Security Fatigue

Brian Stanton  Cognitive Scientist

Mary Theofanos  Computer Scientist

Sandra Spickard-Prettyman  Anthropology/Sociology (Culture Catalyst)

Susanne Furman  Cognitive Scientist

Multi-Disciplinary Team
Security Fatigue

Searching
A mental model is a cognitive representation that helps us make sense of the world around us.

- Germ
- Robber
- Barrier
- Hacker
Experience and Thoughts About Computer Security

1. In the past two years, have you ever received any computer security training or education?
   - How often did you receive that training?
   - What type of training have you received (online, classroom)?
   - Who provided the training?
   - Were you able to understand the content?
   - Was it beneficial?
   - How was it beneficial?

Did you change your behavior after the training? (yes or no)
   - What changed in your behavior?
   - What accounted for that change?
   - How long did that behavior last?

2. Please provide an assessment of your knowledge of computer or internet security from 1 (very little knowledge) to 10 (expert). Please use the following scale:

   ![Graphical representation of knowledge scale]

   *(very little knowledge = participant knows very little about policy or setting up their computer; expert = know how to set up a secure home computer)*

   Why have you chosen the rating?

3. Security Questions
   When you are using your computer, do you ever think about computer security? Please describe what you think about when considering computer security or how you define or describe computer security.

   Now that you have given me your definition of computer security, now thinking about your computer:
   - What do you think you are protecting?
   - From who/what are you protecting "that" (i.e., insert what they say they are protecting) from?

   When you are using your computer at home do you ever think about protecting something with regards to the computer?
   - What are you protecting?
Analysis #1: Quantitative

- Counted
- Stats
- Personas
Analysis #2: Qualitative

Transcripts

Initial Code List

Code every transcript

Emergent Codes

Code Saturation

Look for relationships, concepts, and ideas

"Leap"

Instant messaging: YES

File Sharing: NO

Chat room: NO

Research/Education: I do a lot of research online but haven’t taken any classes.

Banking: Yes – I check my accounts at least every couple of days.

Why do you prefer online? (Convenience) and the accounts are updated every evening and (they are accurate). I fell into that because balancing my checkbook was a pain. About 10 years ago with the advent of ATM cards – I quick carrying cash and I have quit carrying cash since then.

Online bill paying: YES – I do it about once a week.

Why do you prefer online? I know you money is transferred on any specific day. Bills are paid within two days and max is 5 days. It saves a lot of money.

Emails: YES

Social Networking: YES I have Facebook. I check when I am bored about once a week just to see what people I haven’t seen for 40 years are doing. I never post anything because I have a wide diversity of friends. Who may look and say oh you do that. I don’t post things but I like to see what they are doing. I put my birth date – where I went to school and where I grew up.

Victim of Online Fraud

NO

Security Training or Education

NO

Can we back up about that last question? I am pretty well self-taught. When I look at things from Bank of America – I always read the security information and double checking it. I only do my banking on one specific computer and my IPhone. I never do that on any other computer. It is my personal computer – it is kept at home – I am the only person who uses it.

Assessment:

5

Why? I am self-taught. There are some technical aspects that I don’t need to know because I started using an Apple for a variety of reasons. They are more secure than Windows. At times I
Security Fatigue

What we found
Throughout the Data:

- Poor or non-existent mental models
- Weariness
- Frustration
- Denial
- Worthlessness
- Resignation
- Complacency
"I think I am desensitized to it; I know bad things can happen. You get this warning that some virus is going to attack your computer, and you get a bunch of emails that say don’t open any emails, blah, blah, blah. I think I don’t pay any attention to those things anymore because it’s in the past. People get weary of being bombarded by “watch out for this or watch out for that”"
“I never remember the PIN numbers, there are too many things for me to remember. It is frustrating to have to remember this useless information.”
"It doesn’t appear to me that it poses such a huge security risk. I don’t work for the state department, and I am not sending sensitive information in an email. So, if you want to steal the message about [how] I made blueberry muffins over the weekend, then go ahead and steal that."
Our Participants:

- Making poor decisions about security
- Too many decisions to make
- Tired of making decisions
When people are fatigued they fall back on heuristics and cognitive biases when making decisions.

Cognitive biases are tendencies to think in certain ways that can lead to systematic deviations from a standard of rationality or good judgment.

We found in our data that people often make decisions about security based on heuristics and cognitive biases.
24 Cognitive Biases (Tversky & Kahneman)

You irrationally cling to things that have already cost you something.

When we've invested our time, money, or emotion into something, it hurts to let it go. Ask yourself: had I not already invested something, would I still do so now? yourself — and you are the easiest person to fool. — Richard Feynman
bounded rationality limits our ability to acquire then apply information in the online privacy and security space

- Amount of information we can process
- Cognitive limitations of our mind
- The time we have to make decisions
- Incomplete information
- Systematic psychological deviations from rationality
It has been hypothesized that we make cost benefit tradeoffs about our online security and when the cost of complying is greater than the effort we can make, we choose not to comply or find workarounds.

- Conceptualized Security Fatigue in the workplace
- “Threshold were at which it simply gets too hard of burdensome for users to maintain security”
“No matter how smart or hard-working we are, our ability to make good decisions eventually runs out.”

“Our ability to force ourselves to do difficult things—that is, applying self-control or self-discipline—draws up on a certain limited resource within us. And when we’re forced to make tough decisions, it calls upon that same resource.”
Supporting Literature

- Tversky & Kahneman (1973) Heuristics & Biases
- Acquisti & Grossklags (2005) Bounded Rationality
- Beaument, Sasse, & Wonham (2008) Compliance Budget
- Oto, Limmer, & Training (2012) Decision Fatigue
Security Fatigue

The psychological state one reaches when security decisions become too numerous and/or too complex, inhibiting good security practices, exhibited by attributes such as weariness, hopelessness, frustration, and devaluation on the part of the sufferer.
Security Fatigue Actions

- Avoiding unnecessary decisions;
- Choosing the easiest available option;
- Making decisions driven by immediate motivations;
- Choosing to use a simplified algorithm;
- Behaving impulsively;
- Resignation
Security Fatigue

What can we do?
Suggested Preventions

- Limit the decisions users have to make for security;
- Make it easy for users to have to do the right thing related to security;
- Provide consistency (whenever possible) in the decisions users need to make.
- Help make security a habit
## Usability Considerations

- **Memorized secrets**
- **Look-up Secrets**
- **Out of Band**
- **Single Factor OTP Device**
- **Multi-Factor OTP Device**
- **Single Factor Cryptographic Software**
- **Single Factor Cryptographic Device**
- **Multi-Factor Cryptographic Software**
- **Multi-Factor Cryptographic Device**

### Typical usage

**Authenticator availability** - authenticators readily in user's possession

**Plain language for user facing text** (e.g., instructions, prompts, notifications, error messages)

**Legibility of user facing text or text entered by users**

**Unmasked text entry**

**Support text entry** - length of 64 characters, copy and paste

**Delayed masking during text entry**

**Adequate time allowed for text entry**

**Entry errors** - need clear and meaningful feedback

**Minimum of 10 attempts allowed**

**Remaining allowed attempts** - need clear and meaningful feedback

**Form-factor constraints**

**Location and availability of a direct computer interface such as a USB port**

**Physical input required** (such as pressing a button)

**Cryptographic keys need for descriptive and meaningful names**

**Complexity and size of the prompts**

**Authentication to secondary device to access the authentication secret**

**Continuous hardware connection not required**
Security Fatigue
Thank You

Brian.stanton@nist.gov