Adventures in usable privacy and security
From empirical studies to public policy

Lorrie Faith Cranor
Chief Technologist
US Federal Trade Commission
CyLab Usable Privacy and Security Laboratory (CUPS)

- Design and analysis of secure systems and privacy tools
- Humans are an integral part, rather than a secondary constraint
The author’s views are her own, and do not necessarily represent the views of the Commission or any Commissioner.
What is the FTC?

• Independent law enforcement agency

• ~1,100 lawyers and staff in Washington, DC and 7 regional offices

• 5 Commissioners appointed by President, confirmed by Senate

• Competition and consumer protection
Office of Technology Research and Investigation

The Office of Technology Research and Investigation (OTech) is located at the intersection of consumer protection and new technologies. As a trusted source for research and information on technology’s impact on consumers, the Office conducts independent studies, evaluates new marketing practices, and provides guidance to consumers, businesses, and policy makers. It also assists the FTC’s consumer protection investigators and attorneys by providing technical expertise, investigative assistance, and training. The Office is housed in the Bureau of Consumer Protection and its work supports all facets of the FTC’s consumer protection mission, including issues related to privacy, data security, connected cars, smart homes, algorithmic transparency, emerging payment methods, fraud, big data, and the Internet of Things.
Today’s agenda

• Why are usability studies important for security and privacy?
• How can researchers put study participants in realistic risky situations without actually putting them at risk?
• Why might it be counterproductive to mandate frequent password changes?
• How are identity thieves able to hijack mobile phone accounts?
• How can you help the FTC protect consumers?
Why do usable privacy and security studies?
Change your password

Strengthen the security of your account with a new password.

Your password is weak, create a stronger password.

Confirm new password

☐ show password

Continue

Security Error: Domain Name Mismatch

You have attempted to establish a connection with "www.whitehouse.gov". However, the security certificate presented belongs to "a248.e.akamai.net". It is possible, though unlikely, that someone may be trying to intercept your communication with this website.

If you suspect the certificate shown does not belong to "www.whitehouse.gov", please cancel the connection and notify the site administrator.

View Certificate  Cancel  OK
How can user studies help?

Assess needs
What should we build?

Examine tradeoffs
Which features/approaches best fit particular needs?

Evaluate
Does system meet requirements? What should be improved?

Find root causes
What underlying problems need to be fixed?
Excuses for not doing usability studies

• If people weren’t so lazy/stupid/careless the system would work just fine
• I’m a cryptographer, not a usability expert
• I already know what people want
• No time, no money
• I find the system easy to use so it must be usable
• My kids can use the system so it definitely must be usable
Secure systems must work when under attack.

How can we put study participants in realistic risky situations without actually putting them at risk?
2007 Phishing warnings study

Study design challenges

• Observe users interacting with warnings without them knowing we’re interested in warnings

• Make users feel like they are under attack without actually putting them at risk
Required a little deception

- Lab study on online shopping
- Purchase paper clips from Amazon
- Answer questions about shopping (for another study)
- That’s when we phished them
- Check email to get your receipt
- That’s when they fell for it
Please approve this delay so that we can continue processing your order. (Note that if we haven't received your approval by the end of business tomorrow, the item will be cancelled.)

http://www.amazonaccounts.net/gp/signin/104-3310393-0927909.htm
Success!

- Most participants got phished
- Significant differences between conditions
- Observed interesting user behavior that helped us understand root cause of failures
Confused by domain names

“The address in the browser was of amazonaccounts.net which is a genuine address”
Confused mental models

Some users repeatedly closed their browser, returned to the phishing email, and clicked on the link again.
Research led to better phishing warnings
2008 SSL certificate warning study

- Test SSL certificate warnings
- Design a better warning
- Prevent risky behavior without disrupting non-risky behavior

Some hazards are ALWAYS dangerous
Some hazards are context dependent
Computer security dialogs context dependent

- Security warning dialogs more like warnings on wine than warnings on poison
- Software developers place burden of assessing risk on users
A good warning helps users determine whether they are at risk

• Stops users from doing something dangerous in risky context
• Doesn’t interfere with non-risky contexts
• Need to test warnings in both contexts
Can you spot the suspicious software?

[Windows Security pop-up]

Allow the following publisher to install software with full access to this computer?

Publisher: Microsoft Corporation (microsoft.com)
- I do not trust this publisher. Cancel the installation.
- I trust this publisher with complete control of my computer. Install the software.

benign

[suspicious pop-up]

Allow the following publisher to install software with full access to this computer?

Publisher: Miicr0s0ft Corporation (miicr0s0ft.com)
- I do not trust this publisher. Cancel the installation.
- I trust this publisher with complete control of my computer. Install the software.

suspicious
Key question:
Do you trust publisher?

Name of publisher is critical information in trust decision
More fun with warnings

How can we focus users’ attention on key information they need to make informed decisions?

ANSI standard warning colors
Animated connector

Allow the following publisher to install software with full access to this computer?

Publisher: Miicr0s0ft Corporation (miicr0s0ft.com)

➡️ I do not trust this publisher. Cancel the installation.

➡️ I trust this publisher with complete control of my computer. Install the software.
Slow reveal

Allow the following publisher to install software with full access to this computer?

Publisher: Miicr0s0ft Corporation (miicr0s0ft.com)

- I do not trust this publisher. Cancel the installation.

- I trust this publisher with complete control of my computer. Install the software.
Obstruct install button until user swipes mouse over publisher name
Obstruct install button until user types publisher name
Do any of these work?

• Do attractors and other techniques prevent suspicious installs without preventing benign installs?

• How much do attractors delay benign installs?
Methodology requirements

• Massive, inexpensive, quick
• Remote observation/recording of behavior
• Participants should feel safety/risk and behave as they would in real life
• But should not actually be at increased risk through participation in experiment
Use Amazon Mechanical Turk workers

Mechanical Turk is a marketplace for work.
We give businesses and developers access to an on-demand, scalable workforce. Workers select from thousands of tasks and work whenever it's convenient.

476,446 HITs available. View them now.

Make Money by working on HITs

HITs - Human Intelligence Tasks - are individual tasks that you work on. Find HITs now.

As a Mechanical Turk Worker you:
- Can work from home
- Choose your own work hours
- Get paid for doing good work

Find an interesting task → Work → Earn money

Get Results from Mechanical Turk Workers

Ask workers to complete HITs - Human Intelligence Tasks - and get results using Mechanical Turk. Register Now

As a Mechanical Turk Requester you:
- Have access to a global, on-demand, 24 x 7 workforce
- Get thousands of HITs completed in minutes
- Pay only when you're satisfied with the results

Fund your account → Load your tasks → Get results

or learn more about being a Worker
Online games evaluation survey

Purpose of the study

This survey is part of a research study conducted by Dr. Julie Downs at Carnegie Mellon University. The purpose of this study is to evaluate online games according to criteria that will be explained in the next pages. You will be asked to go to websites, play a game for 2 to 3 minutes, then return to this survey to give us your opinion on each. The whole survey should take you between 15 and 20 minutes in total.

Participants requirements

Participation in this study is limited to individuals age 18 and older. You have to physically be in the United States of America to be eligible to participate in this study, and not having taken before any early version of the same survey.

Risks, benefits, and compensation

The risks and discomfort associated with participation in this study are no greater than those ordinarily encountered in daily life or during other online activities. There may be no personal benefit from your participation in the study but the knowledge received may be of value to humanity. You will receive $1.00 as a compensation for participation in this study. There will be no cost to you if you participate in this study.

The data captured for the research does not include any personally identifiable information about you. We will collect your IP address only to check whether you qualify for the study.

Confidentiality

By participating in this research, you understand and agree that Carnegie Mellon may be required to disclose your consent form, data and other personally identifiable information as required by law, regulation, subpoena or court order. Otherwise, your confidentiality will be maintained in the
Online games evaluation survey

Instructions to evaluate the game:
1. Click on the game to load.
2. When the game loads, answer the questions below.
3. Return to this survey to answer the questions below.

Assigned game #1: Mars Buggy Online

http://www.gametop.com/online-free-games/mars-buggy-online/?i=A2NUXAJFPAX4Z2

Attention: The website whose URL appears above is external to this study. Our researchers do not control its content.
Mars Buggy

Do you like this game?

Tweet

NEW GAME
HOW TO PLAY
MORE FREE GAMES

Play this free online game today and bring your crew back to earth.
Were you able to play the game?
- Yes
- No (you will be assigned another game to evaluate)

Please enter a one-sentence description of the game you played:

Have you ever played this game before?
- Yes (please enter a reason)
- No

Do you think this game is fun?
Online games evaluation survey

Instructions to evaluate:
1. Click on the link provided below.
2. Wait for the game to load in your browser.
3. Return to this survey to answer the questions below.

Assigned game #2: Tom and Jerry Refrigerator Raid Game

http://www.free-online-games-to-play.net/games/kidsgames/onlineflashgame/751/?i=A2NUXAJFPAX4Z2

Attention: The website whose URL appears above is external to this study. Our researchers do not control its content.

2. Were you able to play the game? *

- Yes
- No (you will be assigned another game to evaluate)
2. Were you able to play the game? *

- Yes
- No (you will be assigned another game to evaluate)

Please enter here a one-sentence description of the game you played (between 10 and 50 words): *

A boring Tom-and-Jerry game, may be fun for kids.

Please answer the following questions about the game you played: *

<table>
<thead>
<tr>
<th></th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Have you ever played this game before?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you think this game is fun?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Did the game have any visual glitches, such as stalls in animations or overlapping windows, when running on your computer/browser? *

- Yes (please explain briefly)
- No
Assigned game #3: Colliderix Level Pack

http://www.yourgamefactory.net/wtk/games/index.u1.php?id=2NUXAJFPAX4Z2

Attention: The website whose URL appears above is external to this study. Our researchers do not control its content.

4. Were you able to play the game? *
- Yes
- No (you will be assigned another game to evaluate)
This game requires the latest version of Microsoft Silverlight™ (v5.1.2). Silverlight is either missing or out of date.

Access being requested, please wait.
Benign condition: “Microsoft Corporation”
Suspicious condition: “Miicr0s0ft Corporation”
Results are encouraging

• 2,227 participants encountered dialogs

• Benign scenario
  – Installation not prevented
  – But some approaches slowed people down

• Suspicious scenario
  – Our new dialogs reduced installations
  – Swipe, type, and delay were particularly effective
But what would happen if users saw these attractors repeatedly?

- Conducted two more experiments
- Used a different scenario in which participants had to dismiss a dialog repeatedly for several minutes until the dialog changed
- Measured rate of compliance with instructions in changed dialog

Control and ANSI decline with habituation
Reveal and AC+Delay start out better, decline with habituation
Swipe and Type are resilient to habituation

Could not predict difference between green and purple lines from previous experiments
Why might it be counterproductive to mandate frequent password changes?
Encourage your loved ones to change passwords often, making them long, strong, and unique. More tips: go.usa.gov/cEqkH. #ChatSTC
PASSWORDS ARE LIKE UNDERPANTS

Change them often, keep them private and never share them with anyone.
Time to rethink mandatory password changes

By: Lorrie Cranor, Chief Technologist | Mar 2, 2016 10:55AM

TAGS: Authentication | Human-computer interaction | Passwords | Research

Data security is a process that evolves over time as new threats emerge and new countermeasures are developed. The FTC’s longstanding advice to companies has been to conduct risk assessments, taking into account factors such as the sensitivity of information they collect and the availability of low-cost measures to mitigate risks. The FTC has also advised companies to keep abreast of security research and advice affecting their sector, as that advice may change. What was reasonable in 2006 may not be reasonable in 2016. This blog post provides a case study of why keeping up with security advice is important. It explores some age-old security advice that research suggests may not be as effective as previously thought.
Why changing your password regularly may do more harm than good

Most office workers have had to deal with a password changing requirement, maybe every six months or so. Requiring users to flush out old passwords will cut off access.
Why require password changes?

Lock out attackers who have learned users’ passwords
Password transformations
Password transformations

Capitalization:       tarheels#1 → tArheels#1

Duplication:         tarheels#1 → tarheels#11

Substitution:        tarheels#1 → tarheels#2

Insertion:           tarheels#1 → tarheels#12

Keyboard transform:  tarheels#1 → tarheels#!

Date:                tarheel#0510 → tarheel#0810
10,000+ defunct UNC accounts

• Mandatory password change every 3 months
• Obtained 4-15 hashed passwords to each account
• Cracked >1 non-last password for 7,752 accounts

Zhang, Monrose, and Reiter, CCS 2010
Evaluation

• Pick a known plaintext, non-last password (OLD)

• Pick any later password (NEW)

• Attempt to crack NEW using transform rules applied to OLD

Zhang, Monrose, and Reiter, CCS 2010
Results

• Online attack
  – 17% of accounts cracked in <5 guesses

• Offline attack
  – 41% of accounts cracked within 3 seconds

Zhang, Monrose, and Reiter, CCS 2010
Benefits of expiry are limited

- Brute force attacks only slowed a little bit by password change
  - Slow hash functions slow them down more
- Attacker who gains access may install key logger and observe password change
Survey evidence

• Frequent password expiry → users create weaker passwords (Adams & Sasse, 1999)

• Annoyed at password change → users create weaker passwords (Mazurek et al., 2013)
The problems with forcing regular password expiry

Version: 1
Created: 11 April 2016
Updated: 15 April 2016
Topics: Passwords, Best Practice

Why CESG decided to advise against this long-established security guideline.

Regular password expiry is a common requirement in many security policies. However, in CESG’s Password Guidance published in 2015, we explicitly advised against it. This article explains why we made this (for many) unexpected recommendation, and why we think it’s the right way forward.

Let’s consider how we might limit the harm that comes from an attacker who knows a user’s password. The obvious answer is to make the compromised password useless by forcing the legitimate user to replace it with a new one that the attacker doesn’t know. But there are some risks with this approach that we feel need to be considered.

Related Content
Password Guidance: Simplifying Your Approach
Revealed: the most frequently used passwords of 2015
Certified Cyber Consultancy
Cyber Essentials
CESG advocates new approach to
Welcome to the NIST SP 800-63-3 Public Preview! We’re excited to share the major transformation that this document has undergone, as well as collaboratively enhance and evolve the guidance as we head to a public draft later this summer.

A few formalities

Public preview vs public draft

If you’ve made it to this page, you can see we’re approaching this a little differently by putting our work up on GitHub, rather than the “traditional” comment period for a NIST Special Publication (SP). We’re calling it a public preview because some of our agency partners (and NIST itself) have formal processes for public drafts. Calling it a public preview is our way of letting everyone know those processes aren’t in play. This lets us do things differently...

A different cadence

This public preview is focused on gaining input through successive open comment periods and editing iterations of the SP draft. This phase will include multiple iterations of comments of approximately 2 weeks in length, followed by a 2-3 week period for the editors to adjudicate comments and make appropriate updates to...
Data-driven password meter

Password meter under development at CMU, August 2016
How are identity thieves able to hijack mobile phone accounts?
IdentityTheft.gov can help you report and recover from identity theft.

**HERE'S HOW IT WORKS:**

1. **Tell us what happened.**
2. **Get a recovery plan.**
3. **Put your plan into action.**
What To Do Right Away
Are you dealing with tax, medical, or child identity theft? See: Special forms of identity theft

+ Step 1: Call the companies where you know fraud occurred.
+ Step 2: Place a fraud alert and get your credit reports.
+ Step 3: Report identity theft to the FTC.
+ Step 4: File a report with your local police department.

What To Do Next
Take a deep breath and begin to repair the damage.

+ Close new accounts opened in your name.
Credit Fraud — Take Action

You can add a fraud alert message to your credit report to help protect your credit information by selecting from one of the credit fraud alert options below. Fraud alert messages notify potential credit grantors to verify your identification before extending credit in your name in case someone is using your information without your consent.

What would you like to do?

- Add a Fraud Alert Message
- Review a Copy of My Report
- Learn How to Respond to Identity Theft
- Protect and Monitor My Credit

Information You Should Know
- How Can I Protect Myself?
- How Does Experian Protect Me?
- Minor Child Instructions
- Summary of Rights of Identity Theft Victims
- Removing a Fraud Alert

Deter, Detect, Protect and Resolve with ProtectMyID
Get full service identity theft protection including:
- Online access to your Experian credit report
- Daily internet scanning for unauthorized use of your SSN, debit and credit cards
- Daily 3 bureau credit monitoring with alert notifications when key changes are detected
- Access to dedicated Fraud Resolution Professionals
Report Identity Theft to the FTC

Next, we are going to ask for specific details. We will use the information you provide to create your:

- Identity Theft Affidavit
- Recovery Plan

These will help you fix problems caused by identity theft.

How we handle your information

It's up to you to determine how much personal information you want to provide. The FTC enters this information into a secure online database that law enforcement agencies use in their investigations.

Please read our Privacy Policy to learn more about how we safeguard your personal information.

OMB Control Number: 3084-0047
Your Law Enforcement Report

One way to get a credit reporting agency to quickly block identity information from appearing on your credit report is to submit a law enforcement report ("Identity Theft Report"). You can obtain an Identity Theft Report by taking this form to your local law enforcement office and adding supporting documentation. Ask an officer to witness your signature on this form, then complete the rest of the information in this section. It’s important to get the report number, whether or not you are able to file it in person and if this is the official law enforcement report. Attach a copy of any correspondence to the official law enforcement report you receive when sending the information to reporting agencies.

Select ONE:

☑️ I have not filed a law enforcement report.
☐ I was unable to file any law enforcement report.
☐ I filed an automated report with the law enforcement.
☐ I filed my report in person with the law enforcement.

Select ONE:

Did the victim receive a copy of the report from the law enforcement?

☐ Yes OR ☐ No

Victim’s FTC complaint number (if available): 69211562
Dena Haritos Tsamitis  Same thing happened to me last Thursday!!! Crazy coincidence! I dug into this and discovered mine occurred
Like · Reply · March 9 at 10:15pm

Dena Haritos Tsamitis  Sorry...mine occurred in a store in NYC. Someone actually walked into a store and was granted the authority to access my account and make changes. I firmly believe it was an inside job or someone wasn't doing their job.
Like · Reply · March 9 at 10:17pm
More than 50 Verizon customers tell 7NEWS they are victims of unauthorized charges on their accounts

BY: Marshall Zelinger
POSTED: 12:08 AM, Feb 10, 2015
UPDATED: 5:43 AM, Feb 10, 2015
TAG: scam | fraud | iphone | verizon | unauthorized
Four accused of using stolen identities to purchase iPhones in Johnson County

BY: Nick Sloan, Andres Gutierrez, Shannon Halligan
POSTED: 8:05 AM, Dec 9, 2015
UPDATED: 11:52 AM, Dec 9, 2015

Police: Man tried to use stolen credit card, ID to buy four iPhones

BY KATU.COM STAFF | MONDAY, MAY 9TH 2016
SIM swap fraud: The multi-million pound security issue that UK banks won't talk about

By Mary-Ann Russon
April 4, 2016 14:23 BST

Dozens of cellphone users hit by SIM-swap scam
2016-03-03 09:40

Over 100 Fin24 users say they have also been hit
Consumer Sentinel Network

**Consumer Sentinel** is the unique investigative cyber tool that provides members of the Consumer Sentinel Network with access to millions of consumer complaints. Consumer Sentinel includes complaints about:

- Identity Theft
- Do-Not-Call Registry violations
- Computers, the Internet, and Online Auctions
- Telemarketing Scams
- Advance-fee Loans and Credit Scams
- Immigration Services
- Sweepstakes, Lotteries, and Prizes
- Business Opportunities and Work-at-Home Schemes
- Health and Weight Loss Products
- Debt Collection, Credit Reports, and Financial Matters

**Consumer Sentinel** is based on the premise that sharing information can make law enforcement even more effective. To that end, the Consumer Sentinel Network provides law enforcement members with access to complaints provided directly to the Federal Trade Commission by consumers, as well as providing members with access to complaints shared by data contributors.
# Mobile phone account hijacking and new account fraud

<table>
<thead>
<tr>
<th></th>
<th>Number of incidents reported</th>
<th>% of identity theft reports</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 2013</td>
<td>1,083</td>
<td>3.2%</td>
</tr>
<tr>
<td>January 2016</td>
<td>2,658</td>
<td>6.3%</td>
</tr>
</tbody>
</table>
Add or remove extra security

Learn how to add or remove extra security for your wireless account. Extra security requires your passcode in more situations than standard security.

You're viewing instructions for

Device: Smartphone/myAT&T app

STEP-BY-STEP

How to add or remove extra security from your account

You need to try logging in to your myAT&T account using the myAT&T app¹ or from our mobile site to complete these steps.

Change wireless security passcode settings

Select the menu button > Profile > Login Information.
Your mobile phone account could be hijacked by an identity thief

By: Lorrie Cranor, FTC Chief Technologist | Jun 7, 2016 11:38AM

TAGS: Accountability | Authentication | Identity theft | Mobile | Personal harms | Privacy

A few weeks ago an unknown person walked into a mobile phone store, claimed to be me, asked to upgrade my mobile phones, and walked out with two brand new iPhones assigned to my telephone numbers. My phones immediately stopped receiving calls, and I was left with a large bill and the anxiety and fear of financial injury that spring from identity theft. This post describes my experiences as a victim of ID theft, explains the growing problem of phone account hijacking, and suggests ways consumers and mobile phone carriers can help combat these scams.

My Experiences as a Victim of ID Theft

One evening my mobile phone stopped working mid call. After discovering that another phone on my account also had no signal, I called my mobile carrier on a landline phone. The customer service representative explained that my account had been updated to include new iPhones, and in the process the SIM cards in my Android phones had been deactivated. She assumed it was a mistake, and told me to take my phones to one of my mobile carrier’s retail stores.

The store replaced my SIM cards and got my phones working again. A store employee explained that a thief claiming to be me had gone into a phone store and “upgraded” my two phones to the most expensive iPhone models available and transferred my phone numbers to the new iPhones.

I called my mobile carrier’s fraud department and reported what happened. The representative agreed to remove
How Even the FTC’s Lead Technologist Can Get Hacked

LAW & DISORDER / CIVILIZATION & DISCONTENTS

FTC’s chief technologist gets her mobile phone number hijacked by ID thief
If it can happen to her, chances are it can happen to lots of people.

by Dan Goodin - Jun 7, 2016 2:01pm EDT
@DERAY'S TWITTER HACK REMINDS US EVEN TWO-FACTOR ISN'T ENOUGH

THIS HAS BEEN the week of Twitter hacks, from Mark Zuckerberg to a trove of millions of passwords dumped online to, most recently, Black Lives Matter activist DeRay McKesson.
How can you help the FTC protect consumers?
Upcoming FTC events

- SmartTV workshop – December 7
- PrivacyCon – January 12
We Want You!

Send us your papers
research@ftc.gov

Tell us what you’ve discovered

Come to our workshops

ftc.gov/tech
Research on privacy and security

• What are the best ways to assess the risks posed by breaches and vulnerabilities?

• What can be done to protect consumers from ransomware, malvertising, etc?

• How can we tie exposed data to a specific breach?

• How can we better spot fraud?
Research on IoT devices

• How can IoT device manufacturers and platforms ensure better IoT security?

• What defensive measures can prevent one vulnerable IoT device from compromising other devices on the same network?

• How can consumers identify vulnerable IoT devices on their network?
Research on tools & techniques

• Allow users to control their personal information across contexts

• Allow consumers to observe behavior and communication of their smart devices

• Analyze apps to determine practices associated with third-party libraries

• Identify tracking and cross-device tracking

• Detect discriminatory algorithms