The Johnny 2 Standardized Secure Messaging Scenario

Simson L. Garfinkel

MIT Computer Science and Artificial Intelligence Laboratory

`http://www.simson.net/`

Standardized Scenarios can improve HCI-SEC research.

Data from different experiments can be explored.

Better understand the impact of changing a single variable.

Lowers cost of experimentation: New experiments don’t need to “reinvent the wheel.”

Similar to using software libraries or design patterns.

Cognitive Science has standardized scenarios to measure “Risk Propensity” [Brockhaus, 1980], emotional response to threatening situations [Holff & Maple, 1982], driver performance, etc.

“Why Johnny Can’t Encrypt” [Whitten and Tygar, 99] is the classic HCI-SEC reference.

Great Scenario:

- Subject plays the role of a political campaign worker.
- Encryption used to protect email from opposing campaign.
- Scenario tests usability of PGP for making keys and exchanging encrypted mail.

Why Johnny Can’t Encrypt:
A Usability Evaluation of PGP 5.0

Alma Whitten
School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213
alma@cs.cmu.edu

J. D. Tygar[1]
EECS and SIMS
University of California
Berkeley, CA 94720
tygar@cs.berkeley.edu

Abstract

User errors cause or contribute to most computer security failures, yet user interfaces for security still tend to be clumsy, confusing, or near-nonexistent. Is this simply due to a failure to apply standard user interface design techniques to security? We argue that, on the contrary, effective security requires a different usability standard, and that it will not be achieved through the user interface design techniques appropriate to other types of consumer software.

To test this hypothesis, we performed a case study of a security program which does have a good user interface by general standards: PGP 5.0. Our case study used a cognitive walkthrough analysis together with a laboratory user test to evaluate whether PGP 5.0 can be successfully used by cryptography novices to achieve effective electronic mail security. The analysis found a number of user interface design flaws that may contribute to security failures, and the user test demonstrated that when our test participants were given 90 minutes in which to sign and encrypt a message using PGP 5.0, the majority of them were unable to do so successfully.

We conclude that PGP 5.0 is not usable enough to provide effective security for most computer users, despite its attractive graphical user interface, supporting our hypothesis that user interface design for effective security remains an open problem. We close with a brief description of our continuing work on the development and application of user interface design principles and techniques for security.

1 Introduction

Security mechanisms are only effective when used correctly. Strong cryptography, provably correct protocols, and bug-free code will not provide security if the people who use the software forget to click on the encrypt button when they need privacy, give up on a communication protocol because they are too confused about which cryptographic keys they need to use, or accidentally configure their access control mechanisms to make their private data world-readable. Problems such as these are already quite serious: at least one researcher [2] has claimed that configuration errors are the probable cause of more than 90% of all computer security failures. Since average citizens are now increasingly encouraged to make use of networked computers for private transactions, the need to make security manageable for even untrained users has become critical [4, 9].

This is inescapably a user interface design problem. Legal remedies, increased automation, and user training provide only limited solutions. Individual users may not have the resources to pursue an attacker legally, and may not even realize that an attack took place. Automation may work for securing a communications channel, but not for setting access control policy when a user wants to share some files and not others. Employees can be required to attend training sessions, but home computer users cannot.

Why, then, is there such a lack of good user interface design for security? Are existing general user interface design principles adequate for security? To answer these questions, we must first understand what kind of usability security requires in order to be

[1] Also at Computer Science Department, Carnegie Mellon University (on leave).

Johnny as described doesn’t work as a standardized scenario.

- *Johnny* didn’t have an attacker.
- *Johnny* didn’t use third-party certification.
  (It used email answerback certification.)
- *Johnny* didn’t have a control.
- Different subjects got different messages.

Johnny’s results are qualitative, not quantitative.

The Johnny 2 Scenario:

It’s based on *Johnny*, except:

- The personas are developed
- There are good guys and bad guys
- The bad guys are trying to spoof the experimental subject.

Cryptography can be used for both *authentication* and *privacy*.

Disclosed cast of characters

Maria Page

Campaign Manager (Your Boss)

Paul Butler

Campaign Finance Manager

Ben Donnelly

Paul's Assistant IT Manager

Sara Carson

Graphics Designer

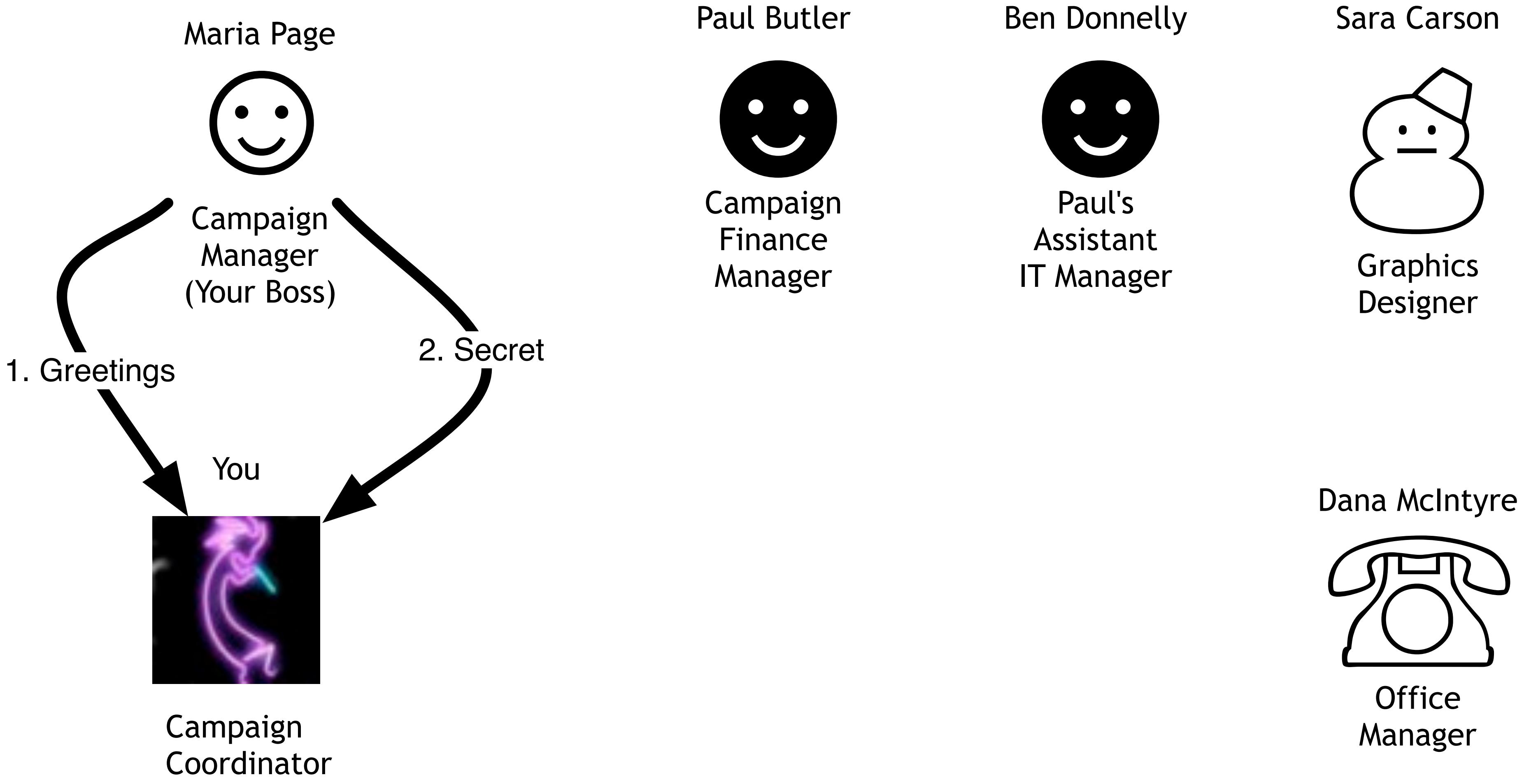
You

Campaign Coordinator

Dana McIntyre

Office Manager

Message 1 & 2: Introduction



Maria Page

Campaign Manager (Your Boss)

1. Greetings

2. Secret

You

Campaign Coordinator

Paul Butler

Campaign Finance Manager

Ben Donnelly

Paul's Assistant IT Manager

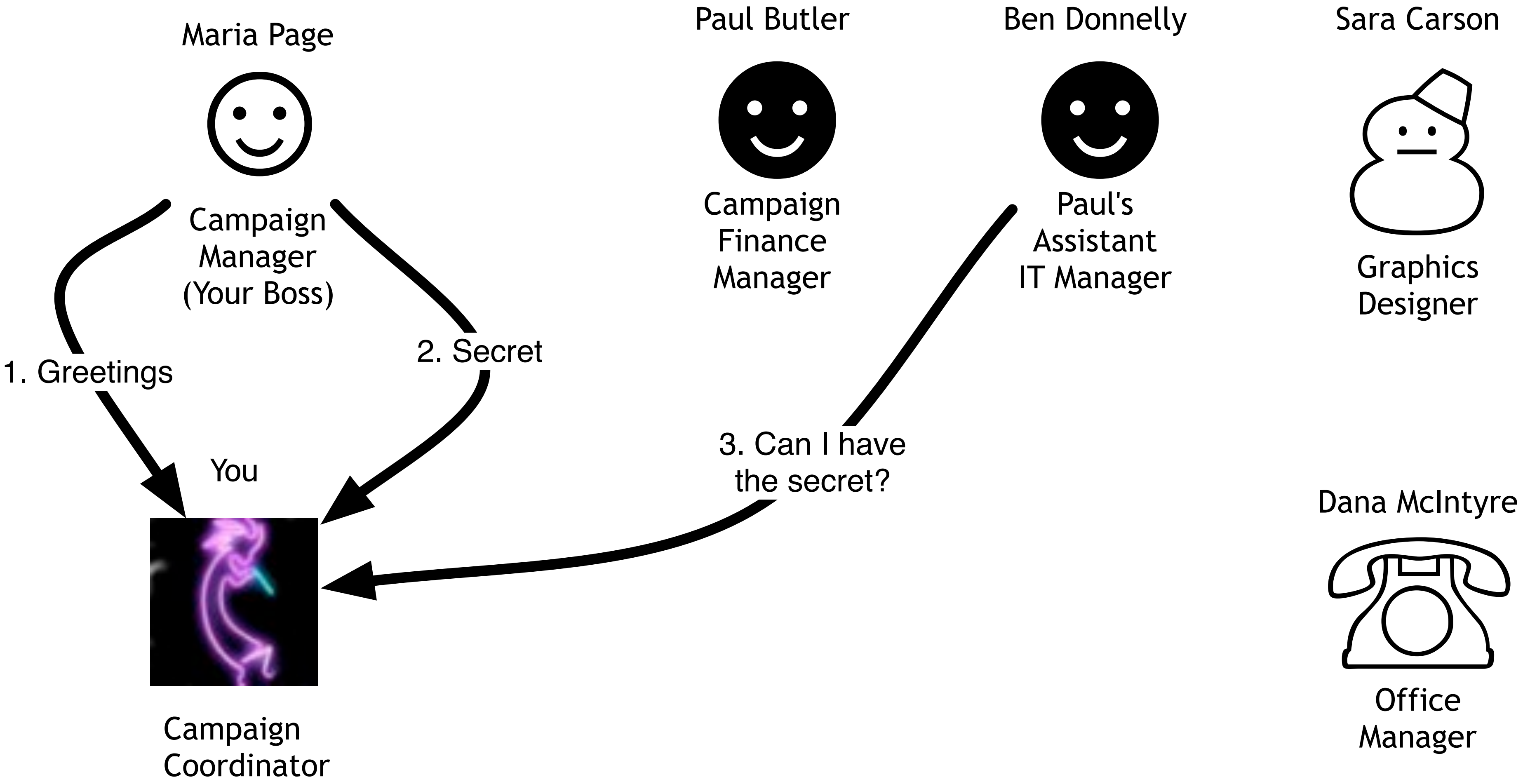
Sara Carson

Graphics Designer

Dana McIntyre

Office Manager

Message 3: Ben wants the secret



Maria Page

Campaign Manager (Your Boss)

Paul Butler

Campaign Finance Manager

Ben Donnelly

Paul's Assistant IT Manager

Sara Carson

Graphics Designer

1. Greetings

2. Secret

3. Can I have the secret?

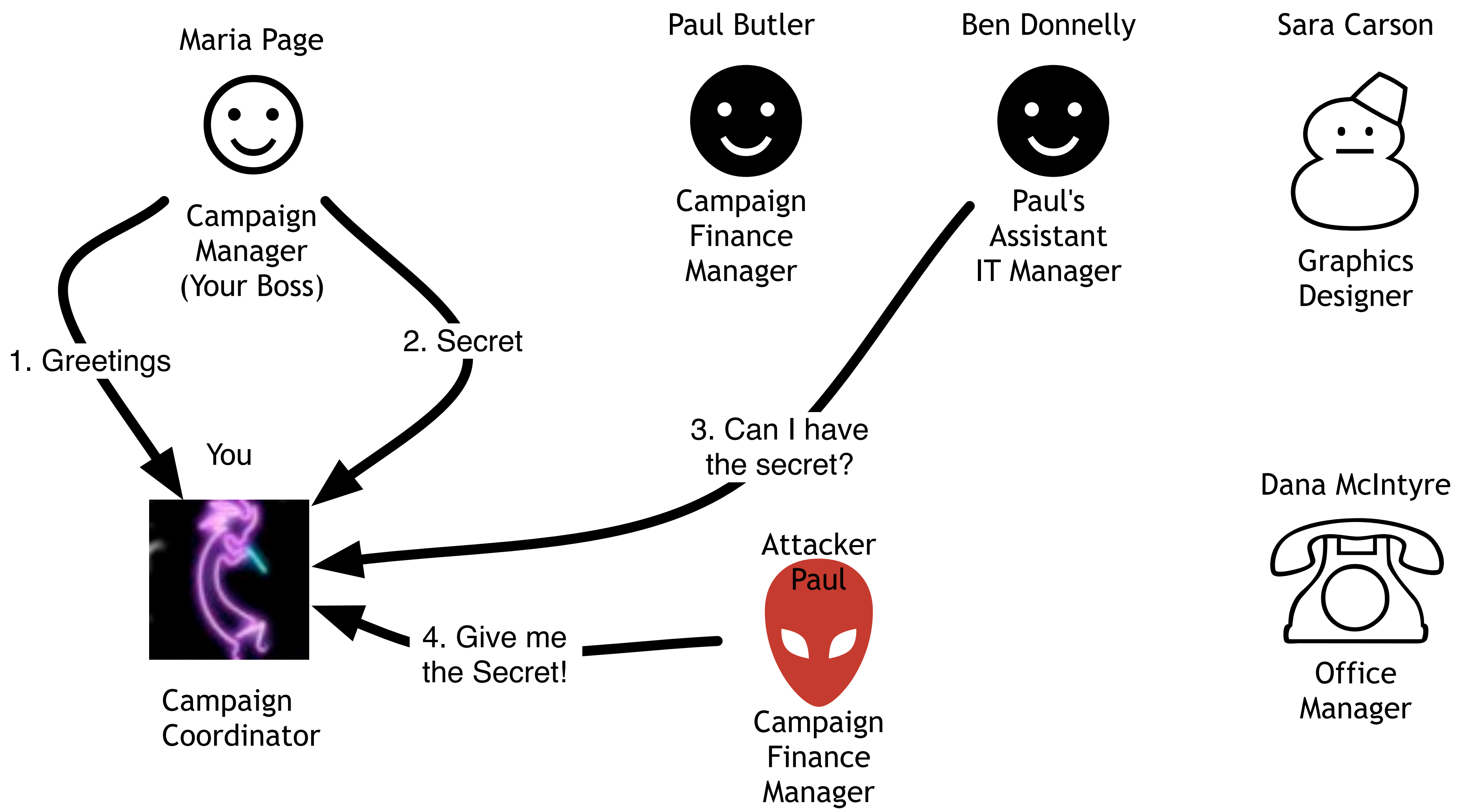
You

Campaign Coordinator

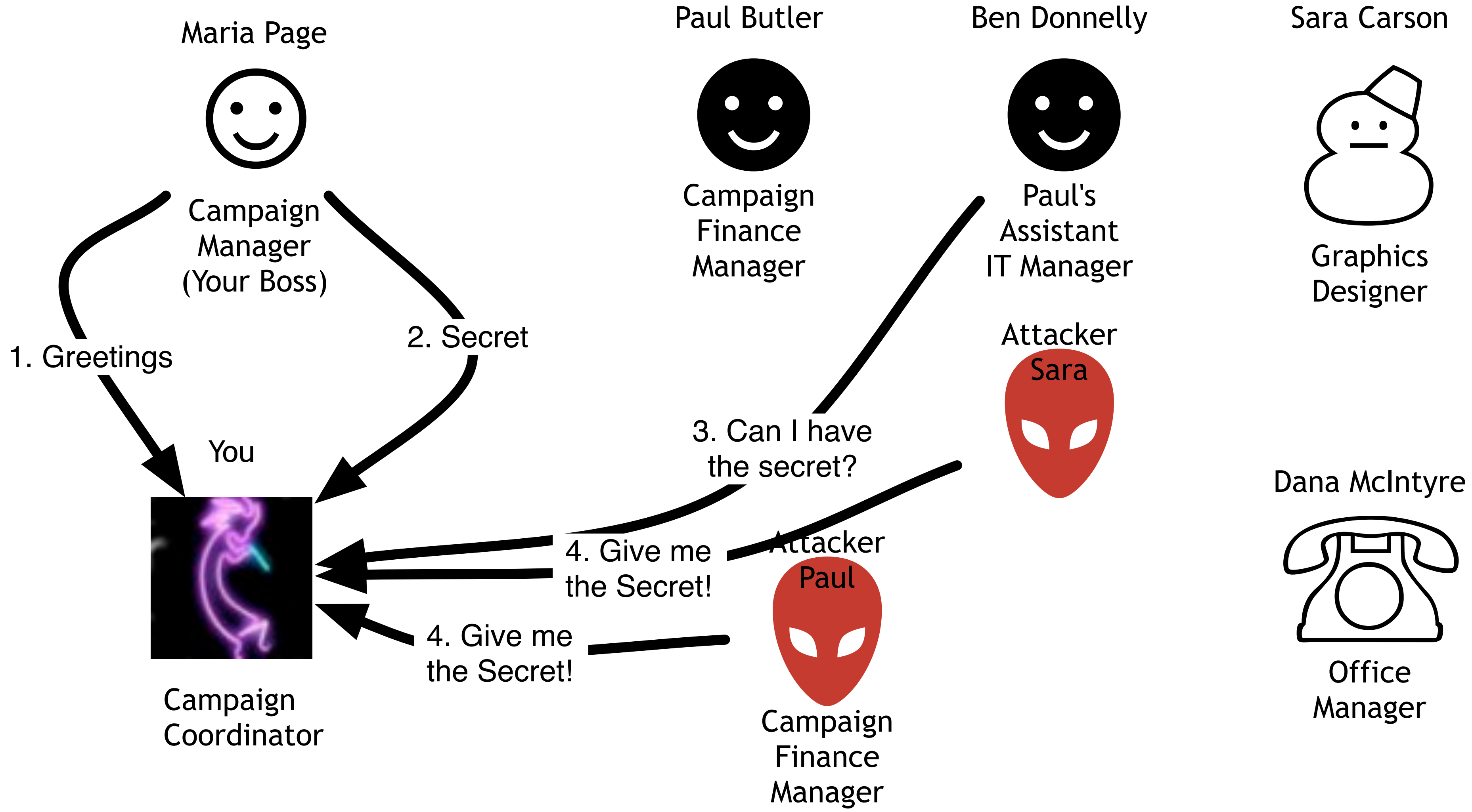
Dana McIntyre

Office Manager

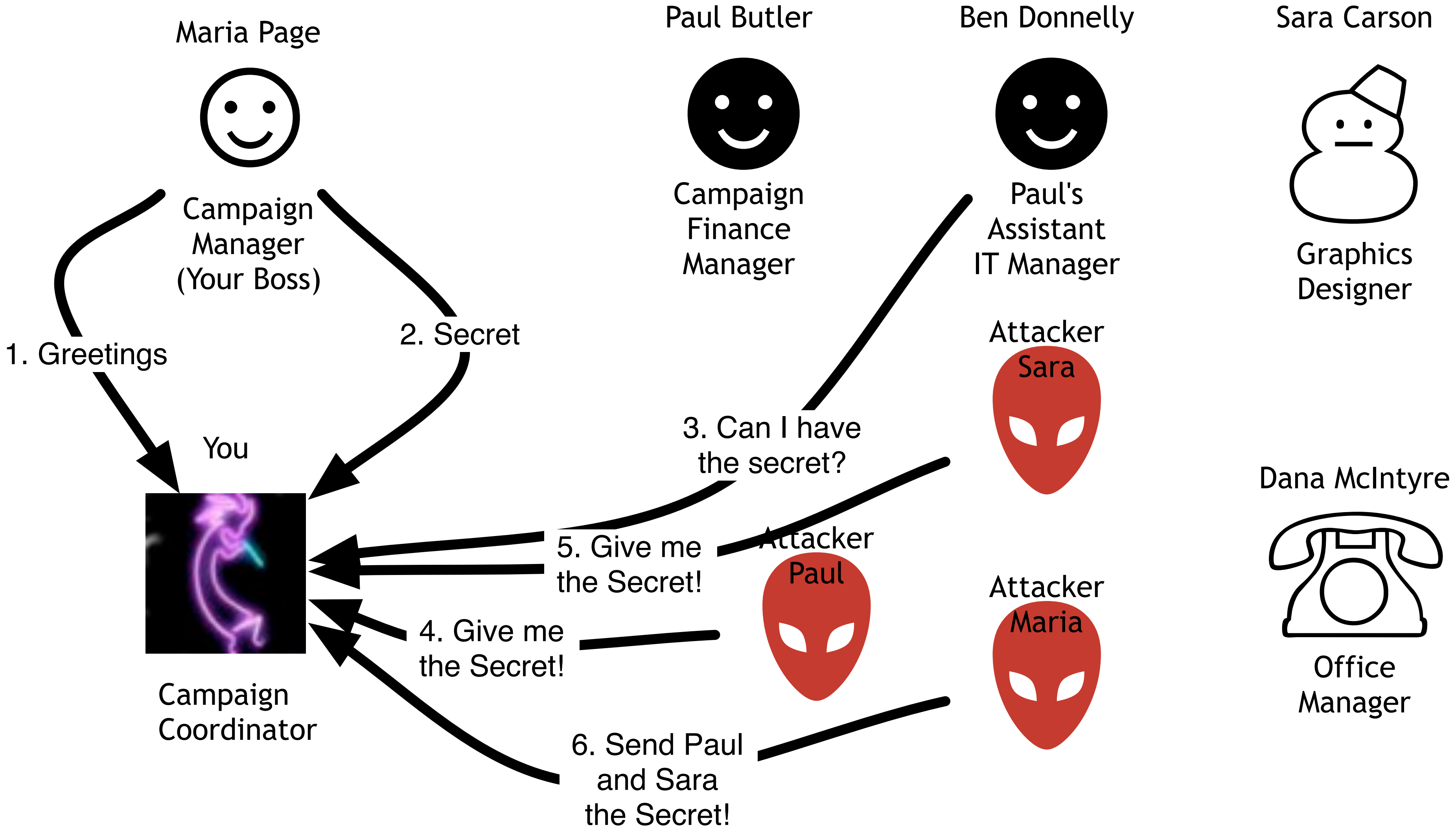
Message 4: Attack by “Paul”



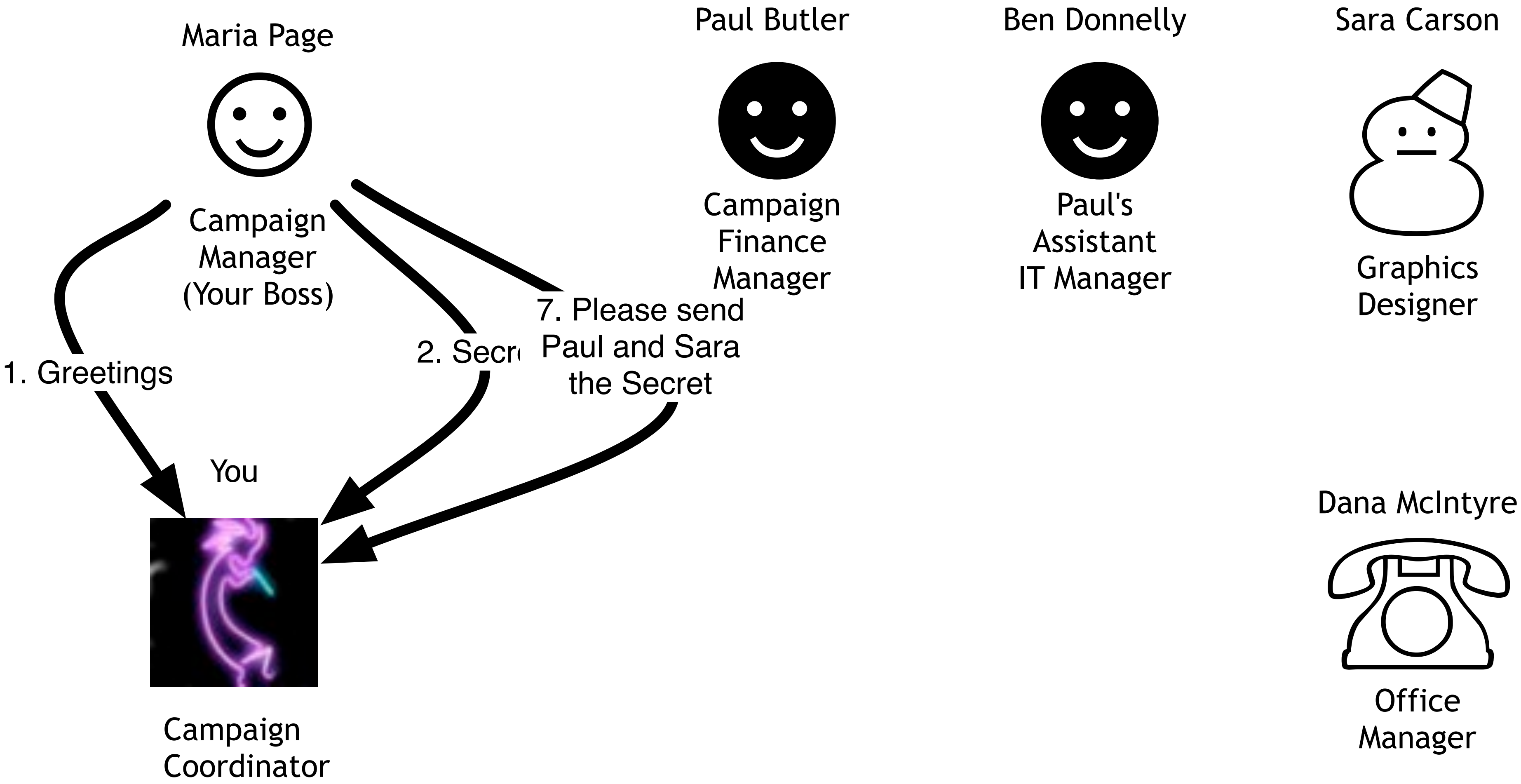
Message 5: Attack by “Sara”



Message 6: Attack by “Maria”



Message 7: Sara says “send the secret.”



Maria Page

Campaign Manager (Your Boss)

Paul Butler

Campaign Finance Manager

Ben Donnelly

Paul's Assistant IT Manager

Sara Carson

Graphics Designer

1. Greetings

2. Secr

7. Please send Paul and Sara the Secret

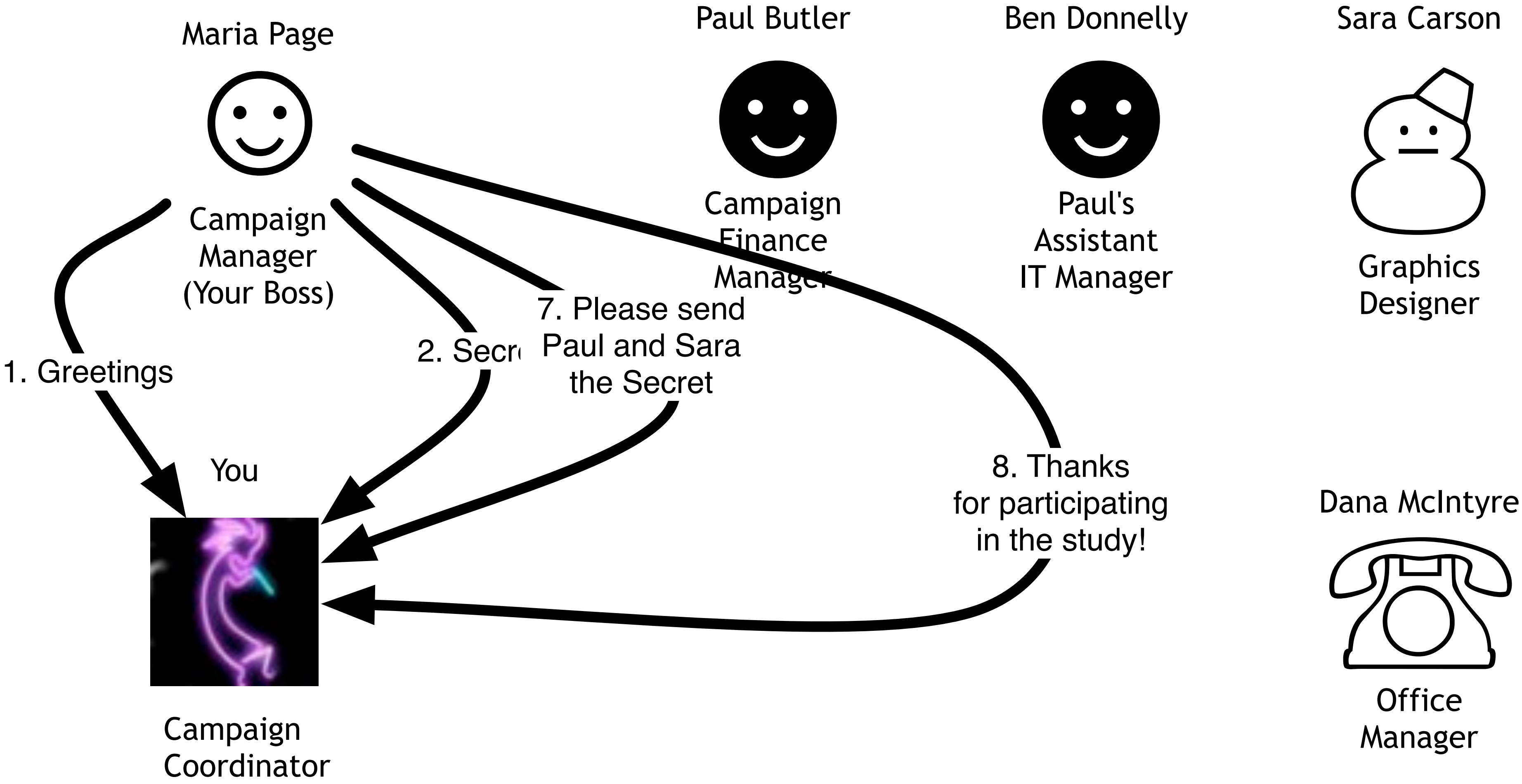
You

Campaign Coordinator

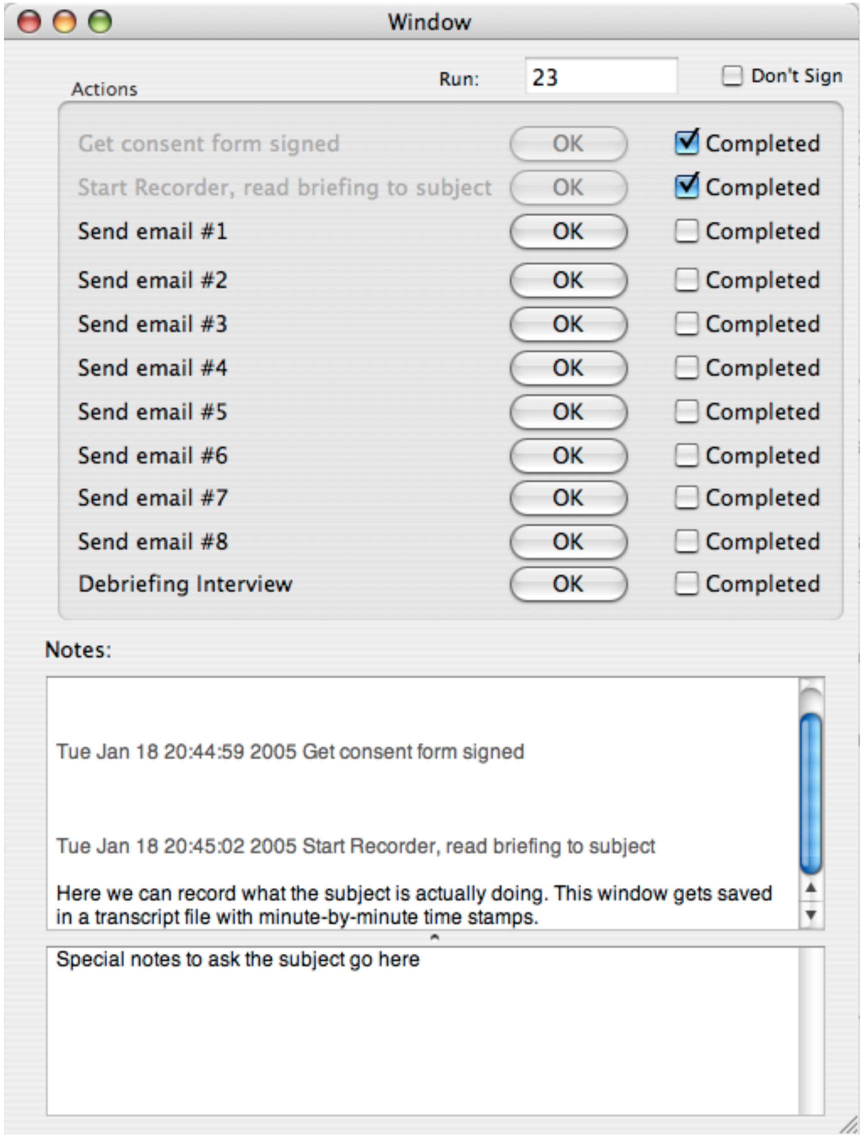
Dana McIntyre

Office Manager

Message 8: Thanks for playing



The Experimenter’s Workbench



Run: 23 □ Don't Sign

Actions

Get consent form signed	OK	☑ Completed
Start Recorder, read briefing to subject	OK	☑ Completed
Send email #1	OK	□ Completed
Send email #2	OK	□ Completed
Send email #3	OK	□ Completed
Send email #4	OK	□ Completed
Send email #5	OK	□ Completed
Send email #6	OK	□ Completed
Send email #7	OK	□ Completed
Send email #8	OK	□ Completed
Debriefing Interview	OK	□ Completed

Notes:

Tue Jan 18 20:44:59 2005 Get consent form signed

Tue Jan 18 20:45:02 2005 Start Recorder, read briefing to subject

Here we can record what the subject is actually doing. This window gets saved in a transcript file with minute-by-minute time stamps.

Special notes to ask the subject go here

Using Multiple Cohorts with Johnny 2

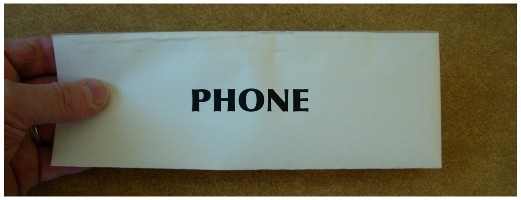
Experiment with:

- Briefing
- Interface
- Background Knowledge / training

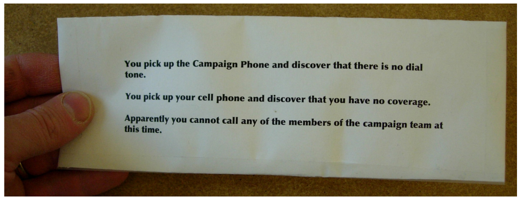
What’s in the Kit? Handouts and MIT_IRB directories:

Briefings for users

Phone:



PHONE



You pick up the Campaign Phone and discover that there is no dial tone.

You pick up your cell phone and discover that you have no coverage.

Apparently you cannot call any of the members of the campaign team at this time.

Recruitment Poster

Screening email

IRB application and consent form

Protocol

Running the Experiment:

`certs/`: Tools for creating S/MIME-signed messages

`exp/`: `message[1-8].html`, `sendmessage`, `send_signed.py_`

`setup checklist.rtf` — How to set up the system

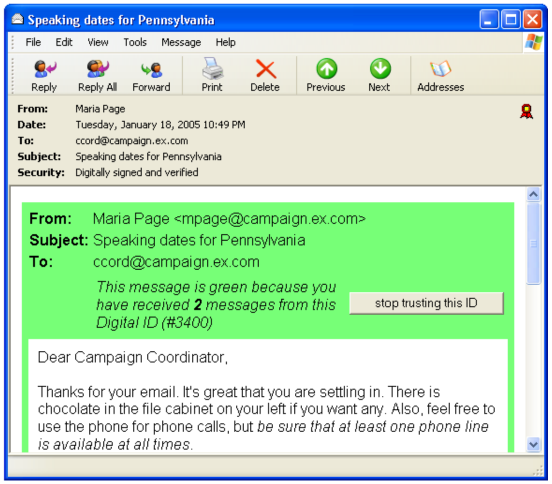
`j2app` — Experimenter’s workbench

Questions that you can answer with Johnny 2

- Do users understand difference between signing and sealing?
- If users can trivially sign and/or seal their email, will they?
- If users can seal confidential information before they send it, will they be less concerned about the destination?

Conclusion and Recommendations:

- We’ve previously argued that much commercial mail sent by eBay, Amazon, etc., should be signed.
- Johnny 2 shows that people can understand and use KCM with little or no training.
- S/MIME is much more usable than people give it credit.
- The hard thing is getting a certificate.
- KCM gives people certificates automatically, but leaves them susceptible to the New Identity Attack.
- We didn’t solve the phishing problem, but we solved some others.



From: Maria Page
Date: Tuesday, January 18, 2005 10:49 PM
To: ccord@campaign.ex.com
Subject: Speaking dates for Pennsylvania
Security: Digitally signed and verified

From: Maria Page <mpage@campaign.ex.com>
Subject: Speaking dates for Pennsylvania
To: ccord@campaign.ex.com

This message is green because you have received ***2*** *messages from this Digital ID (#3400)*

Dear Campaign Coordinator,

Thanks for your email. It's great that you are settling in. There is chocolate in the file cabinet on your left if you want any. Also, feel free to use the phone for phone calls, but *be sure that at least one phone line is available at all times*.

Questions?