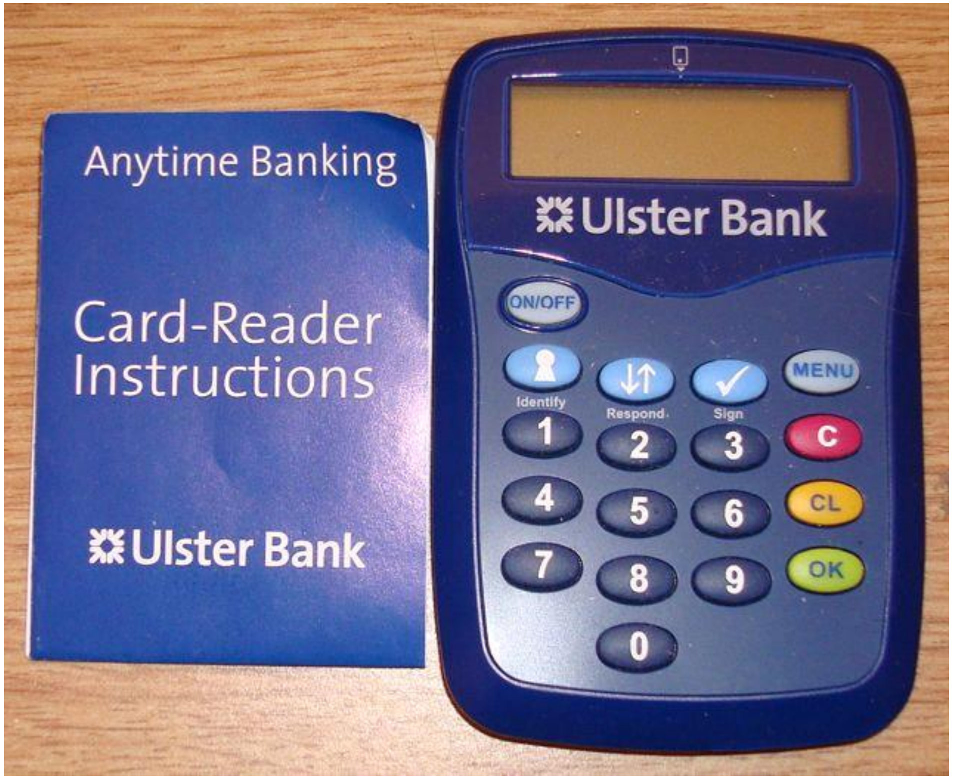
Usability Example: Ulster Bank

When you open an account, the bank sends you four things:

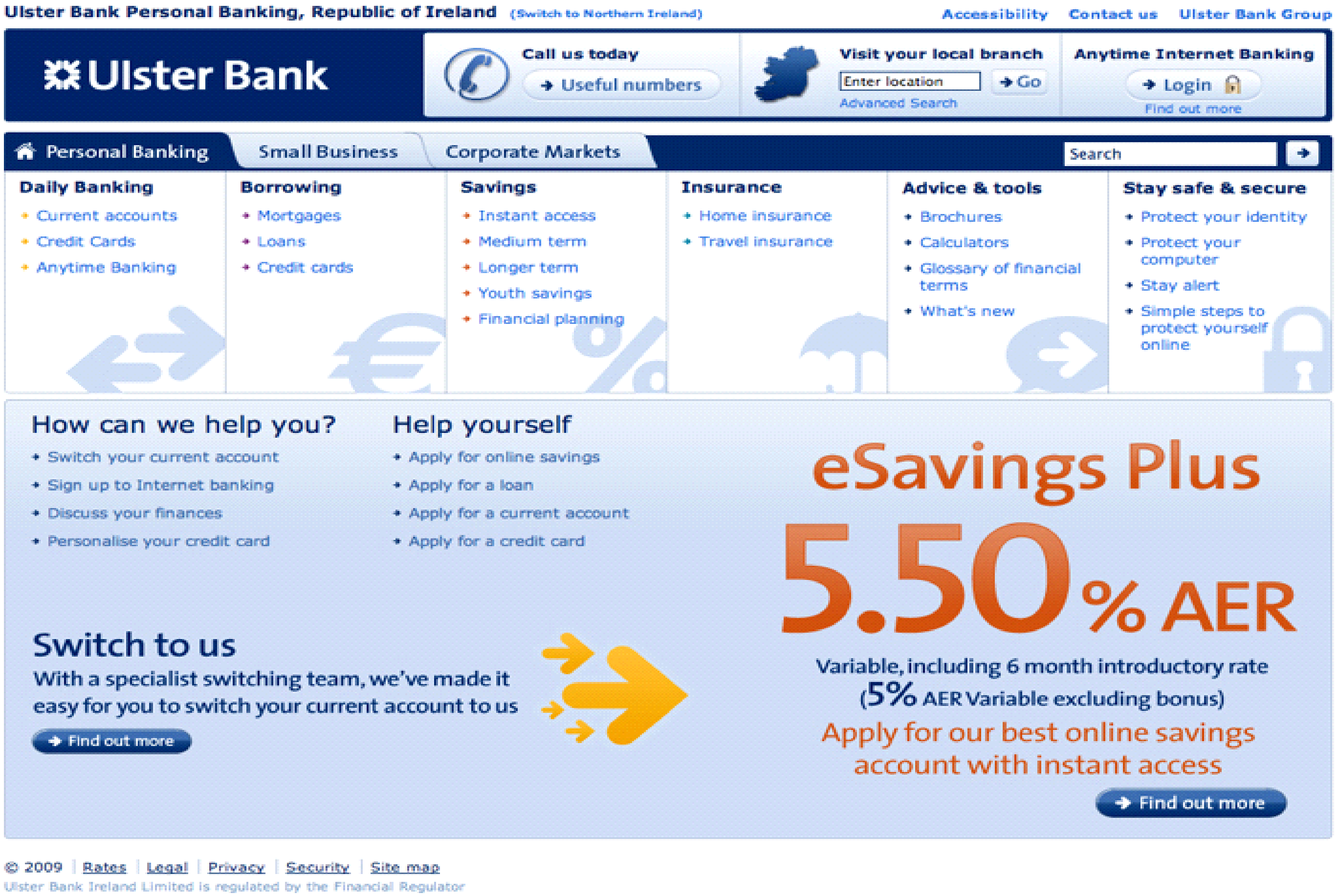
- A smartcard reader
- A separate letter with the actual smartcard
- A separate letter with a onetime PIN for the smartcard
- A separate letter with a onetime 10-digit activation code for the service

So How Do You Establish an Account?

There are several steps. First get out the card-reader and instructions.



Second Step: Go to the Online Site



Ulster Bank Personal Banking, Republic of Ireland (Switch to Northern Ireland)

Accessibility | Contact us | Ulster Bank Group

Call us today

→ Useful numbers

Visit your local branch

Enter location → Go

Advanced Search

Anytime Internet Banking

→ Login

Find out more

Daily Banking
- Current accounts
- Credit Cards
- Anytime Banking

Borrowing
- Mortgages
- Loans
- Credit cards

Savings
- Instant access
- Medium term
- Longer term
- Youth savings
- Financial planning

Insurance
- Home insurance
- Travel insurance

Advice & tools
- Brochures
- Calculators
- Glossary of financial terms
- What's new

Stay safe & secure
- Protect your identity
- Protect your computer
- Stay alert
- Simple steps to protect yourself online

How can we help you?
- Switch your current account
- Sign up to Internet banking
- Discuss your finances
- Personalise your credit card

Help yourself
- Apply for online savings
- Apply for a loan
- Apply for a current account
- Apply for a credit card

Switch to us

With a specialist switching team, we've made it easy for you to switch your current account to us

→ Find out more

eSavings Plus

5.50% AER

Variable, including 6 month introductory rate (5% AER Variable excluding bonus)

Apply for our best online savings account with instant access

→ Find out more

© 2009 | Rates | Legal | Privacy | Security | Site map

Ulster Bank Ireland Limited is regulated by the Financial Regulator

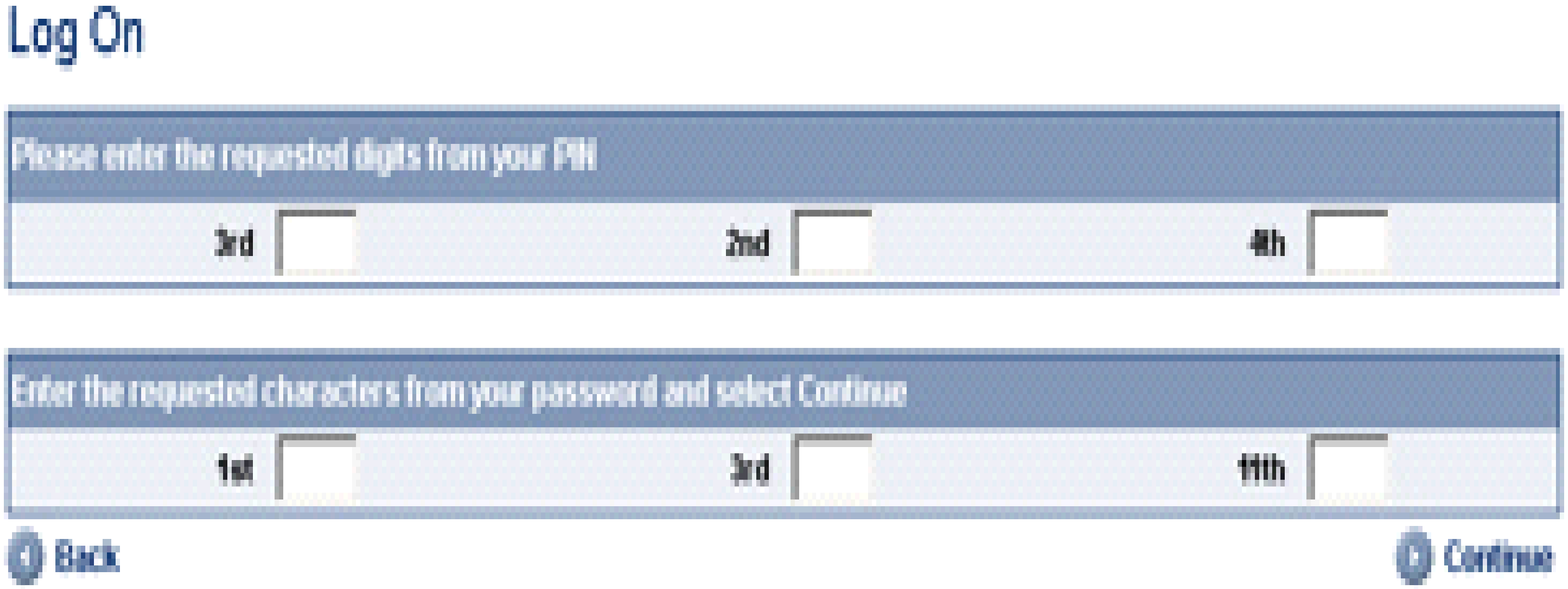
Next Steps

- Change the PIN on the smartcard.
- Enter your customer number.
- Enter your user ID.

So far, so good.

Enter Randomness

- Enter three digits from a different PIN.



Log On

Please enter the requested digits from your PIN

3rd □ 2nd □ 4th □

Enter the requested characters from your password and select Continue

1st □ 3rd □ 11th □

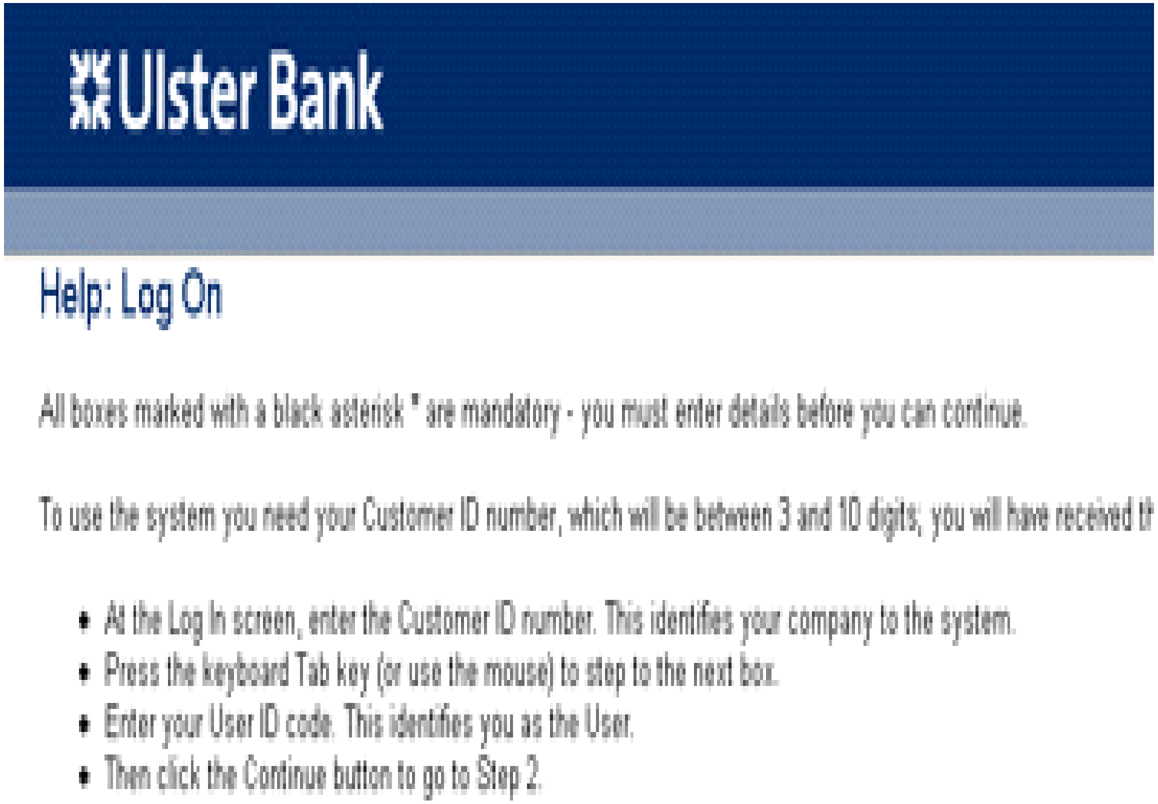
The first line asks for the third, second and fourth digits of your PIN, rather than the entire PIN; this sequence changes each time you log in.

Even More Steps

- Enter a new PIN.
- Enter a new password.
- Enter your activation code.

Help!

There is a Help function, but it does not go into enough detail.



Ulster Bank

Help: Log On

All boxes marked with a black asterisk * are mandatory - you must enter details before you can continue.

To use the system you need your Customer ID number, which will be between 3 and 10 digits, you will have received t

- At the Log In screen, enter the Customer ID number. This identifies your company to the system.
- Press the keyboard Tab key (or use the mouse) to step to the next box.
- Enter your User ID code. This identifies you as the User.
- Then click the Continue button to go to Step 2.

Insider Threat

- What do we mean by an insider?
- What kinds of insider actions put organizations or their resources at some risk?
- What can we do to reduce the risk of threatening insider actions?

Who is an Insider?

- **Insider:** *A person with legitimate access to an organization's computers and networks.*
- Examples:
  - Employees
  - Students
  - Contractors
  - Auditors
  - Temporary business partner

What is an Insider Threat?

An insider’s action that puts at risk an organization’s data, processes, or resources in a disruptive or unwelcome way.

Framework for Understanding the Threat

- The organization
- The system
- The individual
- The environment

The Organization

- Defines legitimate access
- Decides to whom to give access
- Defines security policies
  - De facto policy vs. de jure policy
- Declares goals and strategies
- Encourages an organizational culture
  - What is tolerated
  - What is encouraged

The System

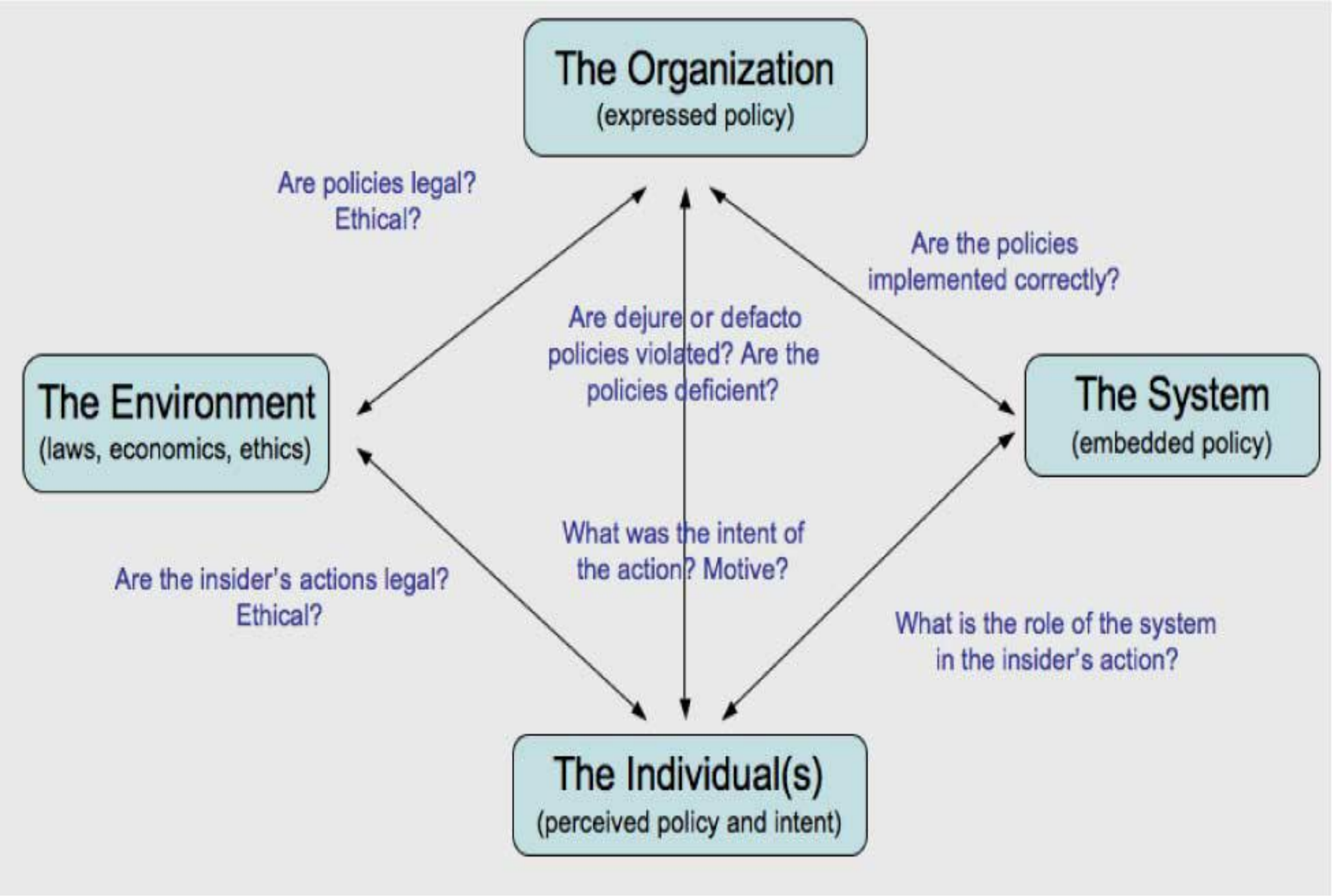
- Physical access control
- Interaction with other systems
- Implements policies (correctly?)
- Three cases:
  - The system is not involved (e.g. stealing money from the till)
  - The system is the object of the behavior (e.g. a logic bomb or denial of service)
  - The system enables the threat

The Individual

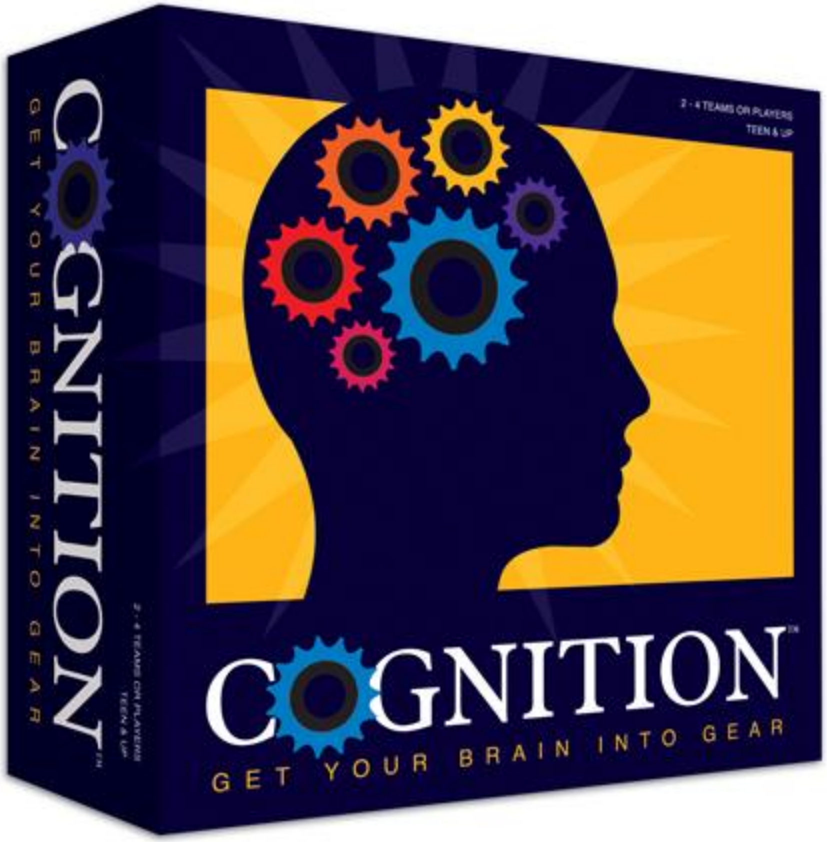
- Not a new notion: employee deviance
- Intent matters: malicious vs. non-malicious
- Motivation matters, too:
  - Derives from inside the organization? The organization has choices for prevention or deterrence
  - Derives from outside the organization? Few choices

The Environment

- Laws
- Regulations
- Ethics
- Organizational rules and customs
  - Example: choosing not to report a breach


The Organization
(expressed policy)
Are policies legal? Ethical?
Are the policies implemented correctly?
Are dejure or defacto policies violated? Are the policies deficient?
The Environment
(laws, economics, ethics)
The System
(embedded policy)
What was the intent of the action? Motive?
Are the insider's actions legal? Ethical?
What is the role of the system in the insider's action?
The Individual(s)
(perceived policy and intent)

Cognition

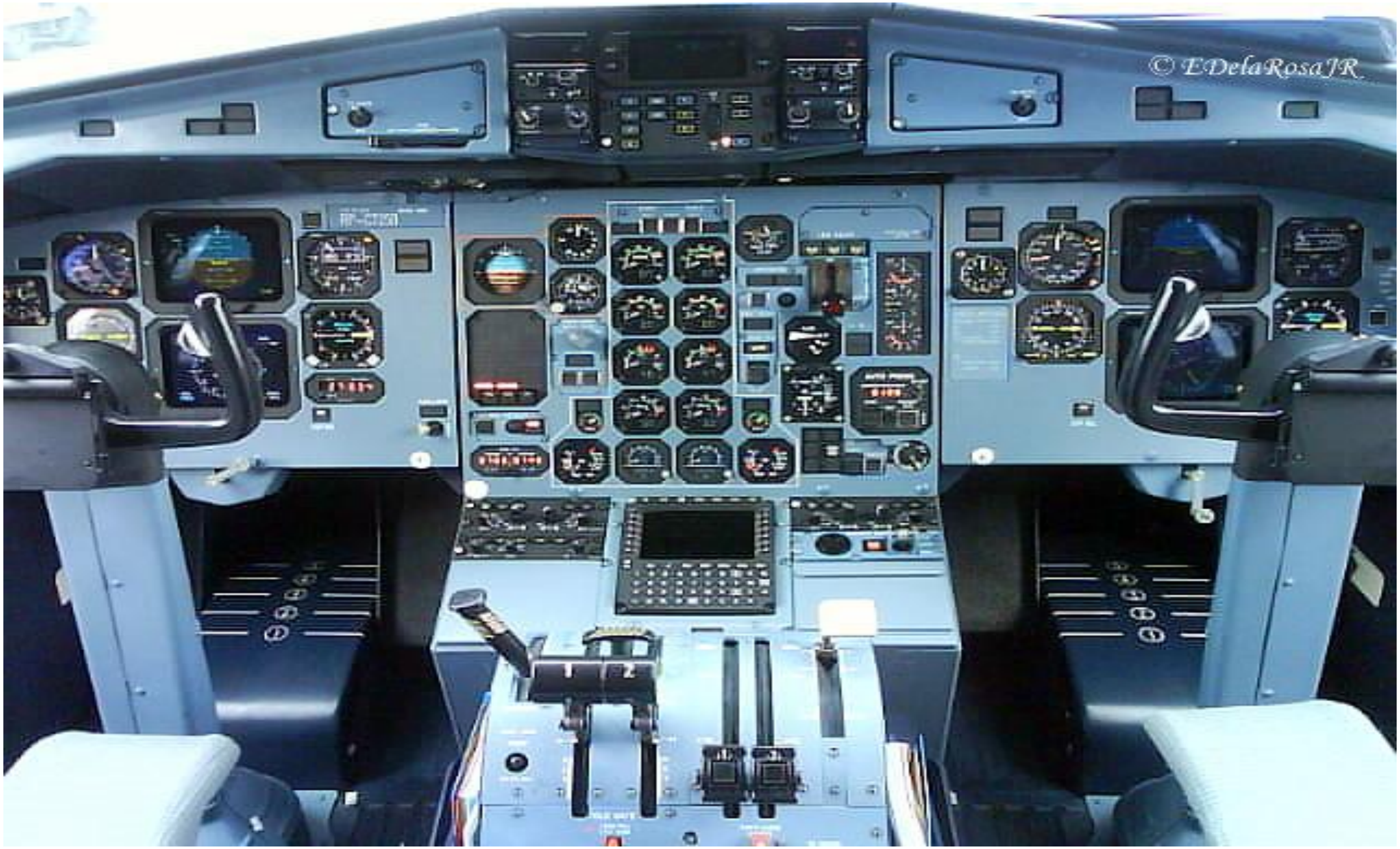

2 - 4 TEAMS OR PLAYERS
TEEN & UP
COGNITION™
GET YOUR BRAIN INTO GEAR

We Can’t Multi-Task

- Primary task vs. secondary task
  - Inattentional blindness
  - Rewards for primary task
- Information overload
  - George Miller: 7 +- 2
  - Intel no-email day
  - Gary Klein: Recognition-primed decision-making

Is This Reasonable?

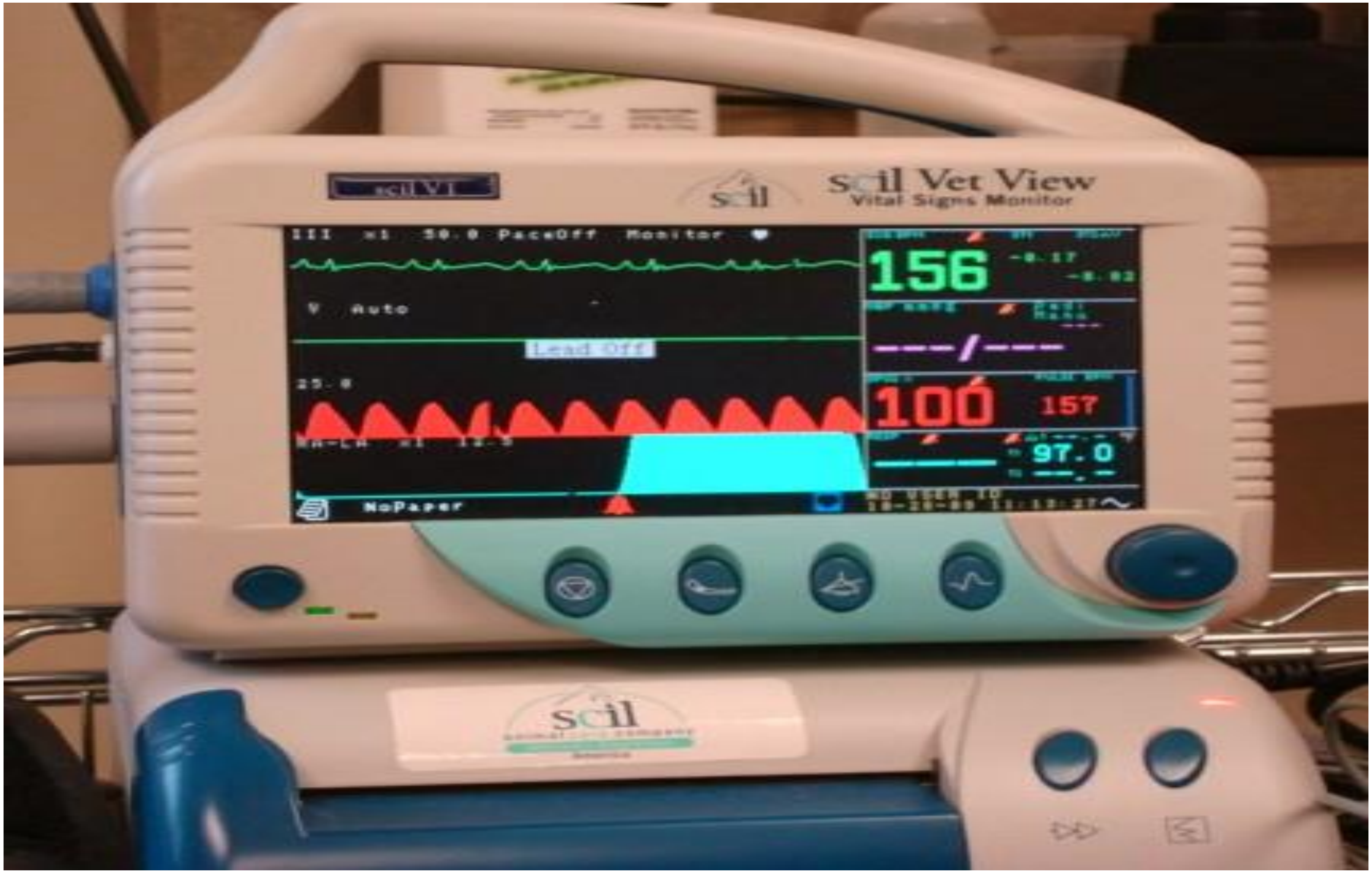
Is This Information Overload?



TMI?

Is This an Improvement?

Is This Better?



Add Other Cognition Effects to the Mix

- Based on experiences
  - Recency effect
  - Status quo bias
  - Recognition better than recollection
  - Interference
  - Identifiable victim effect
- Framing effects
- Confirmation bias
- Bystander effect

Understand the Nature of Trust

Example: Tenner (1991) describes how trust in technology leads to riskier behaviors

Metaphors and Understanding

Incentives Can Help

- Reminders: How often? How much information?
- Incentives to encourage good "security hygiene"

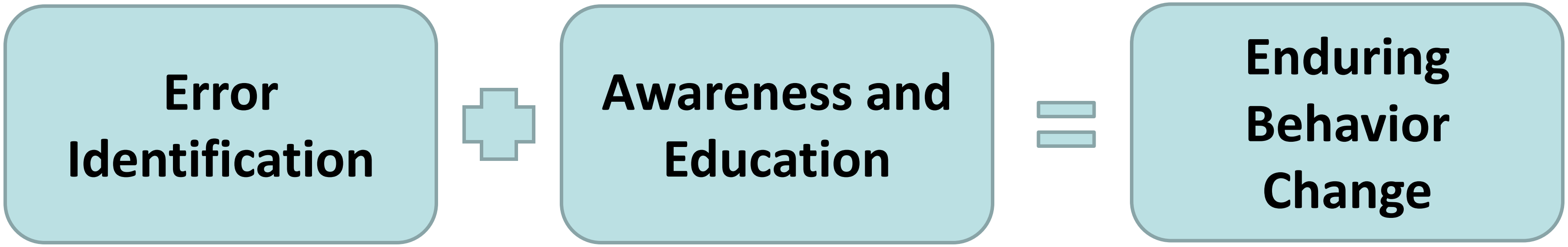
Example: Spear Phishing Studies

- Spear-phishing is a *targeted* form of email phishing.
  - Someone plausible (employer, colleague, associate) seems to be sending the email.
  - Seemingly legitimate topic
  - Urgency of a response: “Just click on link or open attachment”

Example: Spear Phishing Studies

- Why do people click?
  - No red flags, curiosity, haste, illusion of invulnerability
  - "It's not my problem – it's Security's problem."
- What do we want users to do?
  - Think before clicking
  - Know what to do instead of clicking
  - Report if they click

Changing Behavior



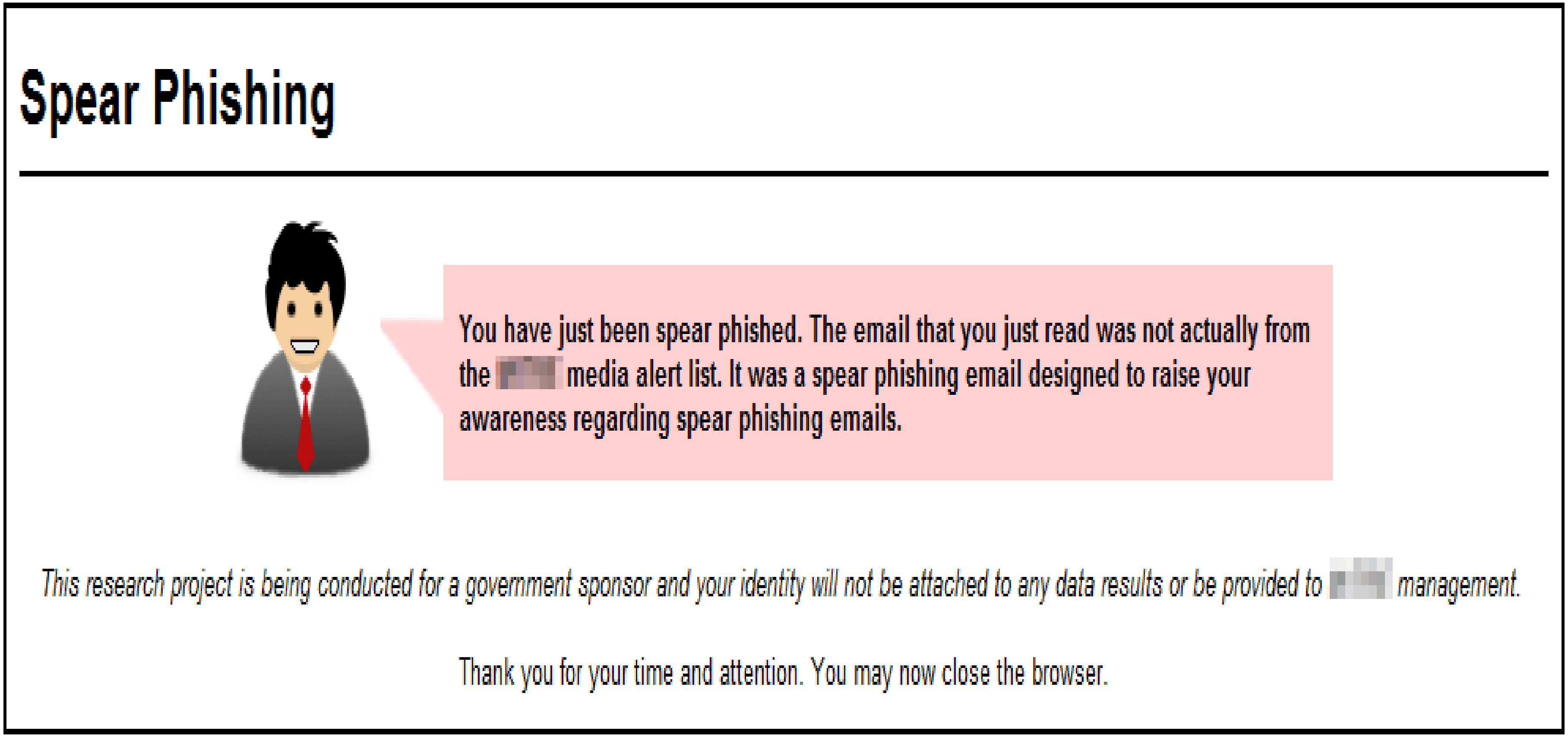
Error Identification + Awareness and Education = Enduring Behavior Change

Hypothesis

If users are provided with training *immediately following* an error in judgment, then they will be less likely to make the same error later, when presented with a similar judgment.

Multiple Frames

- Gain vs. loss
- Individual vs. group



Spear Phishing

You have just been spear phished. The email that you just read was not actually from the [redacted] media alert list. It was a spear phishing email designed to raise your awareness regarding spear phishing emails.

This research project is being conducted for a government sponsor and your identity will not be attached to any data results or be provided to [redacted] management.

Thank you for your time and attention. You may now close the browser.

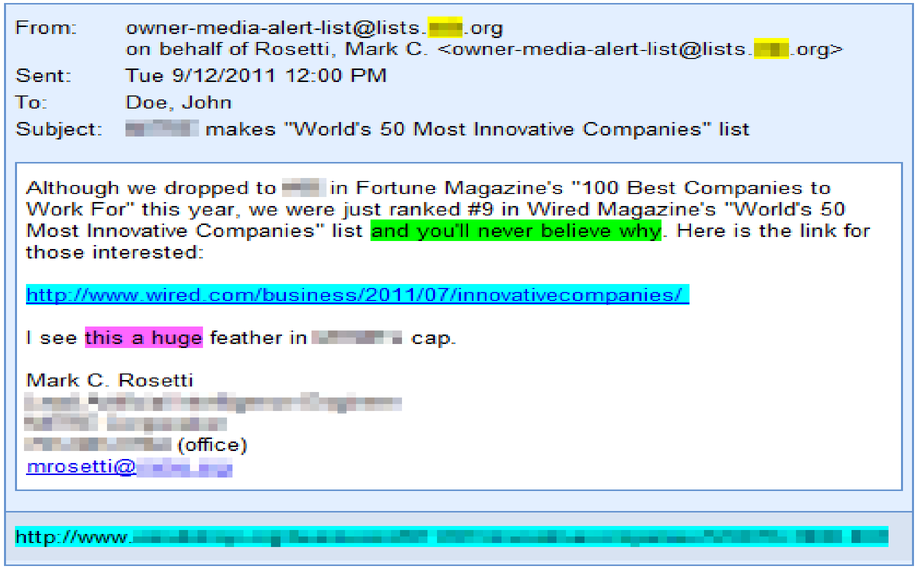
How to Defend against

Spear Phishing

<u>You have just been spear phished!</u> **The email that you just read was not actually from the [redacted] media alert list. It was a spear phishing email designed to help you learn how to protect your co-workers from cyber attackers.**

How could you have recognized the spear phishing email you just received?

Spear phishing emails seem professional and legitimate. However, there are several ways to recognize them:



From: owner-media-alert-list@lists.[redacted].org
on behalf of Rosetti, Mark C. <owner-media-alert-list@lists.[redacted].org>
Sent: Tue 9/12/2011 12:00 PM
To: Doe, John
Subject: [redacted] makes "World's 50 Most Innovative Companies" list

Although we dropped to [redacted] in Fortune Magazine's "100 Best Companies to Work For" this year, we were just ranked #9 in Wired Magazine's "World's 50 Most Innovative Companies" list and you'll never believe why. Here is the link for those interested:

http://www.wired.com/business/2011/07/innovativecompanies/

I see this a huge feather in [redacted] cap.

Mark C. Rosetti
[redacted]
[redacted] (office)
mrosetti@[redacted]

http://www.[redacted]

Mismatch between name and address in "From:" field

Motivation to take immediate action

Links don't match status bar when mouse is hovered over

Typos, improper grammar, odd spacing

Intuition - overall feeling that something isn't right

1. What is spear phishing?

Spear phishing is a form of cyber attack attempting to infiltrate your system or organization for cyber crime or espionage purposes. Such cyber attackers find inside information specifically relevant to you and craft fake email messages, usually impersonating well-known companies, trusted relationships, or contexts. In order for the attack to succeed, it requires that you take action. For example, by clicking on a link in the email message you could install malicious software on your system.

2. What do your co-workers stand to save when you don't fall for spear phishing attempts?

By not clicking on links within spear phishing emails your co-workers save three things:

1. **Identity** - Your co-workers save their identity because cyber attackers can't access sensitive details (e.g., logins, passwords, etc.) from their systems.
2. **Time** - Your co-workers save their time because their systems won't have to be wiped and then restored with the last backup.
3. **Data** - Your co-workers save data because cyber attackers can't steal sensitive information from their systems.

3. What are simple ways to protect your co-workers?

There are several easy things that you can do to protect your co-workers from spear phishing attacks:

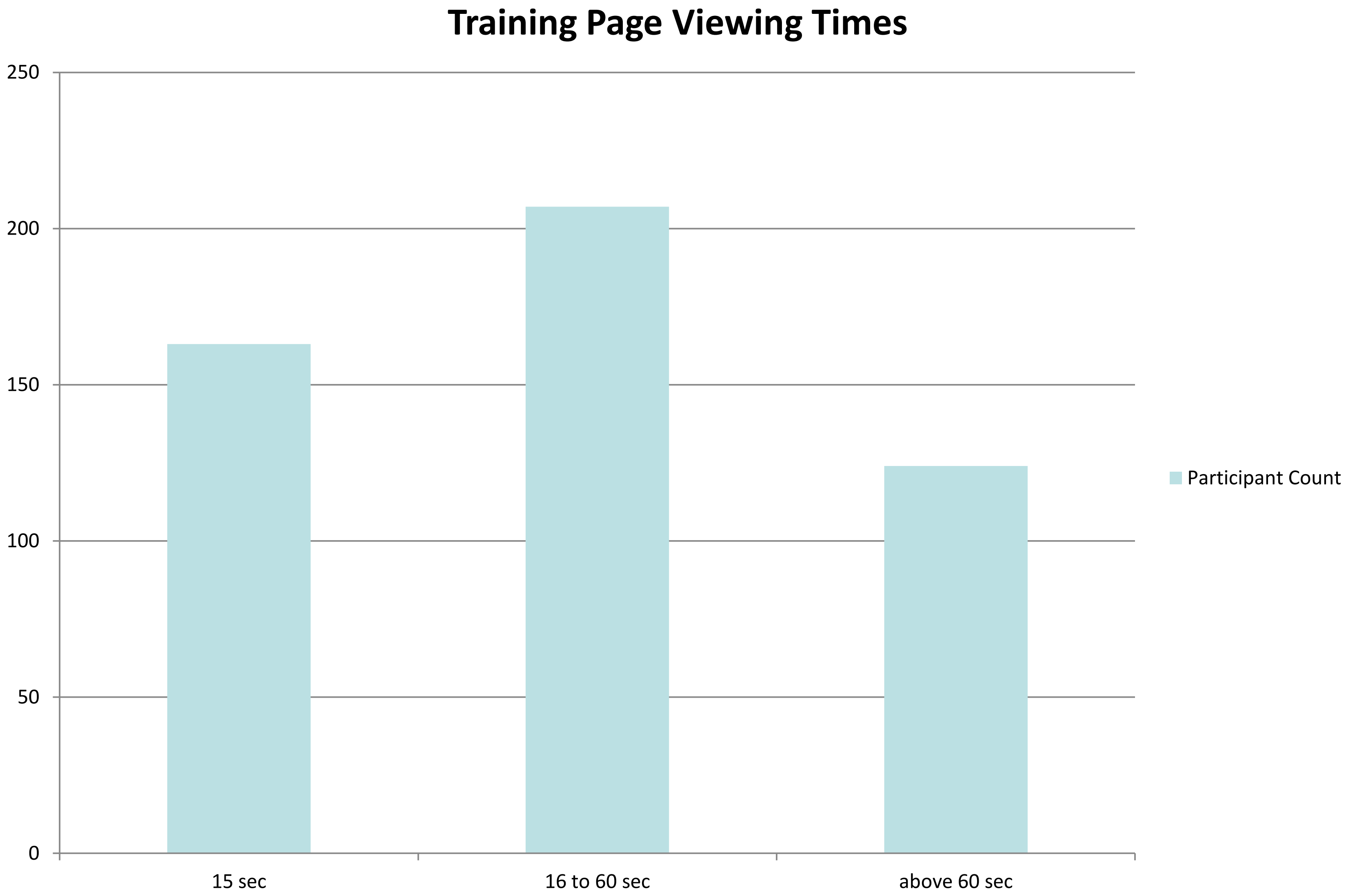
- **Never click on unanticipated links or attachments** within emails or forward/reply to emails asking for private information.
- **Always verify contact information** by going directly to the source (i.e., using official phone numbers, emails, and websites instead of those provided).
- **Report suspicious emails immediately** by calling the Help Desk, especially if you have clicked on the links provided.

This research project is being conducted for a government sponsor and your identity will not be attached to any data results or be provided to [redacted] management. For more comprehensive [redacted] awareness material on spear phishing, [redacted].

Thank you for your time and attention. Now that you have finished the training please close the browser.

Results?

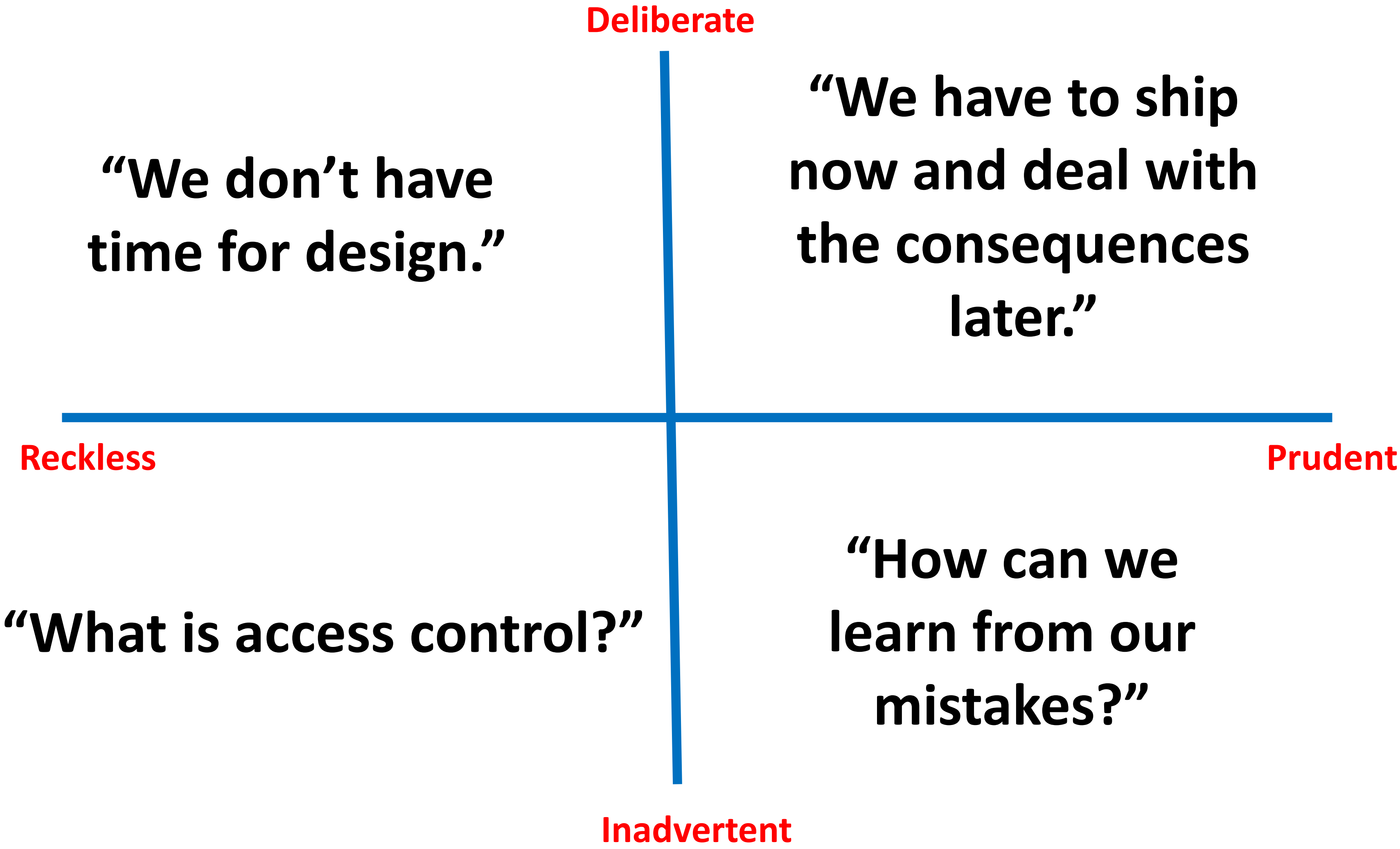
- Good news:
  - 98 (7%) of participants clicked on none of the three trials
  - What are they doing right? Oblivious, lucky, or smart?
- Bad news:
  - 146 (10%) of participants clicked on all three trials
  - Will any training affect this group?


Training Page Viewing Times
250
200
150
100
50
0
15 sec
16 to 60 sec
above 60 sec
Participant Count

What Should We Do?

First, Examine Your Current Approach

(Source: Gunnar Peterson)



Deliberate

Reckless

Prudent

Inadvertent

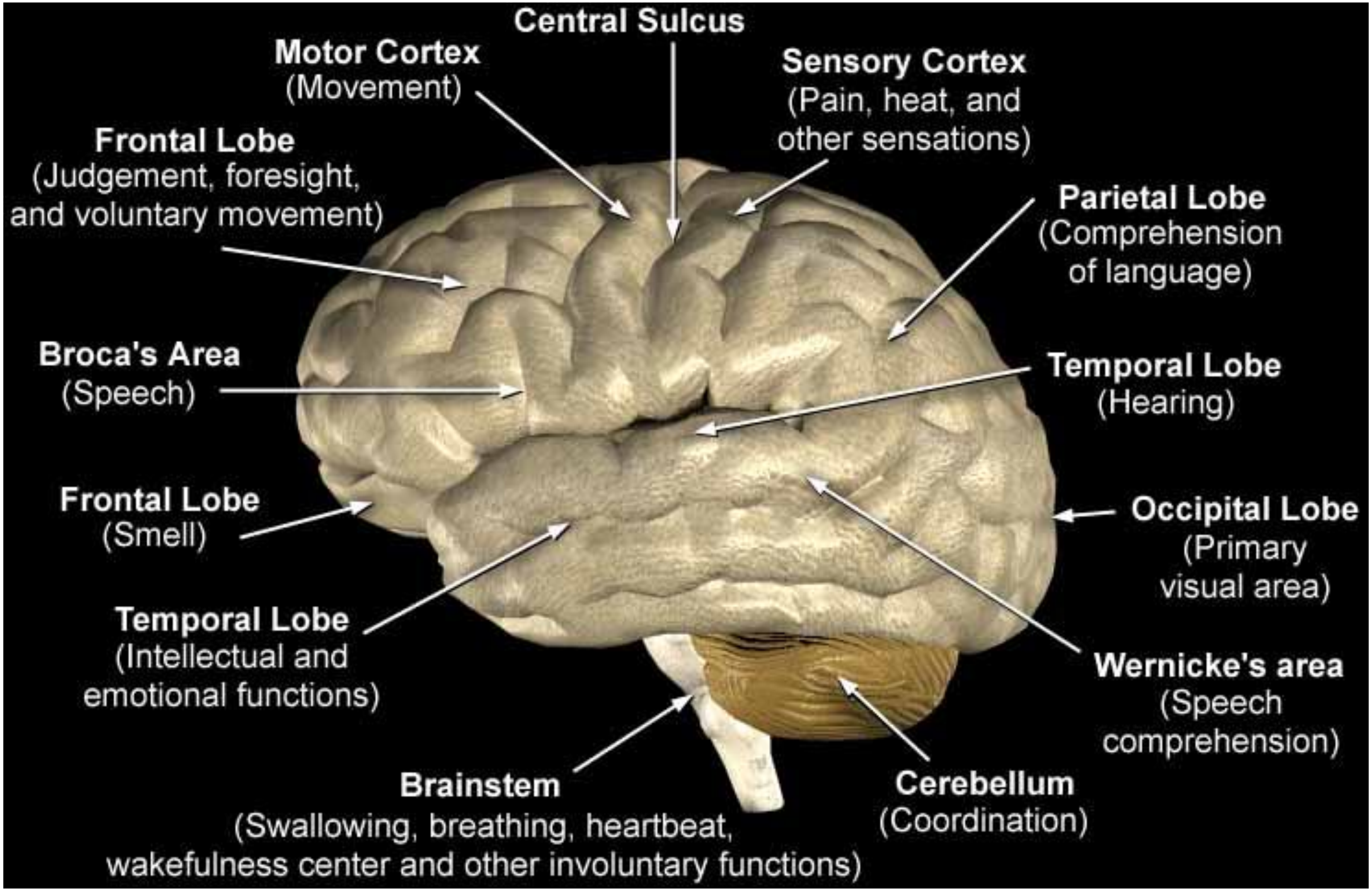
"We don't have time for design."

"We have to ship now and deal with the consequences later."

"What is access control?"

"How can we learn from our mistakes?"

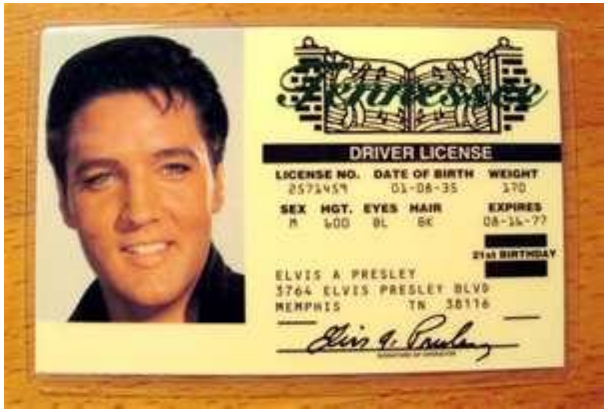
Next, Pay Attention to This


Central Sulcus
Motor Cortex (Movement)
Sensory Cortex (Pain, heat, and other sensations)
Frontal Lobe (Judgement, foresight, and voluntary movement)
Parietal Lobe (Comprehension of language)
Broca's Area (Speech)
Temporal Lobe (Hearing)
Frontal Lobe (Smell)
Occipital Lobe (Primary visual area)
Temporal Lobe (Intellectual and emotional functions)
Wernicke's area (Speech comprehension)
Brainstem (Swallowing, breathing, heartbeat, wakefulness center and other involuntary functions)
Cerebellum (Coordination)

Example: Opt-in vs. Opt-out

Agreeing to organ donation during drivers' license registration:

- In Germany and the US: opt-in
  - – Result? About 14% of drivers are organ donors
- In Poland and France: opt-out
  - – Result? About 90% of drivers are organ donors



Tennessee

DRIVER LICENSE

LICENSE NO.	DATE OF BIRTH	WEIGHT
2571459	01-08-35	170

SEX	HGT.	EYES	HAIR	EXPIRES
M	600	BL	BK	08-16-77

21st BIRTHDAY

ELVIS A PRESLEY
3764 ELVIS PRESLEY BLVD
MEMPHIS TN 38116

Elvis A. Presley

Account for Human Variation

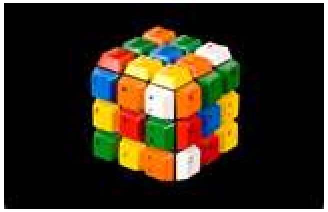
Especially Novice, Master, Expert

Account for Cognitive Load

And Have Realistic Expectations

What to Do? (1 of 2)

- Requirements
  - Include significant user-sensible, testable requirements that reflect how people perceive and react
- Design
  - User-centered design that can be prototyped and evaluated
- Testing
  - Simulations
  - Tests in real situations with variety of users: novices, masters, experts



What to Do? (2 of 2)

- Evolution
  - Look at trouble tickets, other evidence of use and consequences, and redesign according to what you learn.
- Include behavioral scientists on development, evaluation and maintenance teams
  - Or at least train your developers to be sensitive to human perception and action.

For More Information (1 of 2)

- Gary Klein, *Sources of Power: How People Make Decisions*, M Press, 1998.
- Deborah Mayo and Rachelle Hollander, *Acceptable Evidence*: *Science and Values in Risk Management*, Oxford University Press, 1991.
- George Miller, “The Magical Number Seven, Plus or Minus Two: Some Limits on Our Capacity for Processing Information,” *Psychological Review*, vol. 63, 1956, pp. 81-97.
- Shari Lawrence Pfleeger et al., “Insiders Behaving Badly: Addressing Bad Actors and Their Actions,” *IEEE Transactions on Information Forensics and Security*, March 2010, pp. 169-179.
- Peter Sandman, “Understanding the Risk: What Frightens Rarely Kills,” Nieman Reports, Nieman Foundation for Journalism, Harvard University, Spring 2007.

For More Information (2 of 2)

- Daniel Simons and Christopher Chabris, “Gorillas in Our Midst: Sustained Inattentional Blindness for Dynamic Events,” *Perception*, 1999, vol. 28, pp. 1059-1074.
- P. Slovic, B. Fischhoff and S. Lichtenstein, “Facts and Fears: Understanding Perceived Risk,” in R. Schwing & W. Albers (Eds.), *Societal Risk Assessment,* New York: Plenum Press, 1980, pp. 67-93.
- Nassim Talib, *The Black Swan: The Impact of the Highly Improbable*, Random House, 2007.
- Edward Tenner, *Why Things Bite Back: Technology and the Revenge of Unintended Consequences*, Vintage Press, 1991.