Usable Security

Mary Theofanos

September 10, 2015

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Cyber Security can only be achieved in partnership with users.

What is Usability?

ISO 9241-210

"Usability: The extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use."

Definition Identifies How to Proceed:

What to measure

- Users
- Goals
- Context of Use

How to measure

- Effectiveness
- Efficiency
- Satisfaction

1st Tenet of Usability: Know thy User!

Many different user groups:

- Policy Makers/Corporate decision makers/investors
- Cyber Security researchers/developers/implementers
- CIO's and those who implement cyber within an organization
- End users

Set out to understand our end users?

We found our end users:

- Don't have a good mental model of security or privacy
- Are overwhelmed with passwords

What We Did

Interviewed 40 people about:

- Experiences with online privacy and/or security
- Use of mental models as they think about privacy and/or security in the online environment

Gender	21-29	30-39	40-49	50-59	60+	Total
Males	4	1	2	9	3	19
Females	5	6	6	2	2	21
Total	**9**	**7**	**8**	**11**	**4**	**40**

Area	HS	Some College	BA/BS	BA+	MA/MS	JD/PhD/MD
Central PA	0	2	6	2	2	1
DC Metro	2	5	16	1	2	1
Total	2	7	22	3	4	2

Numbers Couldn't Tell the Whole Story

Quantitative analysis didn't account for the richness of the data

- *Example: 31 out of 40 said that hackers, bad guys, and cybercriminals were a concern*
- This doesn't tell us why they believe this, what it is based on, what their experiences were.

Qualitative analysis provided a more nuanced view of the data

- *Example: some had a mental model of a hacker as someone who sat in their basement doing nefarious things*
- Context, perceptions, and experiences were more visible.

Mental Models, Privacy, & Security

- Mental Model: "simplified internal concept of how something works in the real world".[1]
  - Generality, generativity, guidance of skills, organization of information
- Previous research used Mental Models from the physical world to explain user perceptions of privacy and security. [2,3]

1. Asgharpour, P., Liu, D., and Camp, L.J.: Mental models of computer security risks. WOODSTOCK '97. El Paso TX, (1997)
2. Camp, L. J. (2006). Mental models of privacy and security. Available at SSRN 922735.
3. Wash, R.: Folk models of home computer security. In Proceedings of the Sixth Symposium on Usable Privacy and Security. Redmond WA: ACM. p. 1-16, (2010)

What are user's views of Cyber-Security ?

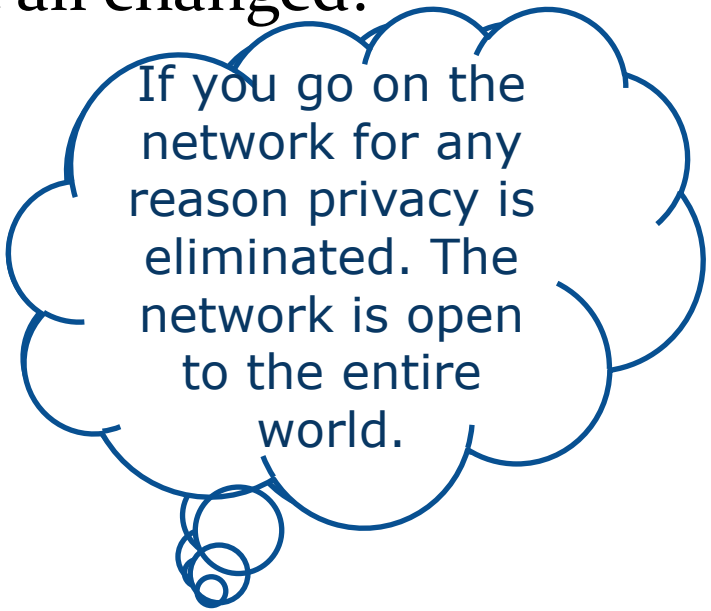
Participants have Multiple Mental Models

- Brave New World
  - Good 'Ole Days
  - No Privacy
- Fatalistic
- Little Value
- Maintenance
- Not My Job
- Optimistic
- Reputation
- Verification

I Can't Keep Up

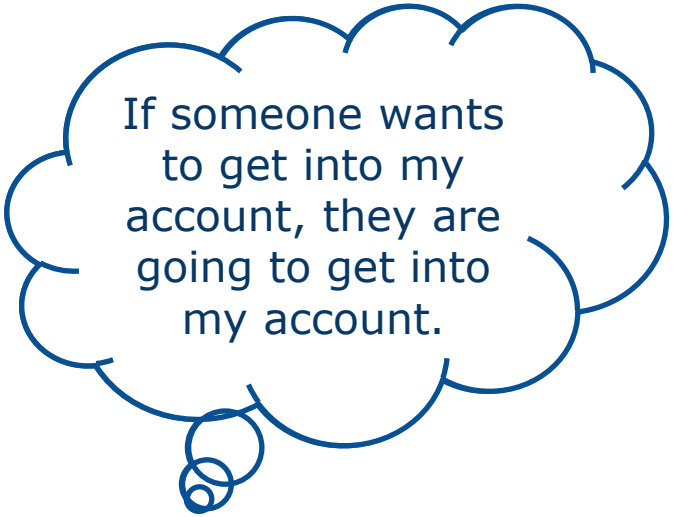
Brave New World Model: Pace, types, and consequences of interactions have all changed:

- No Privacy



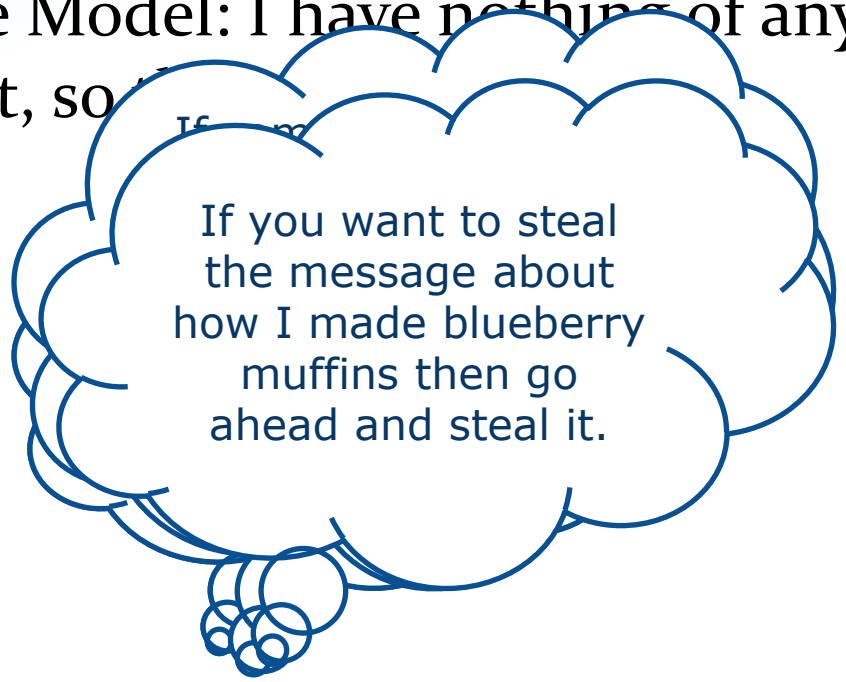
It Doesn't Matter What I Do

Fatalistic Model: a sense of resignation and immunity to worry.



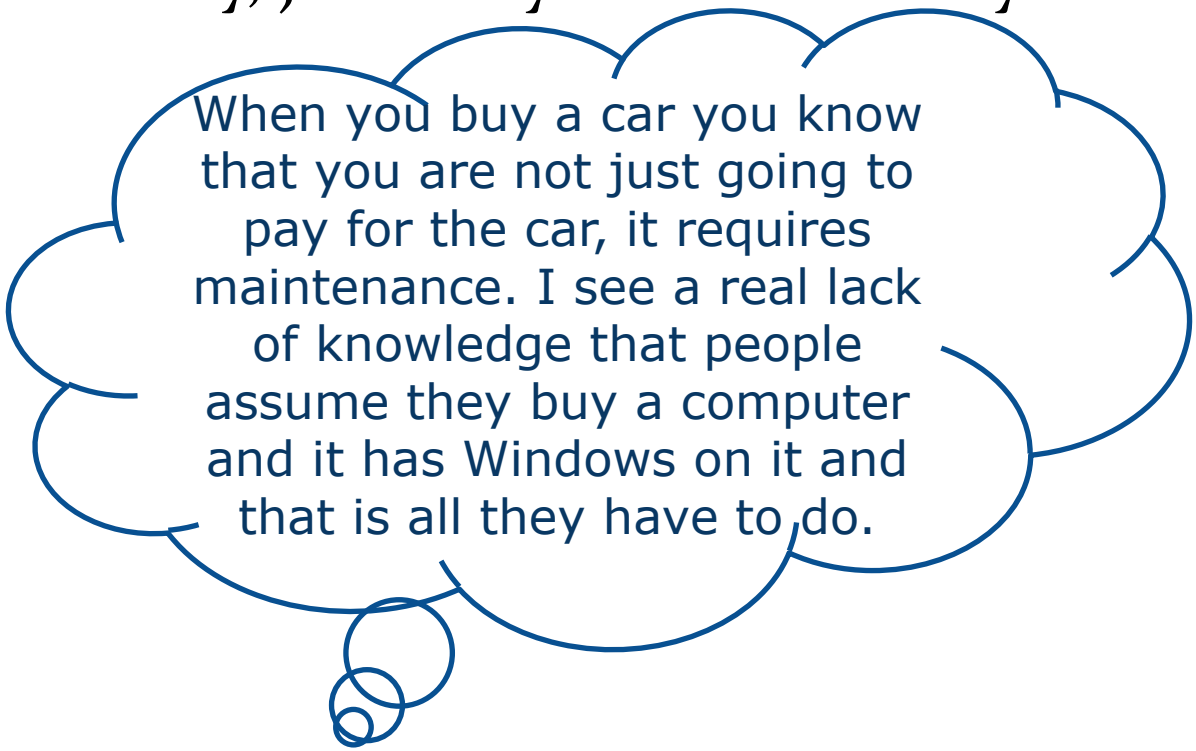
Who Wants a Blueberry Muffin Recipe?

Little Value Model: I have nothing of any value that others would want, so



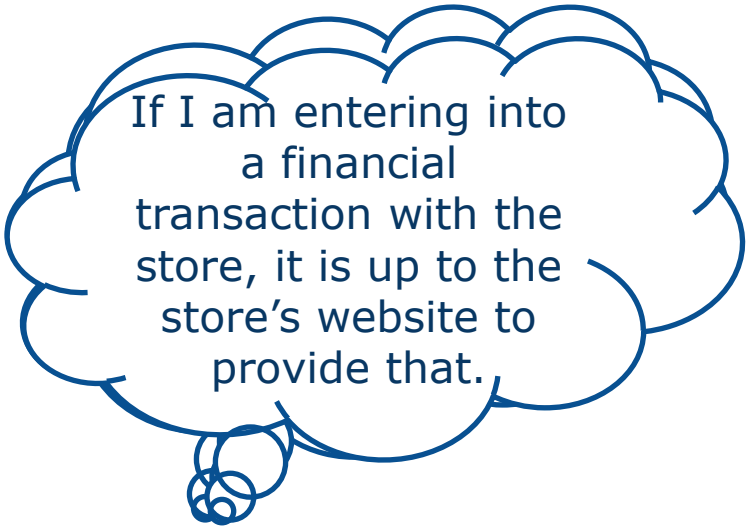
It's Like an Oil Change

Maintenance Model: You need to take care of your computer to ensure security, just like you take care of your car.



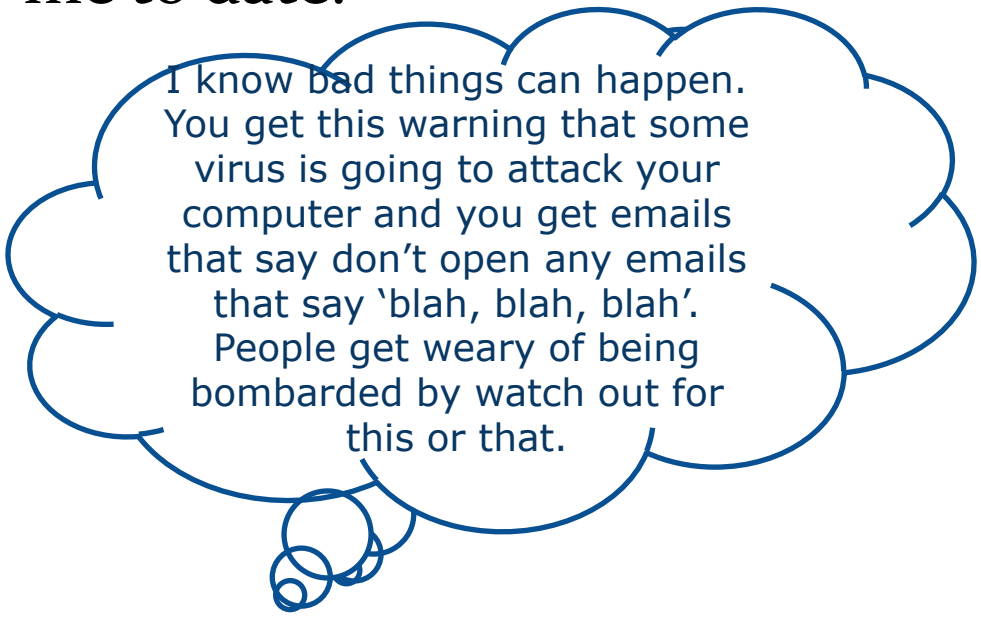
Whose Responsibility Is It Anyway?

Not My Job Model: the responsibility for privacy and security belongs to someone else (e.g., work, IT, the bank, the website…).



Nothing to Hide, Nothing to Fear

Optimistic Model: everything is fine since nothing bad has happened to me to date.

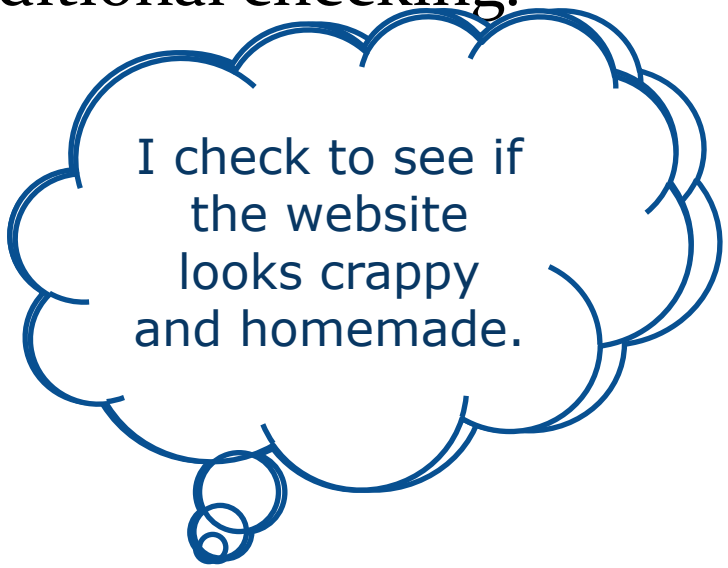


It's What I Know

Reputation Model: Knowing and trusting a specific site or brand because of its size or a previous physical relationship.

More Information Please

Verification Model: Something sets off a trigger that induces the need for additional checking.



Painting the Picture of Privacy & Security

Drawing on Multiple Mental Models:

- Partially formed, contradictory, based on misinformation
- Flip-flopping in use

Our research supports the NIST Computer Security Organization

- Password research results will inform the upcoming NIST SP 800-63-2 revision
  - Policies in plain language
  - Appropriate formatting and ordering
  - Expiry, 3 strikes you're out
  - Type of devices (desktop, mobile)
- Password and Authentication Research supports and informs the NSTIC program
- Mental models supports and informs the NICE and NCCoE programs

Secure in practice not just in theory

Making it easy to do the right thing, hard to do the wrong thing and easy to recover gracefully when the wrong thing happens

Mary Theofanos

maryt@nist.gov