National Institute of Standards and Technology US Department of Commerce

Security Fatigue

Brian Stanton Cognitive Scientist

Mary Theofanos Computer Scientist

Sandra Spickard-Prettyman
(Culture Catalyst)

Susanne Furman Cognitive Scientist

Anthropology/Sociology

Multi-Disciplinary Team

Security Fatigue

Searching

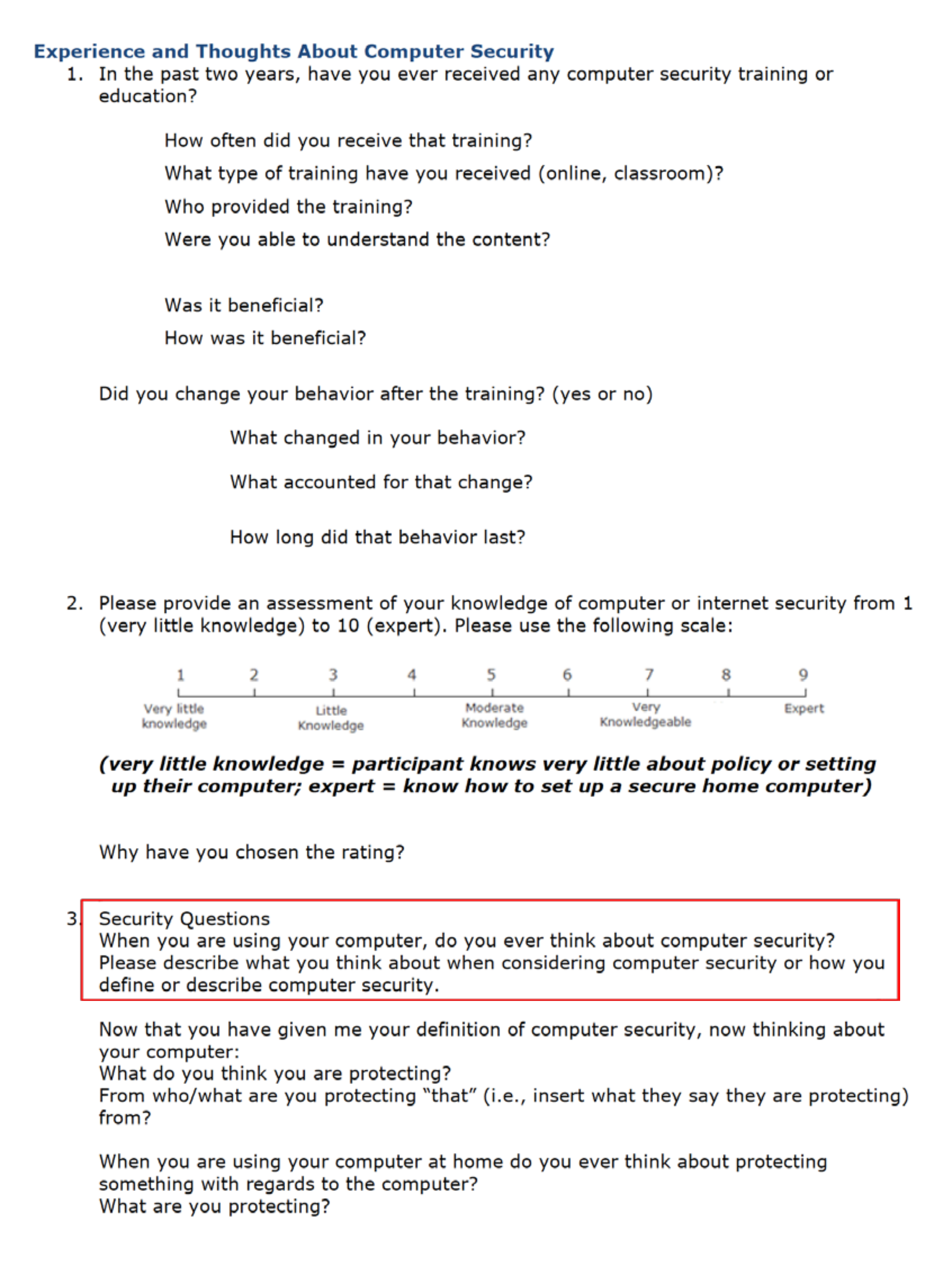
Looking for Mental Models

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

- Germ
- Robber
- Barrier
- Hacker

Pop

- General Pu
  - 40 non-p
  - Men and
  - Urban an
  - In depth
  - Attitudes



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:

1	2	3	4	5	6	7	8	9
Very little knowledge		Little Knowledge		Moderate Knowledge		Very Knowledgeable		Expert

   (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?

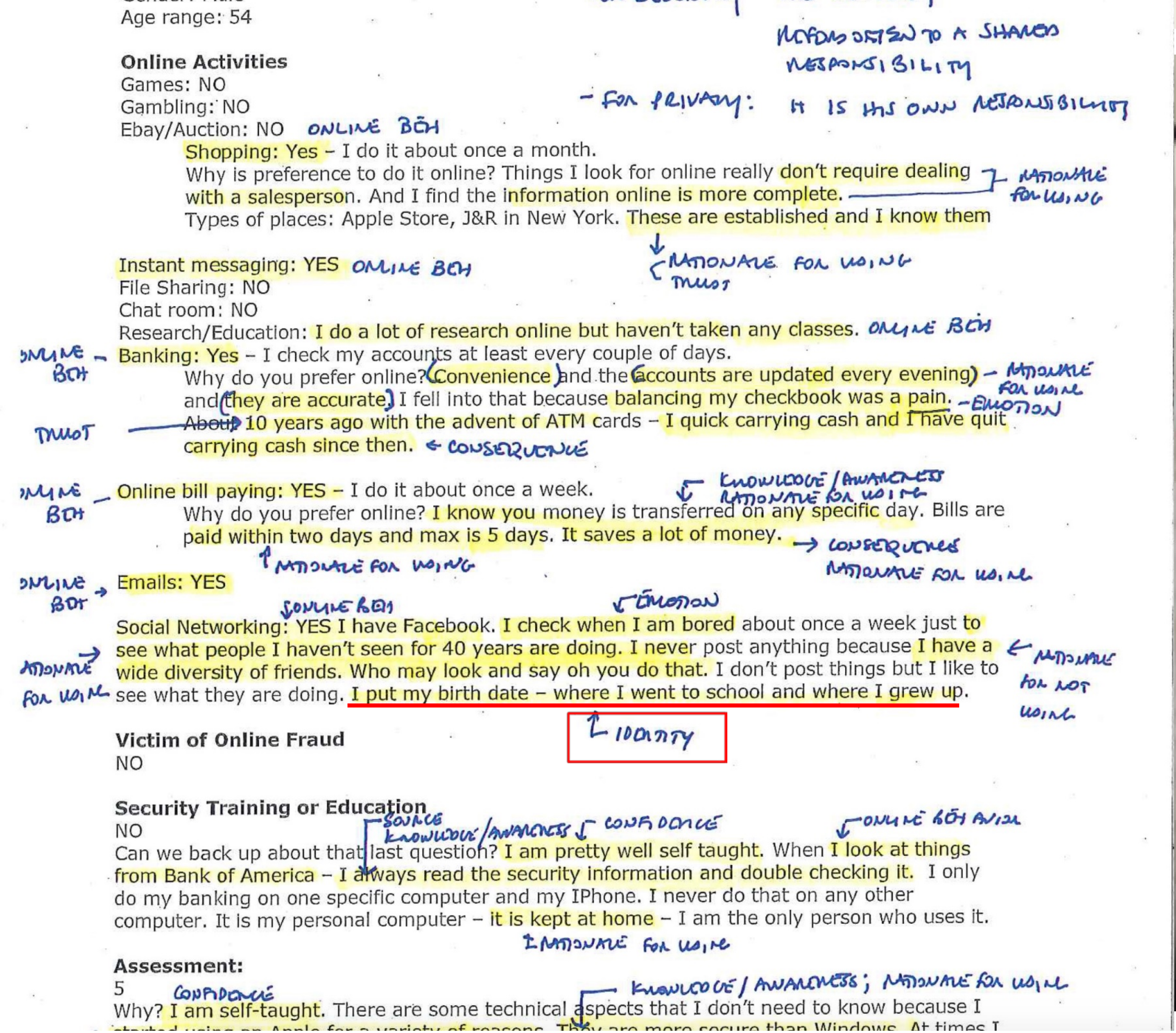
3. Security Questions
   When you are using your computer, do you ever think about computer security?
   Please describe what you think about when considering computer security or how you define or describe computer security.

   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



Age range: 54

REFERS OFTEN TO A SHARED RESPONSIBILITY

– FOR PRIVACY: IT IS HIS OWN RESPONSIBILITY

Online Activities
Games: NO
Gambling: NO
Ebay/Auction: NO ONLINE BEH

Shopping: Yes – I do it about once a month.
Why is preference to do it online? Things I look for online really don't require dealing with a salesperson. And I find the information online is more complete. RATIONALE FOR USING
Types of places: Apple Store, J&R in New York. These are established and I know them

RATIONALE FOR USING
TRUST

Instant messaging: YES ONLINE BEH
File Sharing: NO
Chat room: NO
Research/Education: I do a lot of research online but haven't taken any classes. ONLINE BEH

ONLINE BEH – 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) – RATIONALE FOR USING
and (they are accurate) I fell into that because balancing my checkbook was a pain. – EMOTION
TRUST ~~About~~ 10 years ago with the advent of ATM cards – I quick carrying cash and I have quit carrying cash since then. ← CONSEQUENCE

ONLINE BEH – Online bill paying: YES – I do it about once a week.
KNOWLEDGE / AWARENESS
RATIONALE FOR USING
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. → CONSEQUENCES
RATIONALE FOR USING
RATIONALE FOR USING

ONLINE BEH → Emails: YES

ONLINE BEH
EMOTION

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.

RATIONALE FOR USING
← RATIONALE FOR NOT USING

IDENTITY

Victim of Online Fraud
NO

Security Training or Education
NO

SOURCE
KNOWLEDGE / AWARENESS
CONFIDENCE
ONLINE BEHAVIOR

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.

RATIONALE FOR USING

Assessment:
5 CONFIDENCE

KNOWLEDGE / AWARENESS; RATIONALE FOR USING

Why? I am self-taught. There are some technical aspects that I don't need to know because I

Security Fatigue

What we found

Throughout the Data:

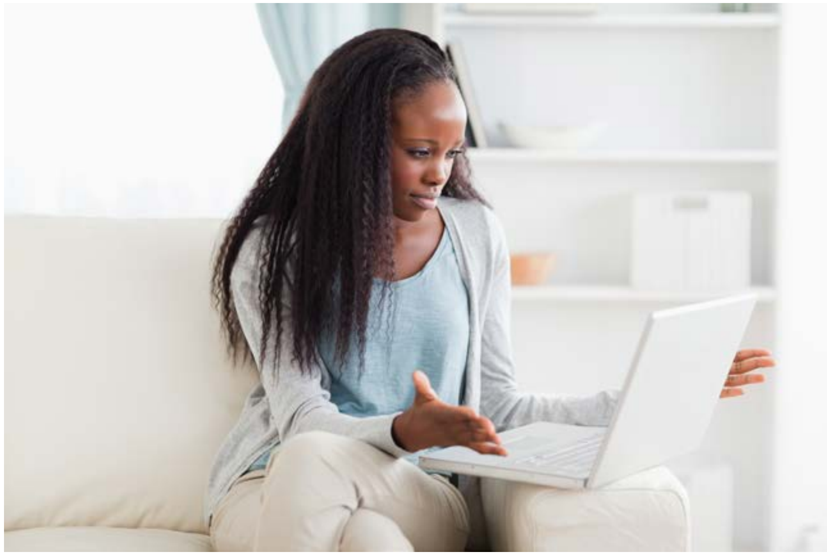
- Poor or non-existent mental models
- Weariness
- Frustration
- Denial
- Worthlessness
- Resignation
- Complacency

Quote: Participant 101

"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'"

Quote: Participant 209

"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."



Quote: Participant 108

"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

Tversky & Kahneman (1973) Heuristics & Biases

- 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)

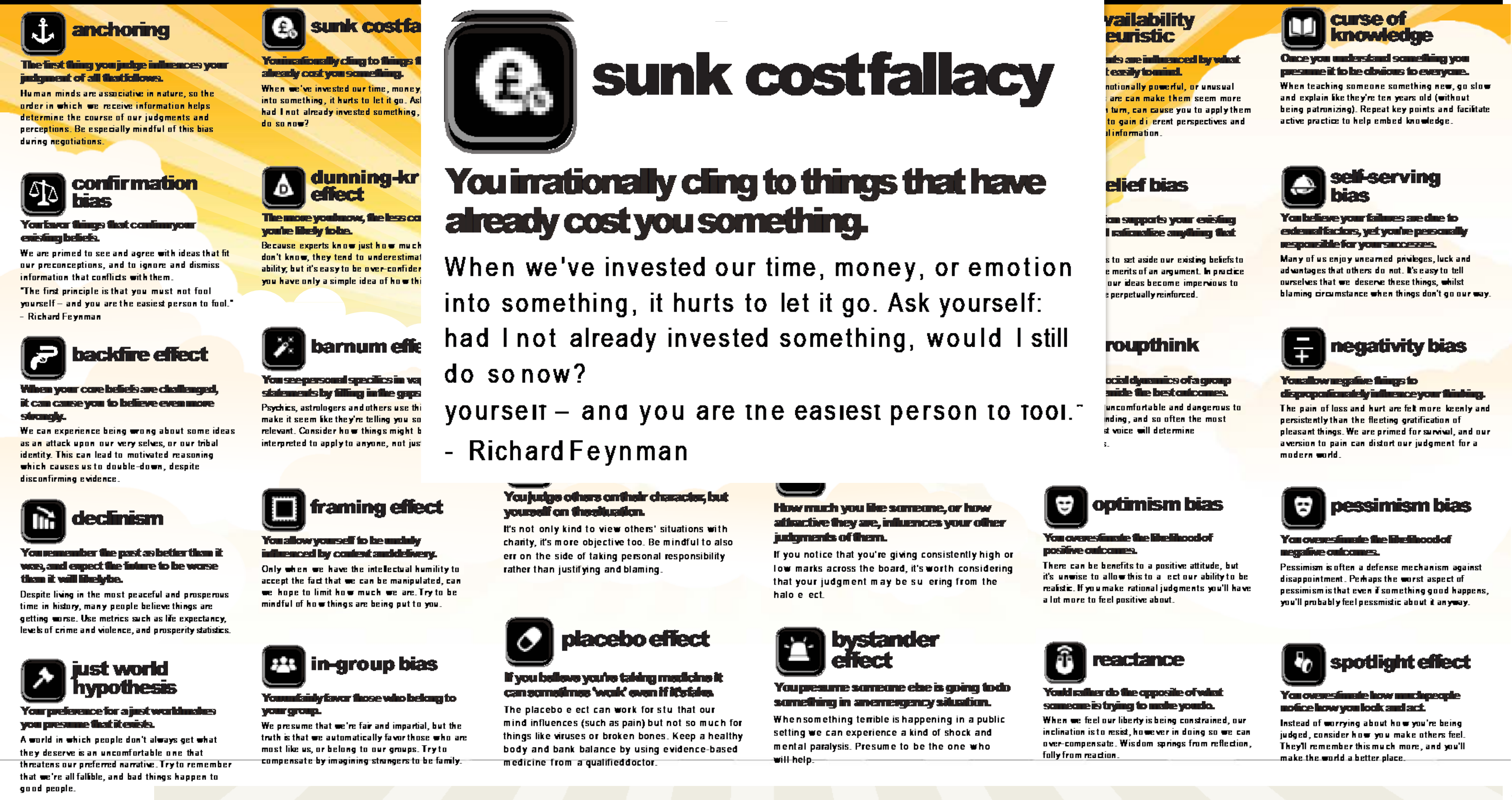
sunk cost fallacy

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



anchoring

The first thing you judge influences your judgment of all that follows.

Human minds are associative in nature, so the order in which we receive information helps determine the course of our judgments and perceptions. Be especially mindful of this bias during negotiations.

confirmation bias

You favor things that confirm your existing beliefs.

We are primed to see and agree with ideas that fit our preconceptions, and to ignore and dismiss information that conflicts with them.

"The first principle is that you must not fool yourself – and you are the easiest person to fool." – Richard Feynman

backfire effect

When your core beliefs are challenged, it can cause you to believe even more strongly.

We can experience being wrong about some ideas as an attack upon our very selves, or our tribal identity. This can lead to motivated reasoning which causes us to double-down, despite disconfirming evidence.

declinism

You remember the past as better than it was, and expect the future to be worse than it will likely be.

Despite living in the most peaceful and prosperous time in history, many people believe things are getting worse. Use metrics such as life expectancy, levels of crime and violence, and prosperity statistics.

just world hypothesis

Your preference for a just world makes you presume that it exists.

A world in which people don't always get what they deserve is an uncomfortable one that threatens our preferred narrative. Try to remember that we're all fallible, and bad things happen to good people.

sunk cost fa

You irrationally cling to things th already cost you something.

When we've invested our time, money, into something, it hurts to let it go. Ask had I not already invested something, do so now?

dunning-kr effect

The more you know, the less co you're likely to be.

Because experts know just how much don't know, they tend to underestimat ability; but it's easy to be over-confiden you have only a simple idea of how thi

barnum effe

You see personal specifics in va statements by filling in the gaps

Psychics, astrologers and others use thi make it seem like they're telling you so relevant. Consider how things might b interpreted to apply to anyone, not jus

framing effect

You allow yourself to be unduly influenced by context and delivery.

Only when we have the intellectual humility to accept the fact that we can be manipulated, can we hope to limit how much we are. Try to be mindful of how things are being put to you.

in-group bias

You unfairly favor those who belong to your group.

We presume that we're fair and impartial, but the truth is that we automatically favor those who are most like us, or belong to our groups. Try to compensate by imagining strangers to be family.

You judge others on their character, but yourself on the situation.

It's not only kind to view others' situations with charity, it's more objective too. Be mindful to also err on the side of taking personal responsibility rather than justifying and blaming.

placebo effect

If you believe you're taking medicine it can sometimes 'work' even if it's fake.

The placebo e ect can work for stu that our mind influences (such as pain) but not so much for things like viruses or broken bones. Keep a healthy body and bank balance by using evidence-based medicine from a qualifieddoctor.

How much you like someone, or how attractive they are, influences your other judgments of them.

If you notice that you're giving consistently high or low marks across the board, it's worth considering that your judgment may be su ering from the halo e ect.

bystander effect

You presume someone else is going to do something in an emergency situation.

When something terrible is happening in a public setting we can experience a kind of shock and mental paralysis. Presume to be the one who will help.

vailability euristic

nts are influenced by what t easily to mind.

notionally powerful, or unusual are can make them seem more n turn, can cause you to apply them to gain di erent perspectives and al information.

elief bias

ion supports your existing l rationalise anything that

s to set aside our existing beliefs to e merits of an argument. In practice our ideas become impervious to e perpetually reinforced.

roupthink

ocial dynamics of a group ride the best outcomes.

uncomfortable and dangerous to nding, and so often the most st voice will determine s.

optimism bias

You overestimate the likelihood of positive outcomes.

There can be benefits to a positive attitude, but it's unwise to allow this to a ect our ability to be realistic. If you make rational judgments you'll have a lot more to feel positive about.

reactance

You'd rather do the opposite of what someone is trying to make you do.

When we feel our liberty is being constrained, our inclination is to resist, however in doing so we can over-compensate. Wisdom springs from reflection, folly from reaction.

curse of knowledge

Once you understand something you presume it to be obvious to everyone.

When teaching someone something new, go slow and explain like they're ten years old (without being patronizing). Repeat key points and facilitate active practice to help embed knowledge.

self-serving bias

You believe your failures are due to external factors, yet you're personally responsible for your successes.

Many of us enjoy unearned privileges, luck and advantages that others do not. It's easy to tell ourselves that we deserve these things, whilst blaming circumstance when things don't go our way.

negativity bias

You allow negative things to disproportionately influence your thinking.

The pain of loss and hurt are felt more keenly and persistently than the fleeting gratification of pleasant things. We are primed for survival, and our aversion to pain can distort our judgment for a modern world.

pessimism bias

You overestimate the likelihood of negative outcomes.

Pessimism is often a defense mechanism against disappointment. Perhaps the worst aspect of pessimism is that even if something good happens, you'll probably feel pessmistic about it anyway.

spotlight effect

You overestimate how much people notice how you look and act.

Instead of worrying about how you're being judged, consider how you make others feel. They'll remember this much more, and you'll make the world a better place.

Acquisti & Grossklags (2005) Bounded Rationality

- 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

Beautement, Sasse, & Wonham (2008) Compliance Budget

- 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 we find workarounds

Thomson & Furnell (2009)Work Place Security Fatigue

- Conceptualized Security Fatigue in the workplace
- “Threshold were at which it simply gets too hard of burdensome for users to maintain security”

Oto, Limmer, & Training (2012)
Decision Fatigue

- “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 upon 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
- Beautement, Sasse, & Wonham (2008) Compliance Budget
- Thomson & Furnell (2009) Workplace Security Fatigue
- 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

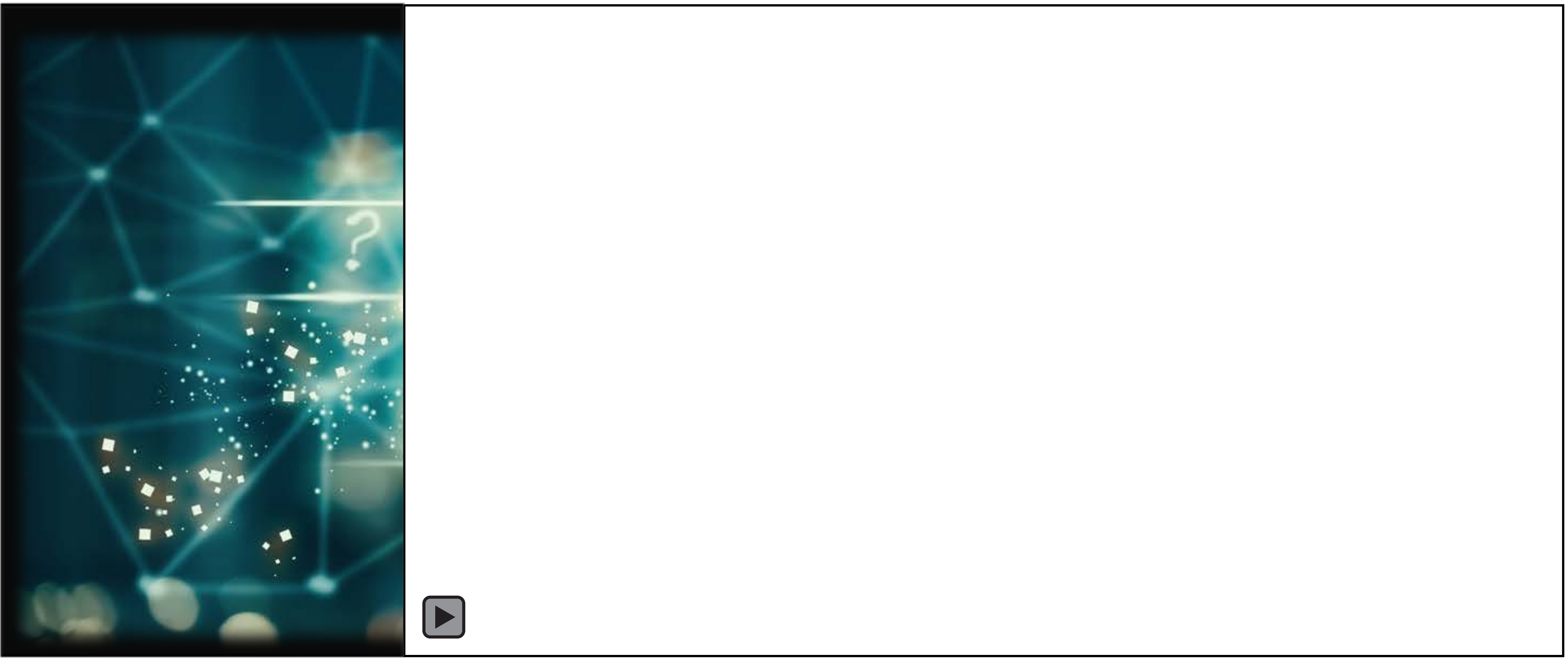
What can we do?

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