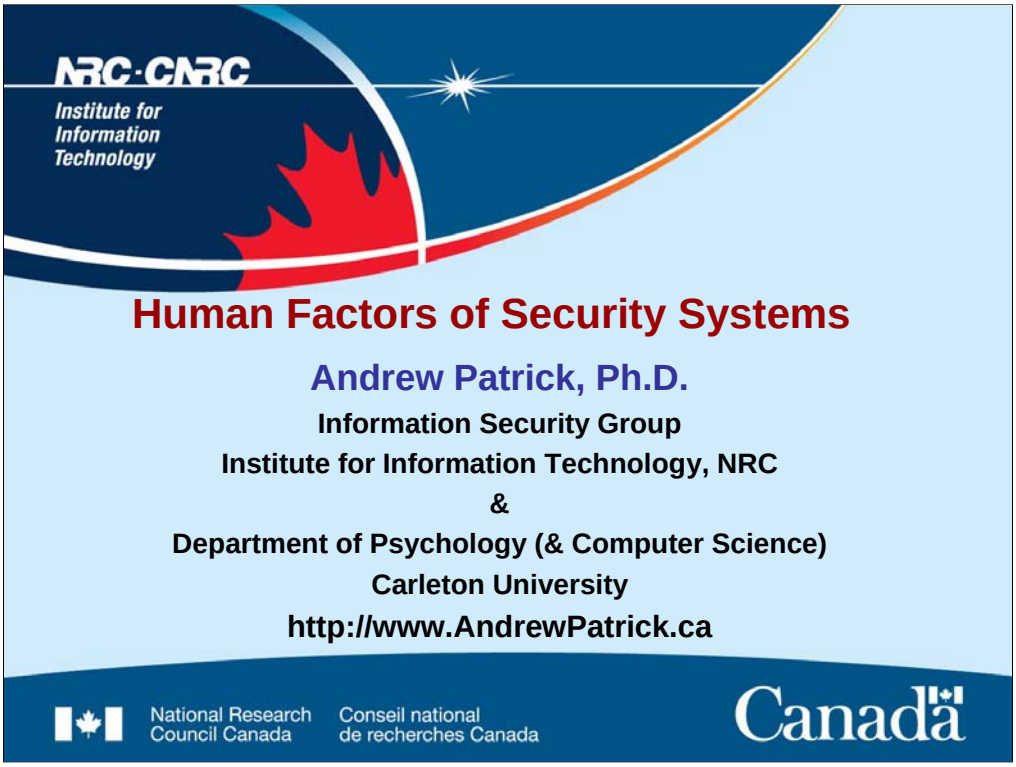
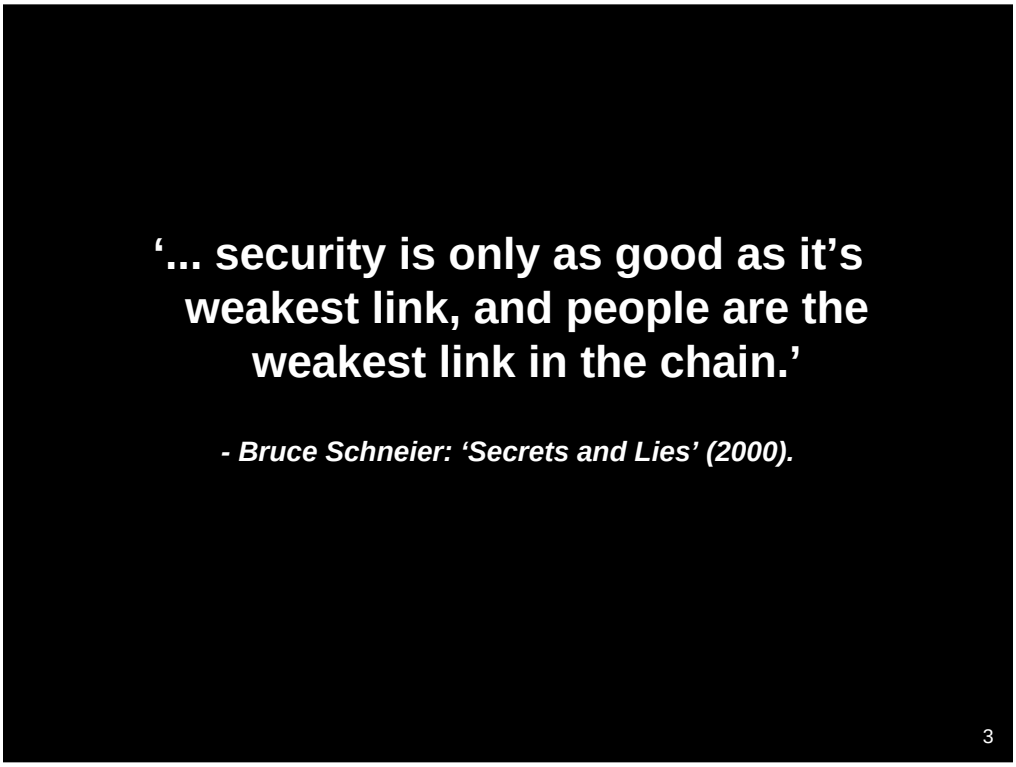


Dr. Andrew Patrick is a Senior Scientist at the National Research Council of Canada and an Adjunct Research Professor of Psychology at Carleton University. He is currently conducting research on new tools for privacy protection, the human factors of security systems, and trust decisions in e-commerce contexts. Prior to joining the NRC, Dr. Patrick worked at Nortel where he managed research and development groups focused on Voice over IP (VoIP) quality, and conducted field research to evaluated new product and service concepts. Dr. Patrick has also worked at the Communications Research Centre, where he conducted research on new multimedia services and natural language interfaces. WWW Site: www.andrewpatrick.ca

Great research on usability and security can be found each year at the Symposium on Usable Privacy and Security (SOUPS).

SOUPS 2009 will take place at Google in Mountain View California.



When we talk about humans and security, this is the typical message that we hear.

"... the human side of computer security is easily exploited and constantly overlooked. Companies spend millions of dollars on firewalls, encryption and secure access devices, and it's money wasted, because none of these measures address the weakest link in the security chain"

- Kevin Mitnick, 2000

4

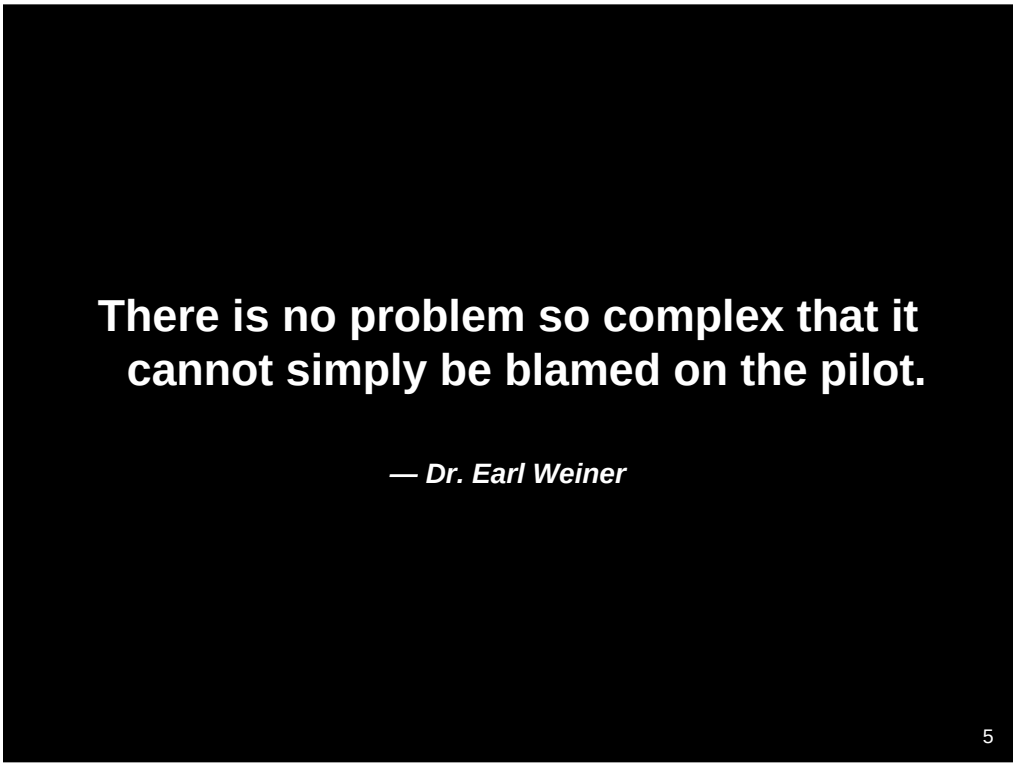
… and here is another. Mitnick was referring to his successful social engineering attacks.

…a famous computer cracker, who was convicted of wire fraud and of breaking into the computer systems of Fujitsu, Motorola, Nokia, and Sun Microsystems.

Mitnick served five years in prison (four years of it pre-trial), 8 months of that in solitary confinement, and was released on January 21, 2000. During his supervised release, which ended on January 21, 2003, he was initially restricted from using any communications technology other than a landline telephone.

He offers security consulting services through his company Mitnick Security Consulting, LLC and has co-authored two books on computer security. The books are *The Art of Deception* (2002), which focuses on social engineering, and *The Art of Intrusion* (2005), focusing on real stories of security exploits.

Bio from wikipedia:



*** I want to draw a parallel between the state of information security today and the state of airline safety 20 years ago. Back then, it was very common to blame airline accidents on "pilot error", without an investigation to factors that led to that error.**

*** The same is true for information security today. We are too quick to blame the users, without spending enough time understanding, and remedying, the factors that lead to the users' behavior.**

*** A lot of progress was made in airline safety when a systems approach was adopted, and the same can be done for IT security.**

So, what do users do?

They write their passwords down and store them in unsafe places.

Any they make easy to remember (easy to guess) passwords.

They share their passwords with friends and coworkers.

Passwords revealed by sweet deal

More than 70% of people would reveal their computer password in exchange for a bar of chocolate, a survey has found.

It also showed that 34% of respondents volunteered their password when asked without even needing to be bribed.

Security crumbles in the face of sweet bribes

8

And they give away their passwords to just about anybody who asks.

*** And, they are susceptible to phishing attacks – being lured to false web sites to give-up their username/password credentials.**

*** A recent report suggested that 5% of people respond to phishing messages.**

Report on Phishing

A Report to the Minister of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States

Binational Working Group on Cross-Border Mass Marketing Fraud
October 2006

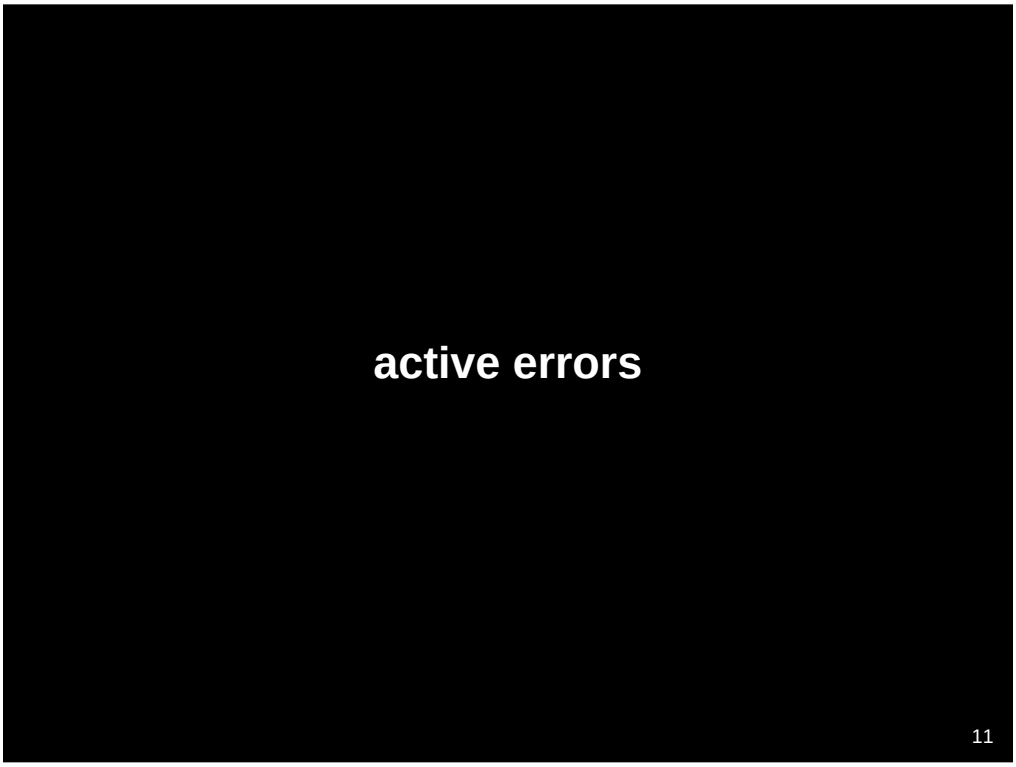
James Reason:

*** blaming the fallible individuals at the front end is universal, natural, satisfying, and convenient**

*** but it does little to solve the problem**

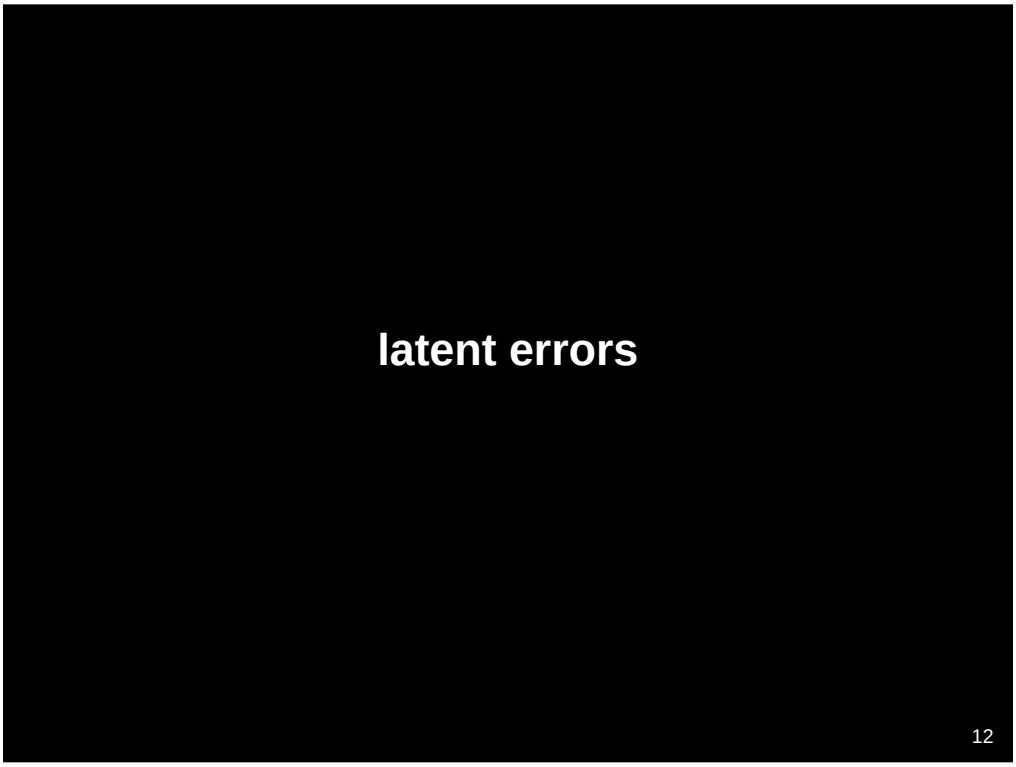
*** and may put focus on the wrong person**

*** and leads to ineffective fixes (e.g., training, procedures, policies, supervision)**



errors made by an individual that directly leads to a problem

e.g., sharing a password



* delayed-action errors made by a system or organization
* consequences are indirect
* often related to design, construction, operation, etc.
* e.g., Chernobyl accident
* e.g., not supporting collaboration between workers

James Reason, talking about Chernobyl Five phases:

1. organizational process leading to latent errors

2. error-producing conditions within specific places

3. active errors made by individuals

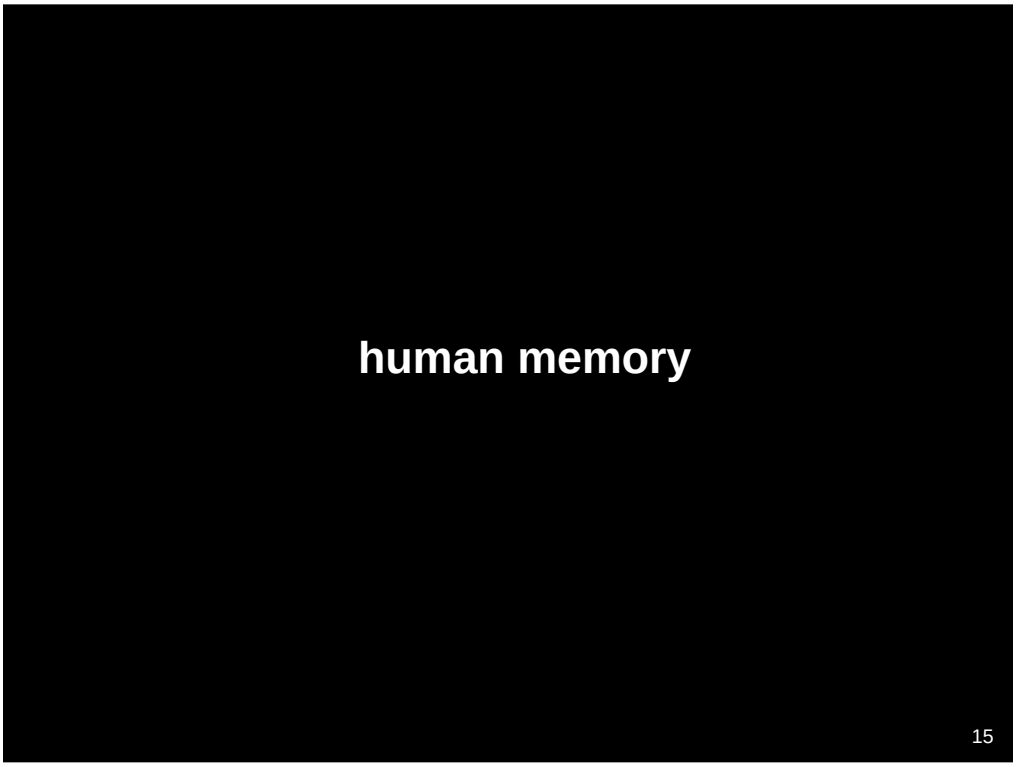
4. events in which one or more safeguards are by-passed

5. outcomes that vary in severity of consequences (free lessons vs. catastrophes)

cognitive psychology

14

* the study of the functions of the human mind
* features, characteristics, limitations
* thoughts, emotions, behaviors are systematic, predictable
    * so we can design with them in mind



characteristics of human memory

*** limited capacity of working memory**

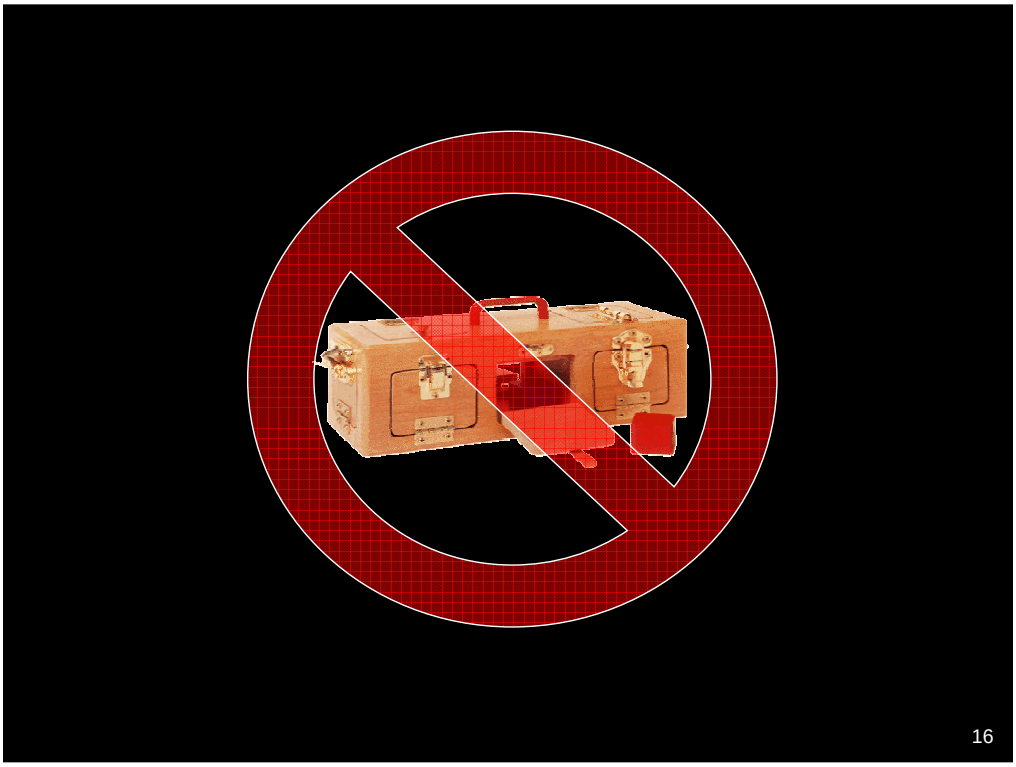
*** decay over time**

*** memory for gist & meaning rather than literal details**

*** strengthening by repetition, weakening by time**

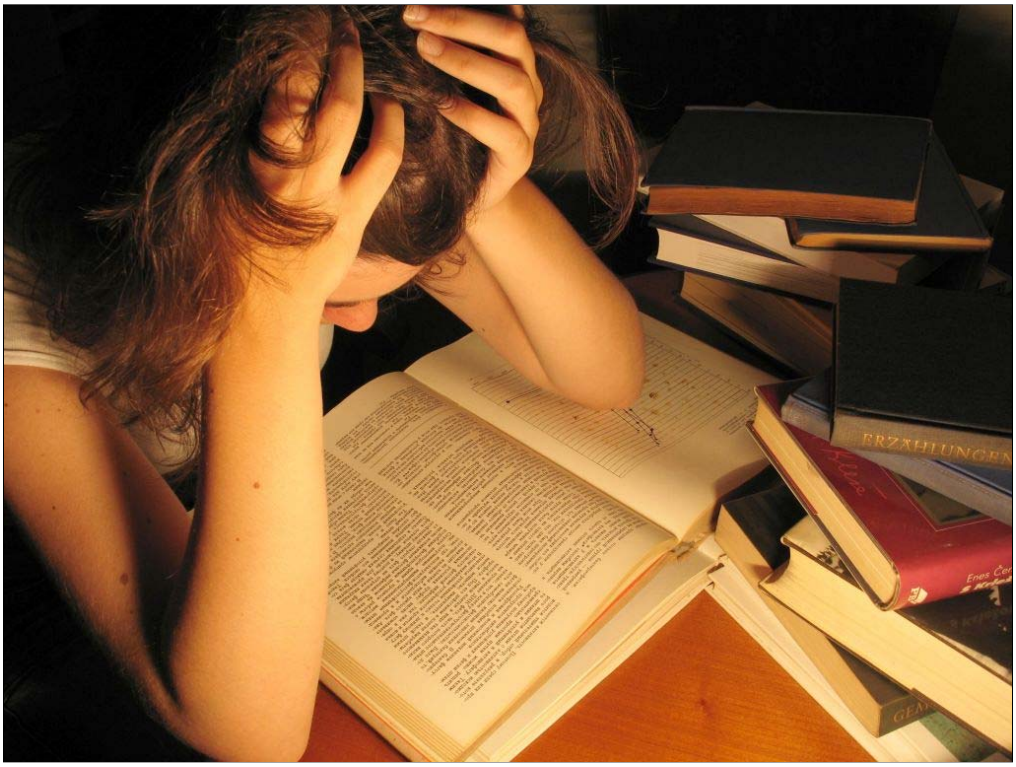
*** cannot forget on demand**

*** recognition better than recall**



- **memory is not a set of compartments where experiences are locked away**

- **memory is meaningful, constructions, schemas, etc.**

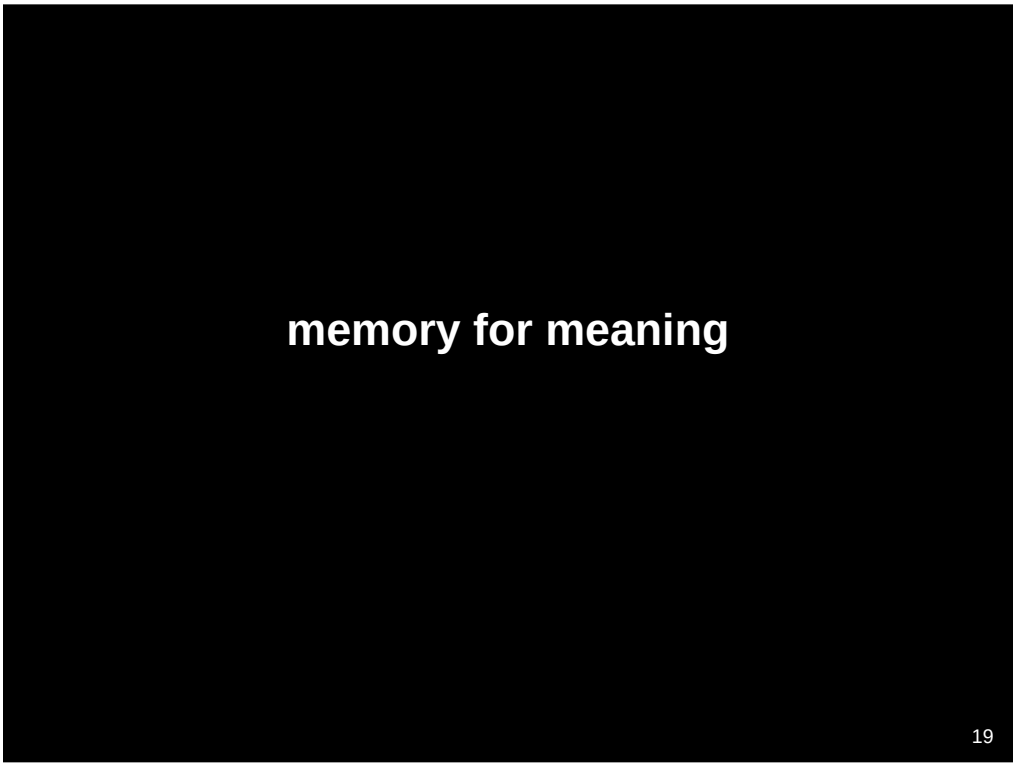


Learning takes time and repetition

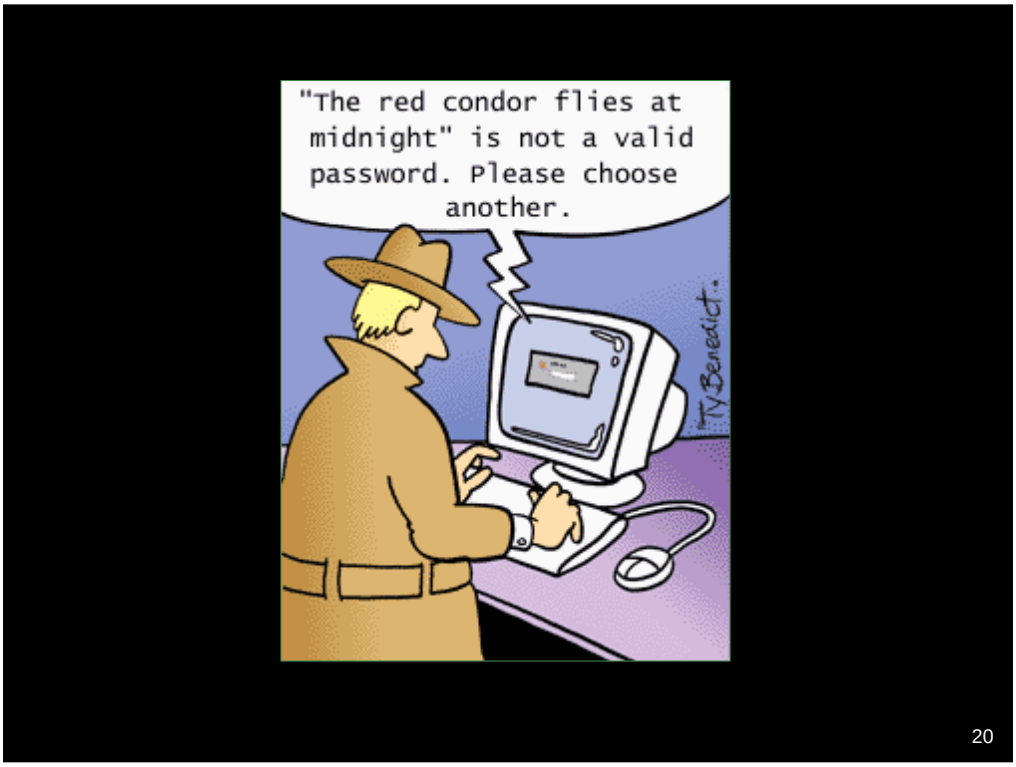
I use a unique password for each login account that I have.

I have collected about 200 different passwords.

I use KeePass to maintain them. Protected by a master key, and stored on an encrypted USB device.



Human memory is constructive and meaningful. We do poorly at remembering random things and much better when the memories have meaning.



… and yet, we are often force to use meaningless passwords

•arbitrary password restrictions?

• exactly 8 characters?

• must have punctuation?

Table 1: Examples of Memorable Phrases and Passwords

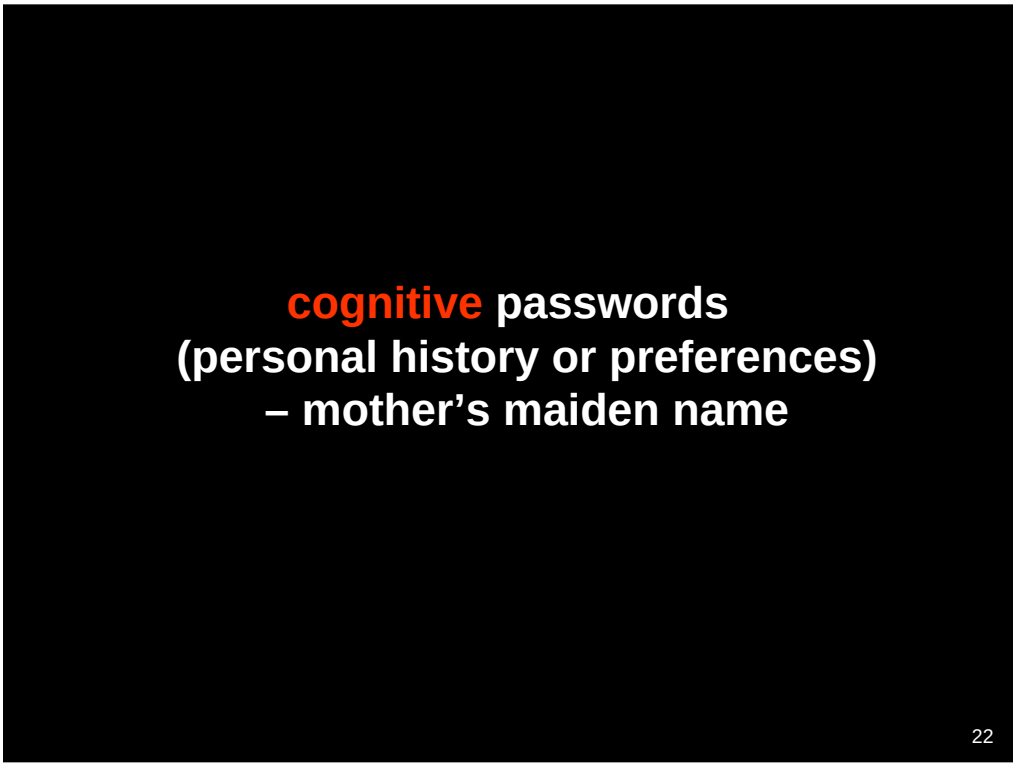
Phrase	Password	Inspiration
Four score and seven years ago, our Fathers	4s&7yaoF	Quotation – Gettysburg Address
I love to ski at Seven Springs!	Ilts@7S!	Personal – Hobby
Alas, poor Yorick! I knew him, Horatio	A,pY!Ikh,H	Literature - "Hamlet" by Shakespeare

21

So, we should adopt techniques that make passwords more meaningful…

HUMAN SELECTION OF MNEMONIC PHRASE-BASED PASSWORDS

Cynthia Kuo, Sasha Romanosky, and Lorrie Faith Cranor (Carnegie Mellon University) SOUPS 2006



… PVQs are based on knowledge, rather than on arbitrary memories

	Password	PVQ answer
CIBC	6-12	4-21 (2 PVQs)
RBC	8-32	4-20 (3 PVQs)
TD	5-8	functionality absent
Scotiabank	8-16	functionality absent
BMO	6	functionality absent
PC Financial	6-12	1-20 (3 PVQs)

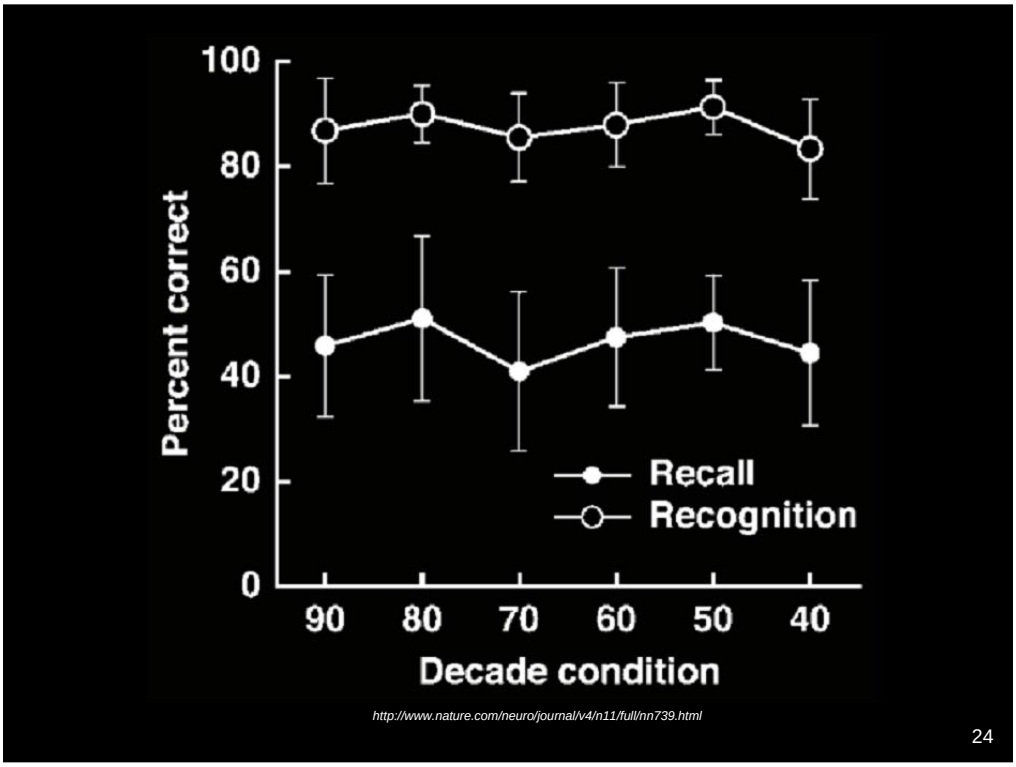
Table 2: Comparing password and PVQ answer length across six banks

Mohammad Mannan, NSPW 2007

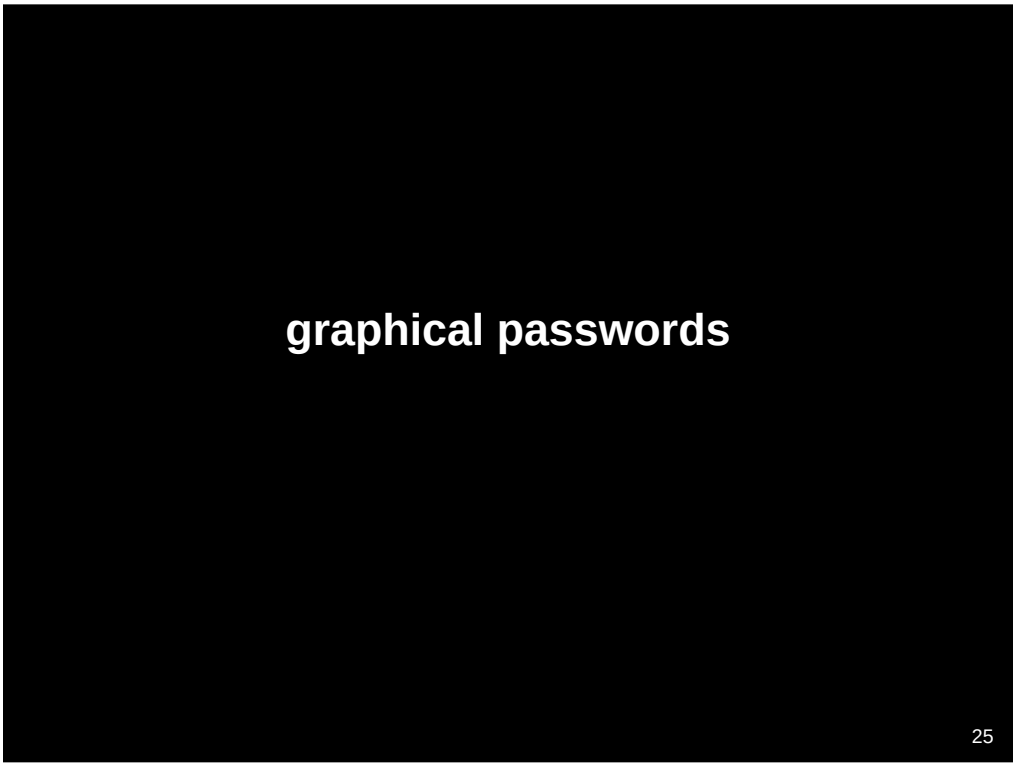
23

… but users are confused about what kinds of passwords to create

Also, users are sometimes, but not always, asked to make Personal Validation Questions (PVQs), also called Challenge Questions



… and we know that we are much better at recognition tasks then we are for recall tasks.

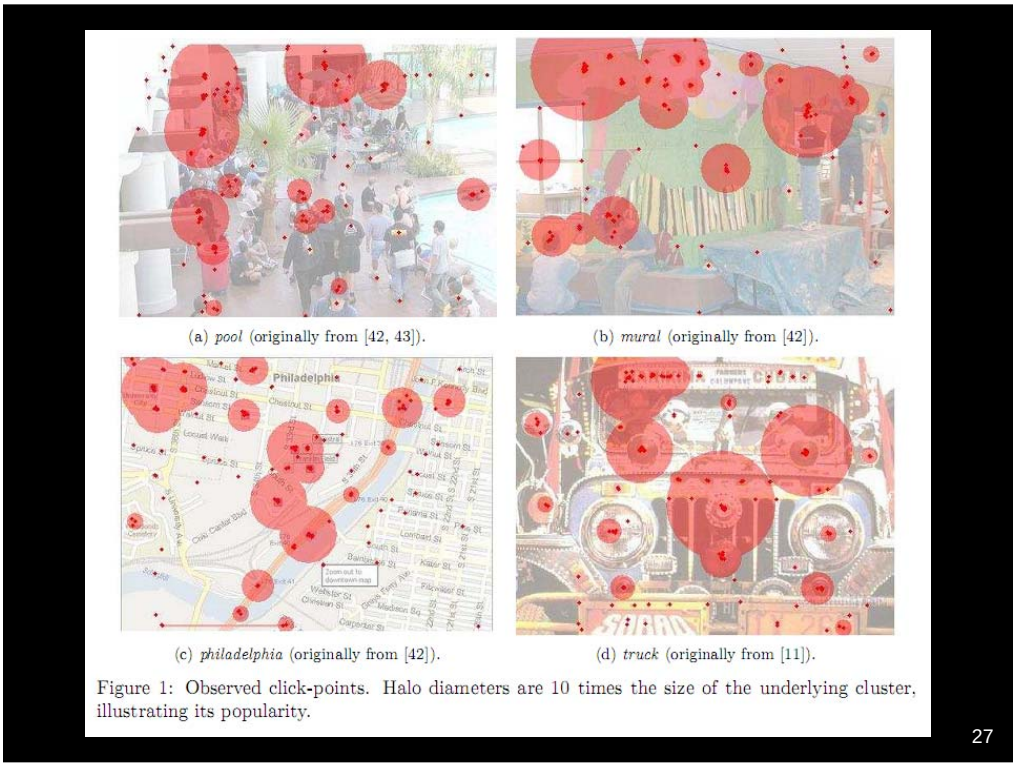


Some people are starting to explore graphical passwords…

Sonia Chiasson

26

In the PassPoints system, people choose 5 points on an image, and have to repeat them later when the login.



(a) *pool* (originally from [42, 43]).

(b) *mural* (originally from [42]).

(c) *philadelphia* (originally from [42]).

(d) *truck* (originally from [11]).

Figure 1: Observed click-points. Halo diameters are 10 times the size of the underlying cluster, illustrating its popularity.

27

… although the system is fairly easy to use, people tend to choose the same click points as other people

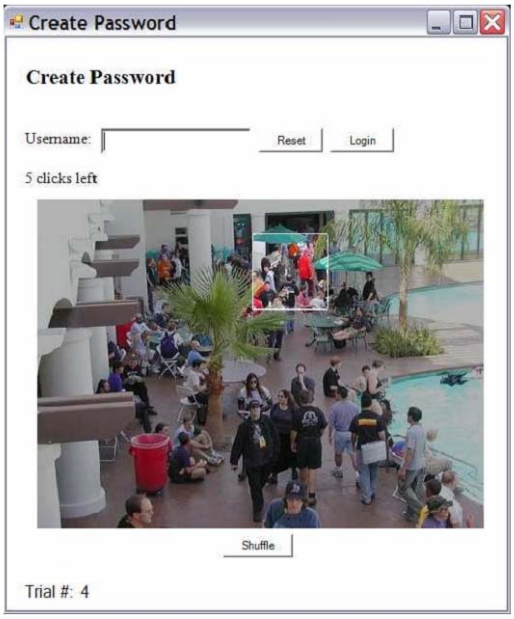


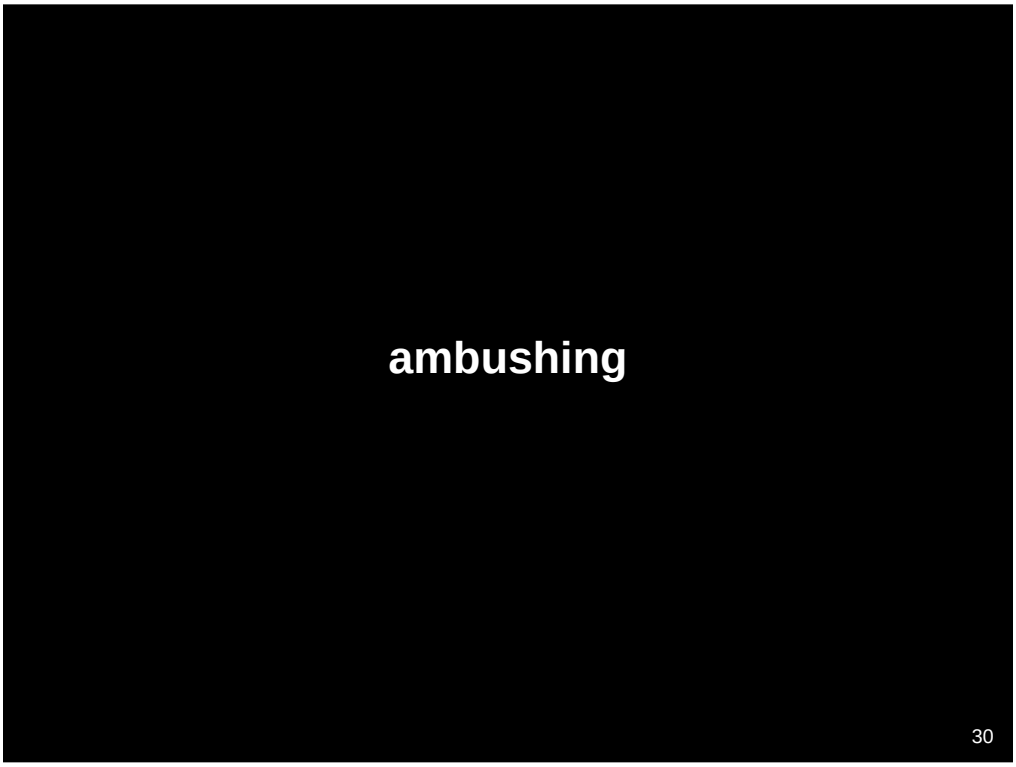
Figure 2: Screenshot of the PCCP Create Password interface with the viewport highlighting a portion of the image. (Pool image from [14])

28

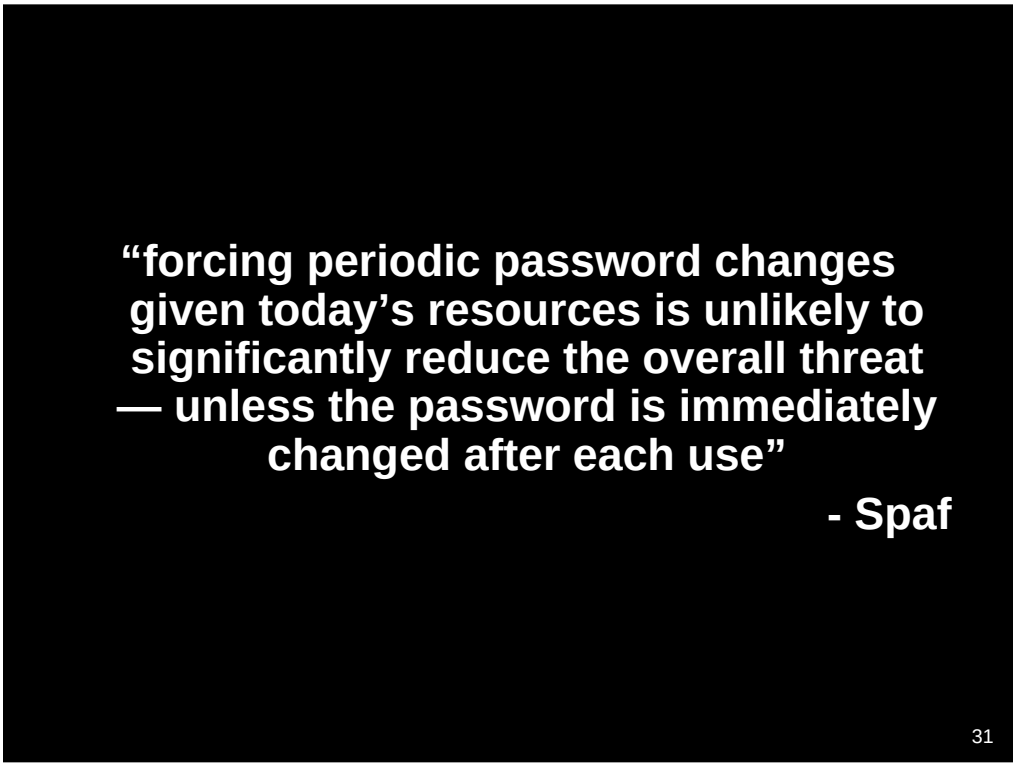
So one technique is to guide them to random parts of the image so everyone does not click at the same places.

… this increase security, but what does it do for usability?

Another characteristic of human memory is that we cannot forget on demand.



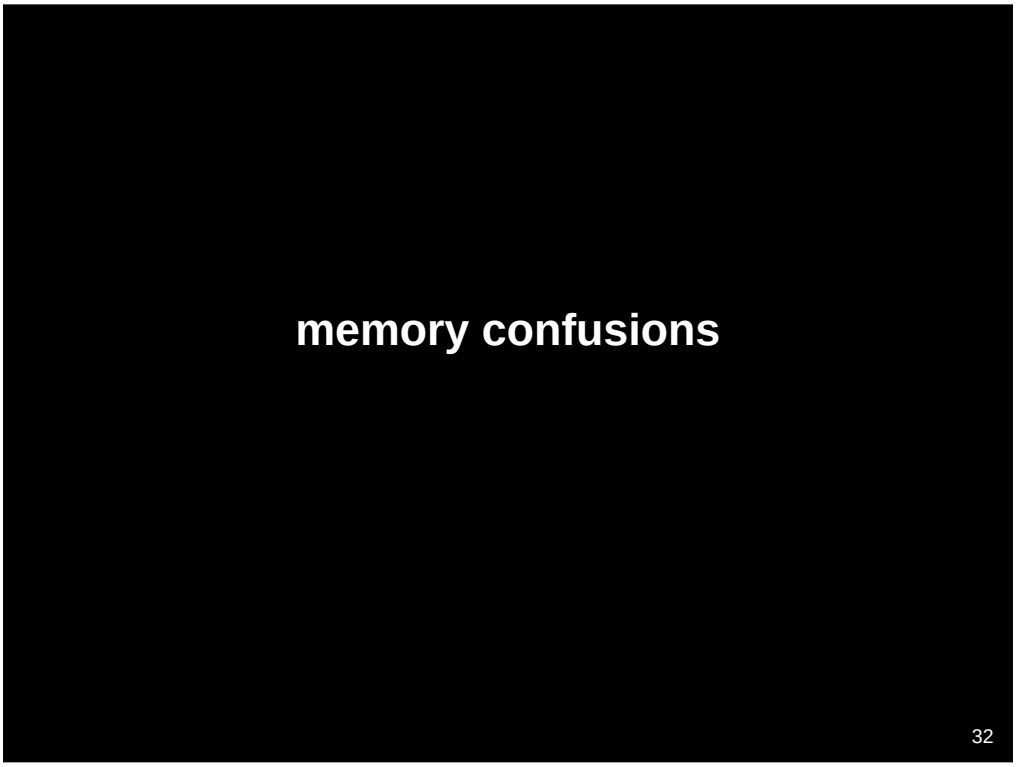
but, we often require people to change their password immediately, with no warning, when they want to do their primary task



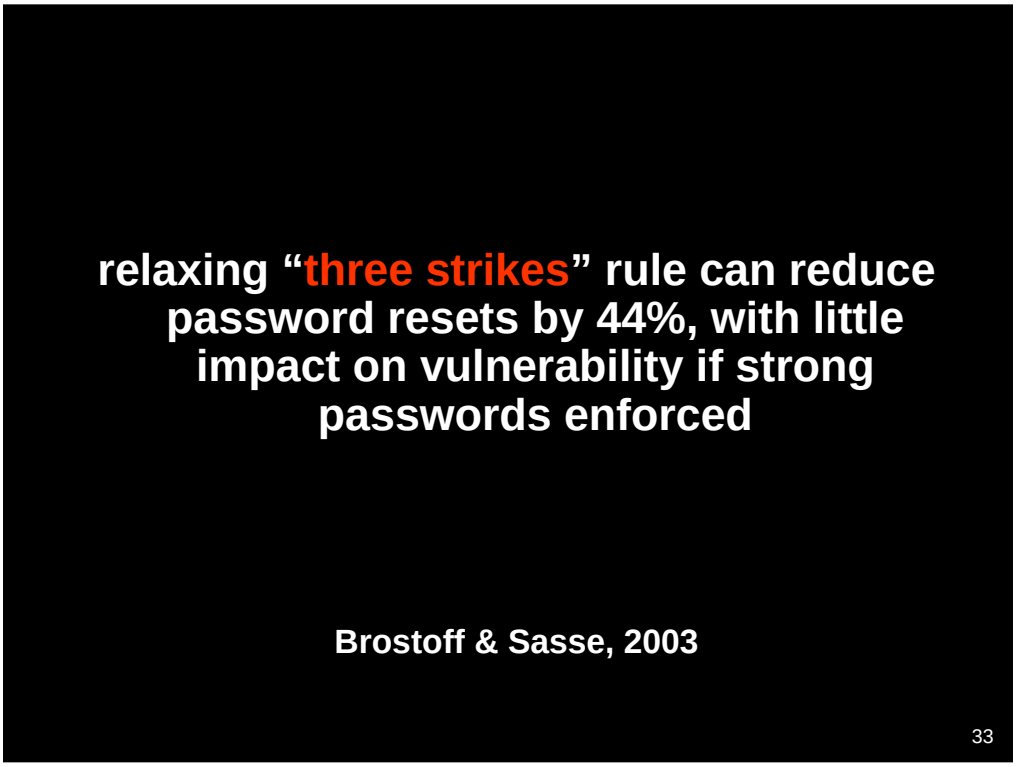
Changing passwords only provides protection against guessing and weak cracking. For other attacks, periodic changes are too late. Today’s threats come from disclosure, inference, loss, and snooping.

http://www.cerias.purdue.edu/weblogs/spaf/general/post-30/

Eugene Spafford, Purdue U



We often confuse memories, or two similar memories, rather than forget them completely



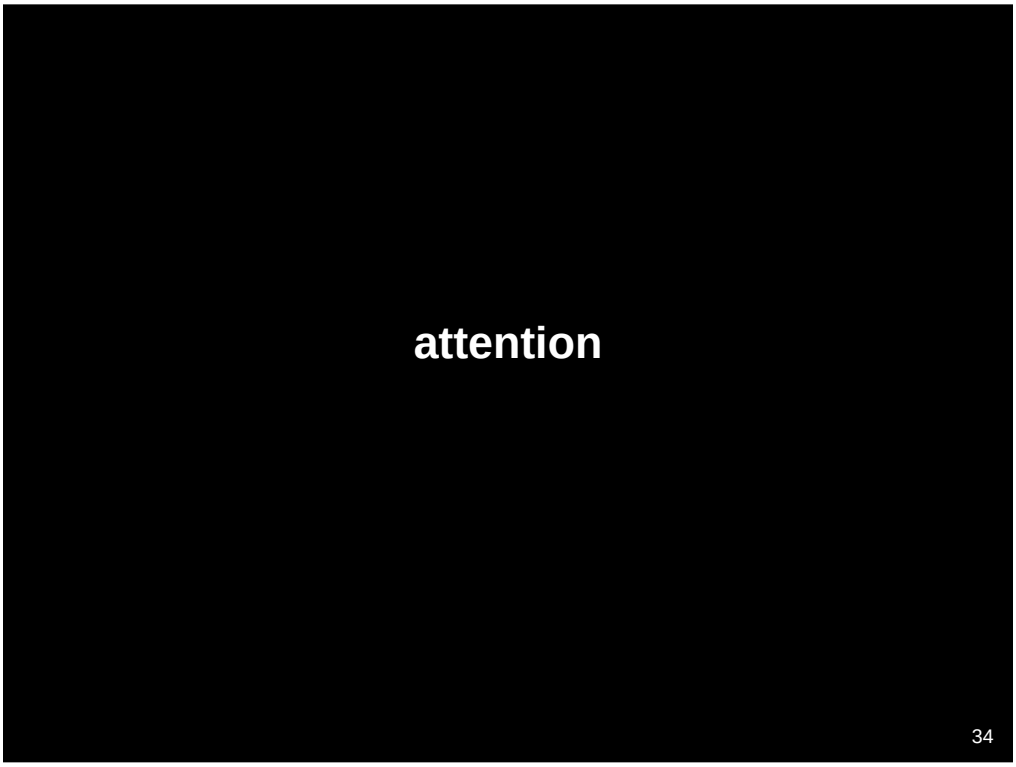
… and since memory is imperfect and reconstructive, we can accommodate it by relaxing some arbitrary restrictions

most failures to remember passwords are confusions, not forgetting (wrong password, old password)

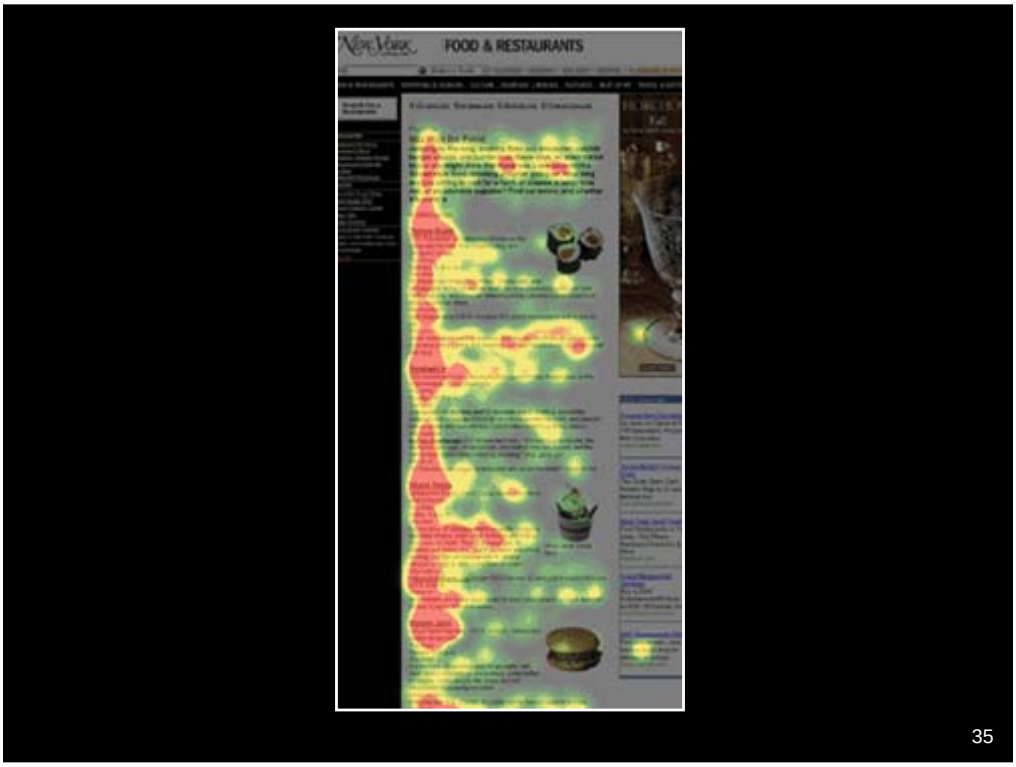
"Ten strikes and you’re out": Increasing the number of login attempts can improve password usability *(revised February 18 2003)*

Sacha Brostoff and Angela Sasse

HCISEC workshop, 2003

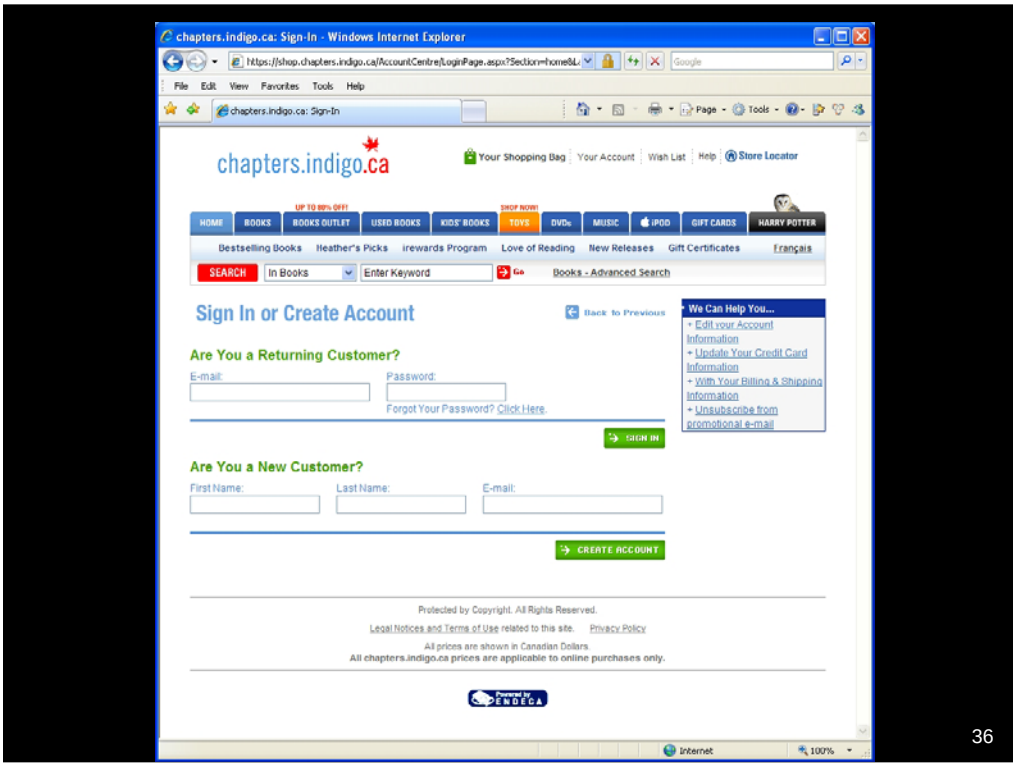


people can be very task-focused



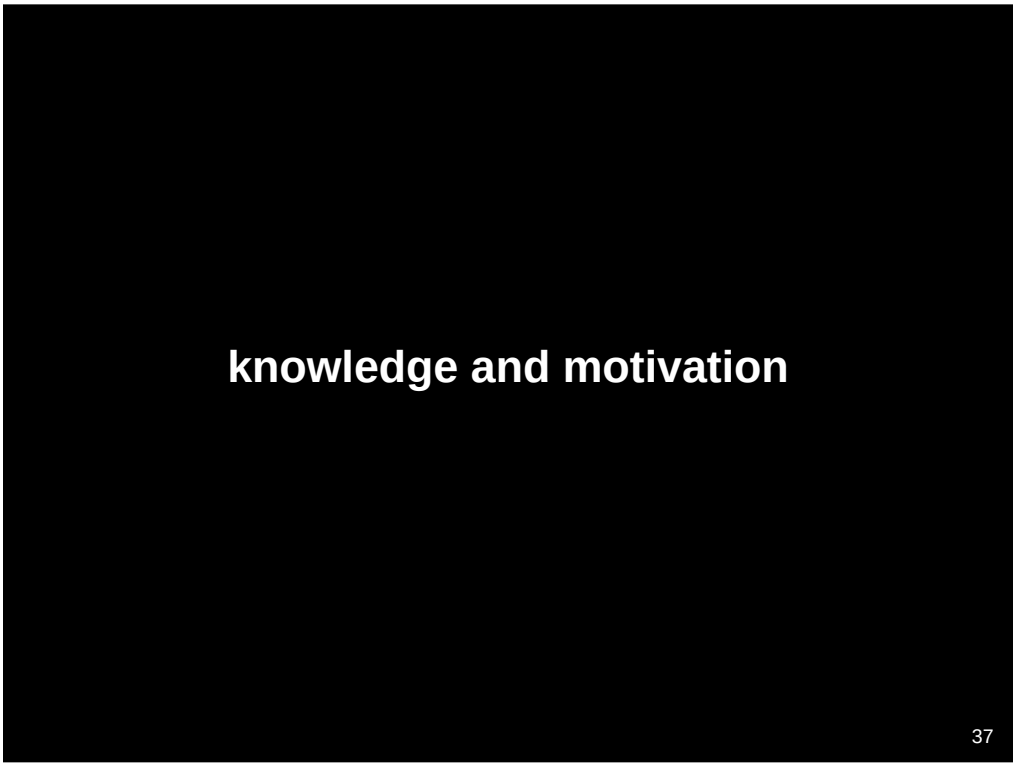
*** scanning patterns of web sites**

*** shows that people selectively scan based on knowledge of where key information is found**

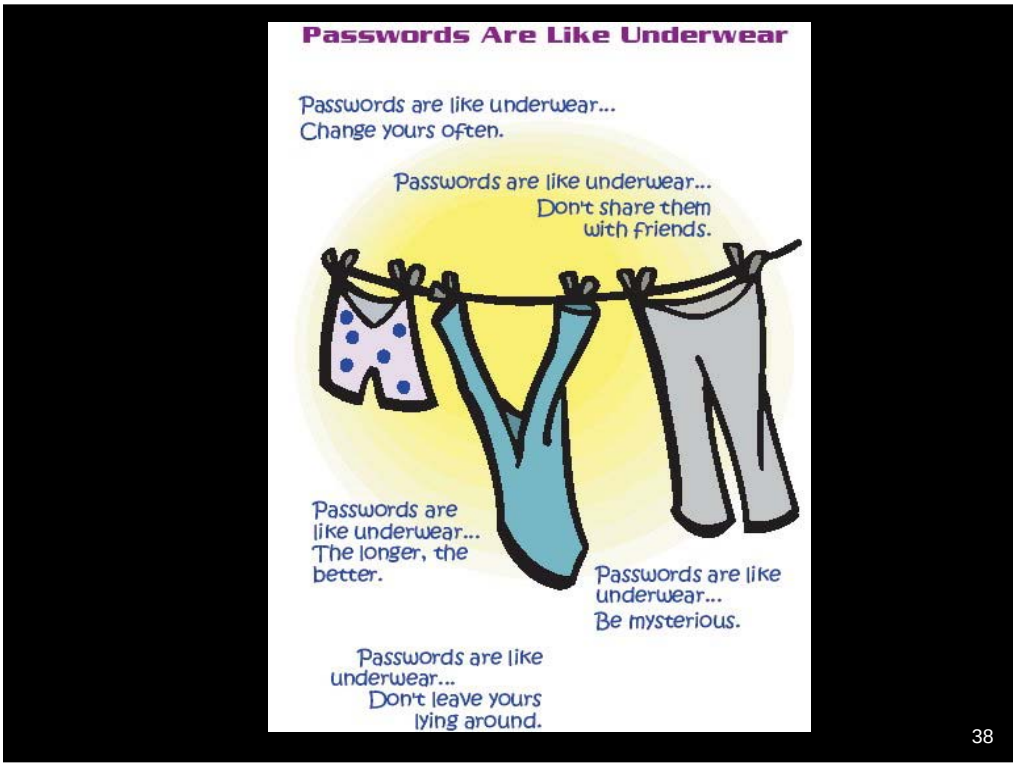


36

… and yet we expect people to pay attention to the presence or absence of a small lock icon far from the key information in a browser display

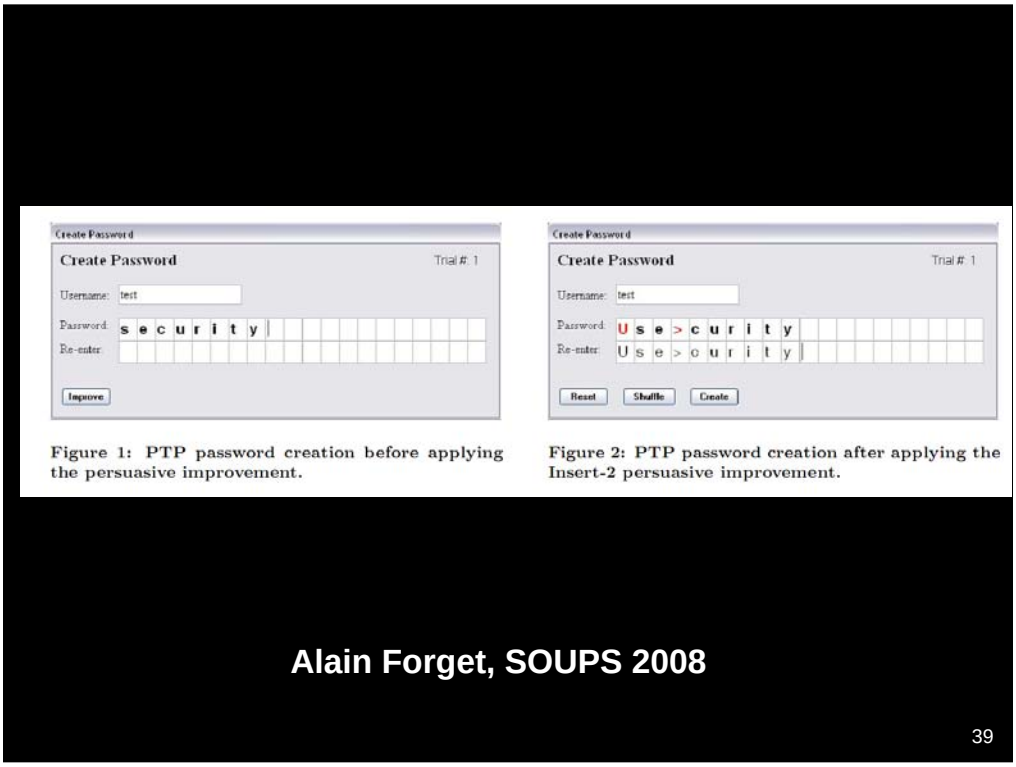


* security is at best an enabling task, and at worst a barrier to real work
* security consciousness can be linked to fear of being labeled “paranoid” or untrusting
* password sharing as a sign of trust
* perceptions of unimportance: nobody will target me, and what would they get if they did
* perceptions of helplessness: hackers will get in anyway
* security policies and procedures unrealistic and user not accountable
* using security encourages others to try to break-in



… so we can train people why and how to use passwords

University of Michigan



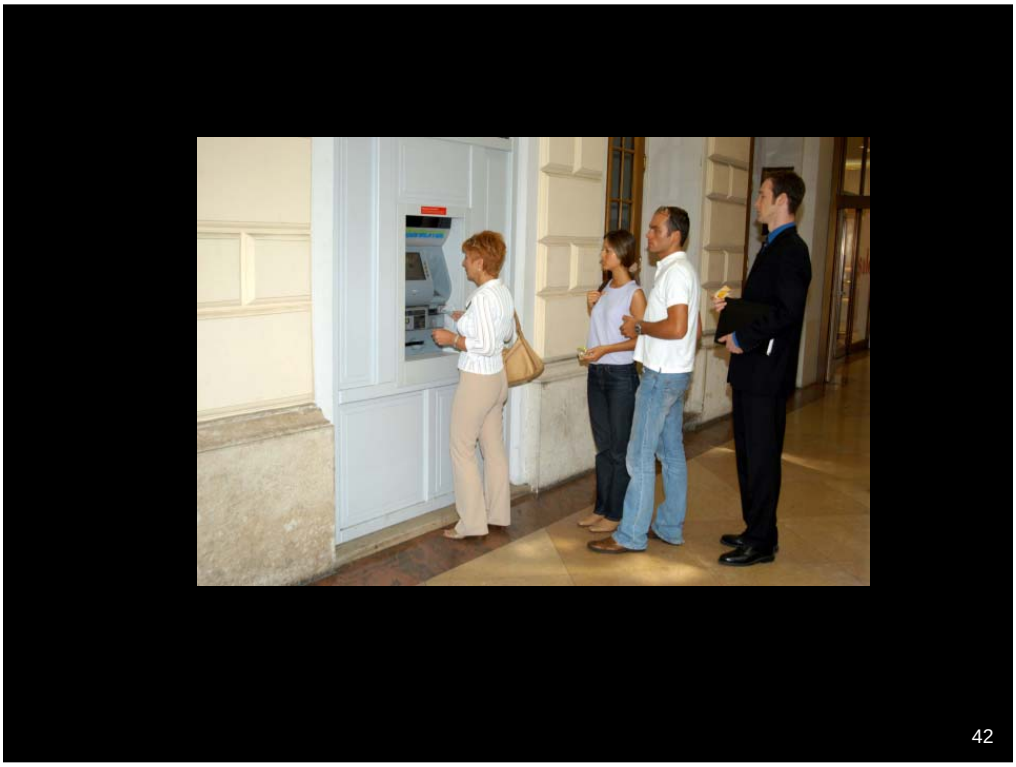
… and we can try to guide them to create better passwords

… this technique was not very successful

Human social behavior also affects security…

time

embarrassment



imagine you are using the machine and can’t remember your password, or can’t get your fingerprint to be recognized

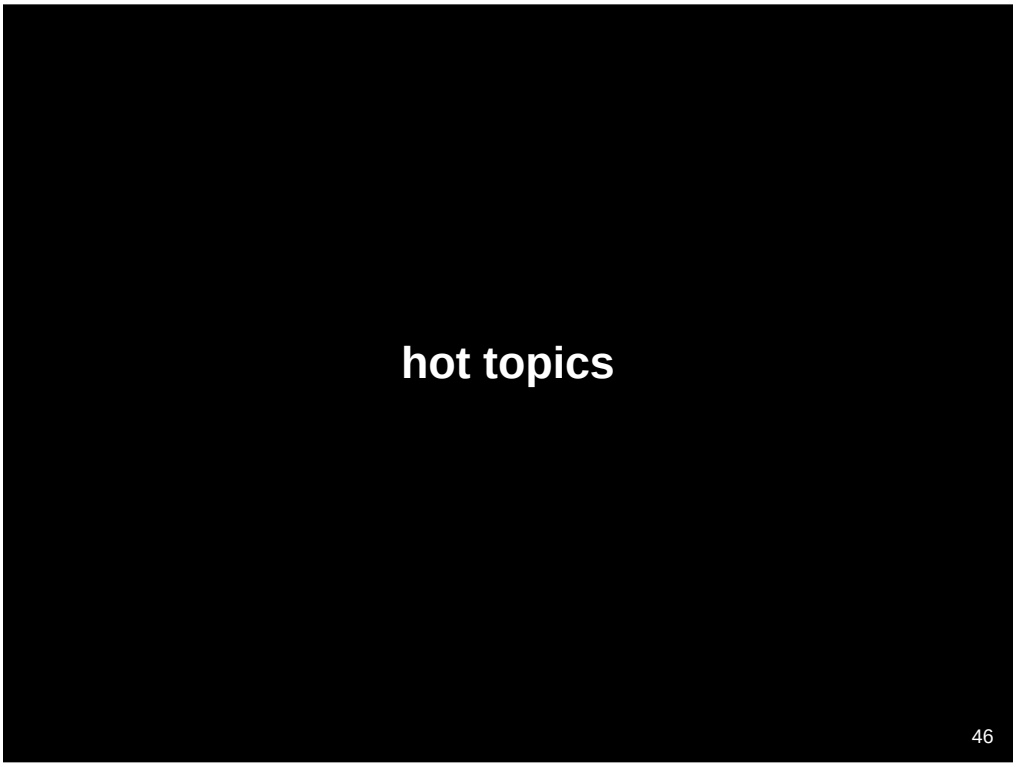
All security behaviors take place in a social context, and people are very social animals.

imagine you are working in an organization that has this as their physical security measure

*** people usually work in groups, where information sharing is essential**

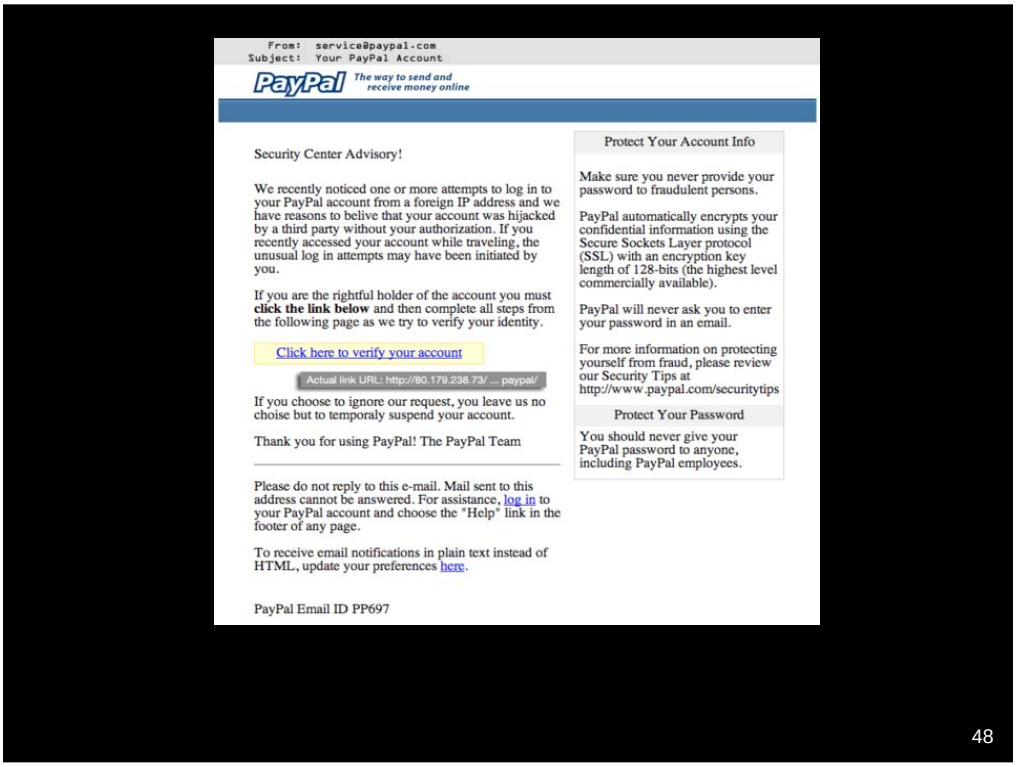
*** and yet, the information system are often not designed to support the level of sharing that goes on**

*** with no other alternative, users will resort to nasty habits, such as password sharing**



new topic: current hot topics in usability and security

Phishing continues to be a major security problem.



Link in the email does not lead to Paypal, but instead to a server in China.

This attack actually writes the address bar, making it harder to recognize as a scam.

*** Notice that the user is asked for their PIN for their bank card!**

*** This is the most common type of phishing attack because of the ease of "cashing" (to be discussed later).**

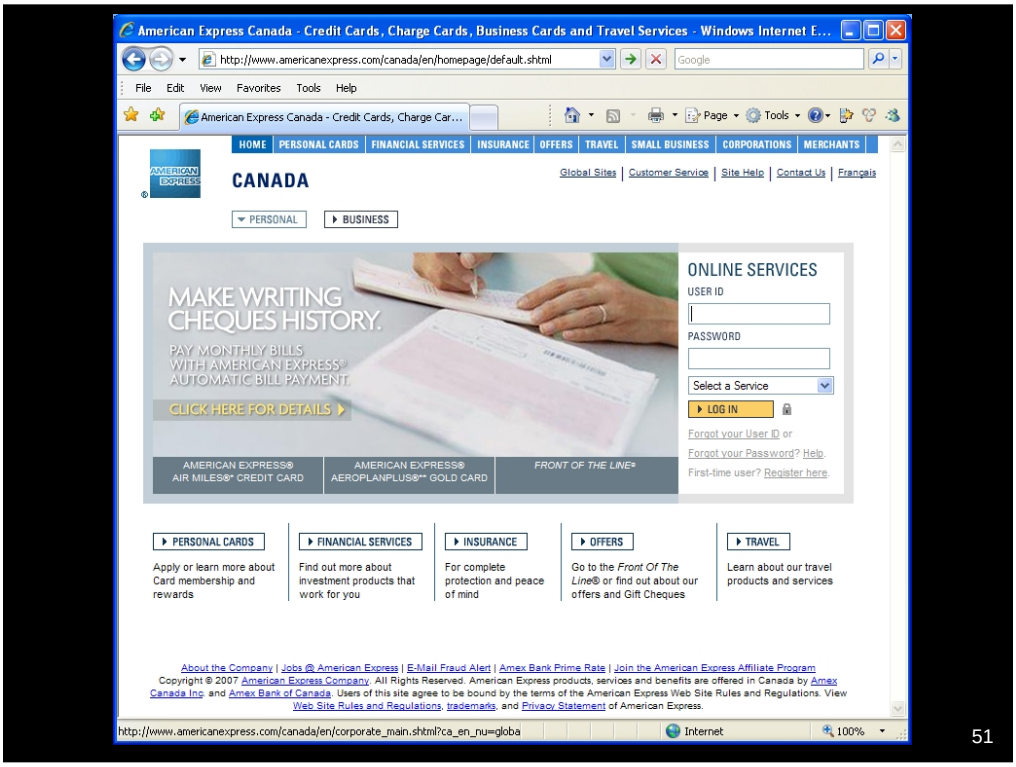
From the Anti-Phishing Working Group

*** supposed to provide site authentication**

*** but, we have seen, anybody can buy a certificate**

*** and many web sites don’t use them properly (e.g., http on page with login form)**

*** and browsers/users not good at checking certificates**



Here the AMEX page is asking for the User ID and password, but there is no SSL connection so there is no indication that the transmission would be sure, other than a loc icon right on the page.

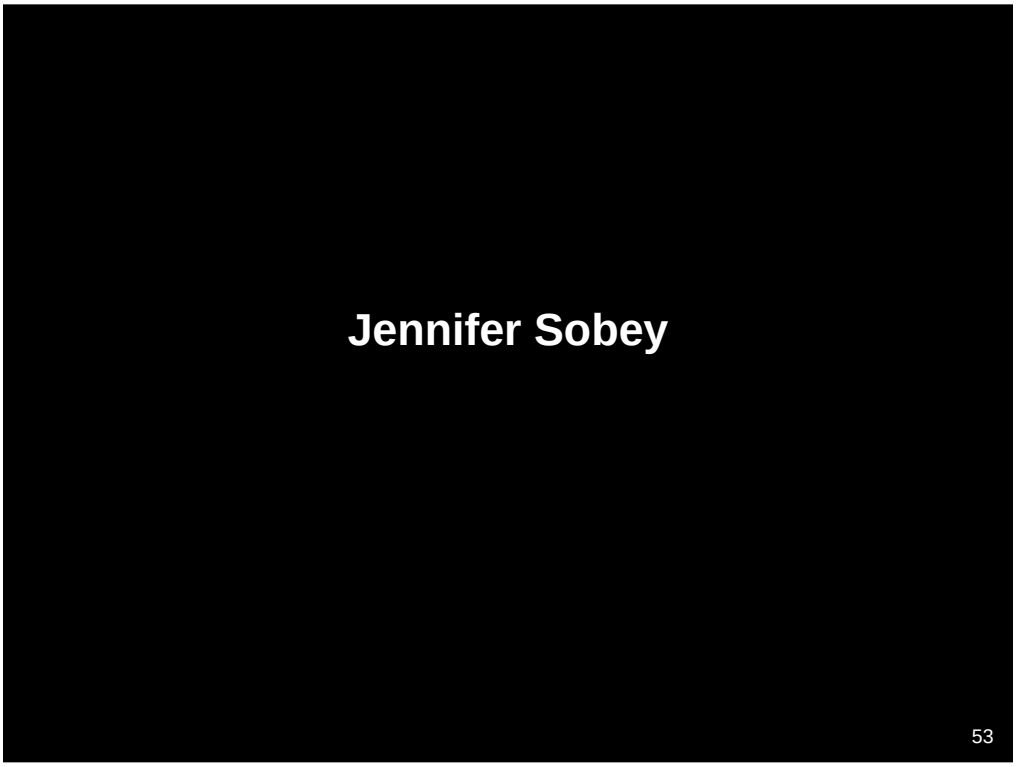
	Common Name (CN)	Organization (O)	Signing CA	Encryption
CIBC	www.cibconline.cibc.com	Canadian Imperial Bank of Commerce	RSA	RC4 128
RBC	www1.royalbank.com	Royal Bank of Canada	Verisign	RC4 128
TD	easyweb.tdcanadatrust.com	The Toronto Dominion Bank	RSA	AES-256
Scotiabank	www.scotiaonline.scotiabank.com	Bank of Nova Scotia	RSA	RC4 128
BMO	www1.bmo.com	Bank of Montreal	Entrust.net	RC4 128
PC Financial	www.txn.banking.pcfinancial.ca	Loblaw Companies LTD	RSA	RC4 128

Mohammad Mannan, NSPW 2007

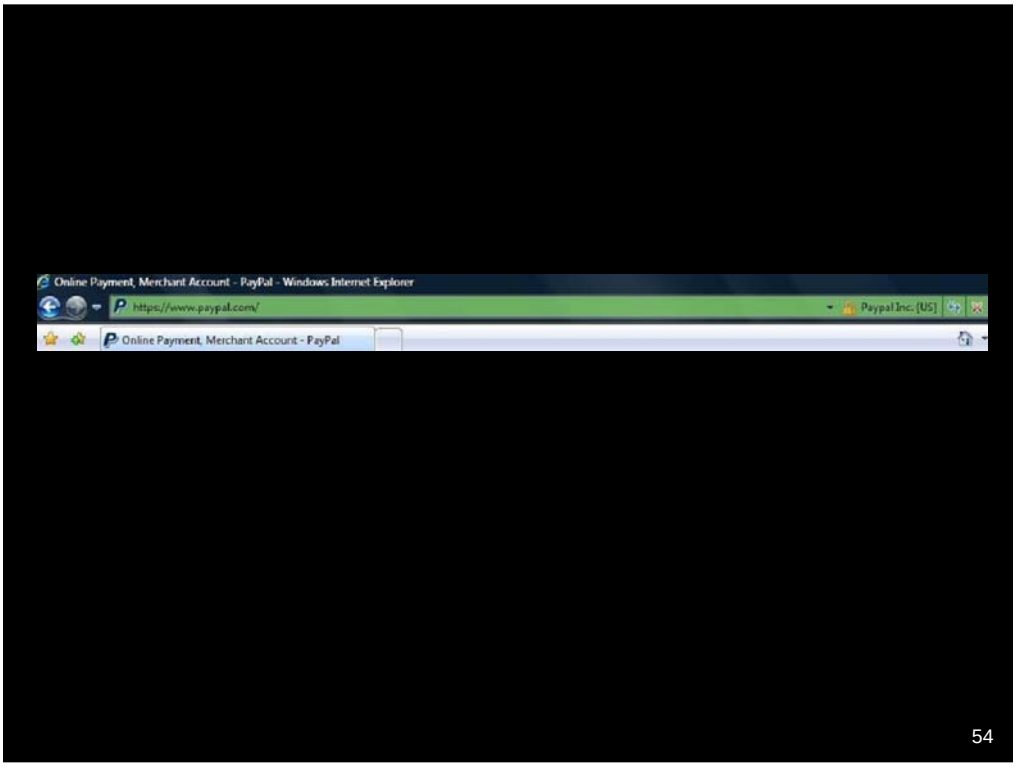
52

… and even if users look for and examine the certificate, the information is very confusing. Note the differences between the branding, Common Name (URL), and Organization Name.

… even worse is when institutions farm-out their online services to third parties.



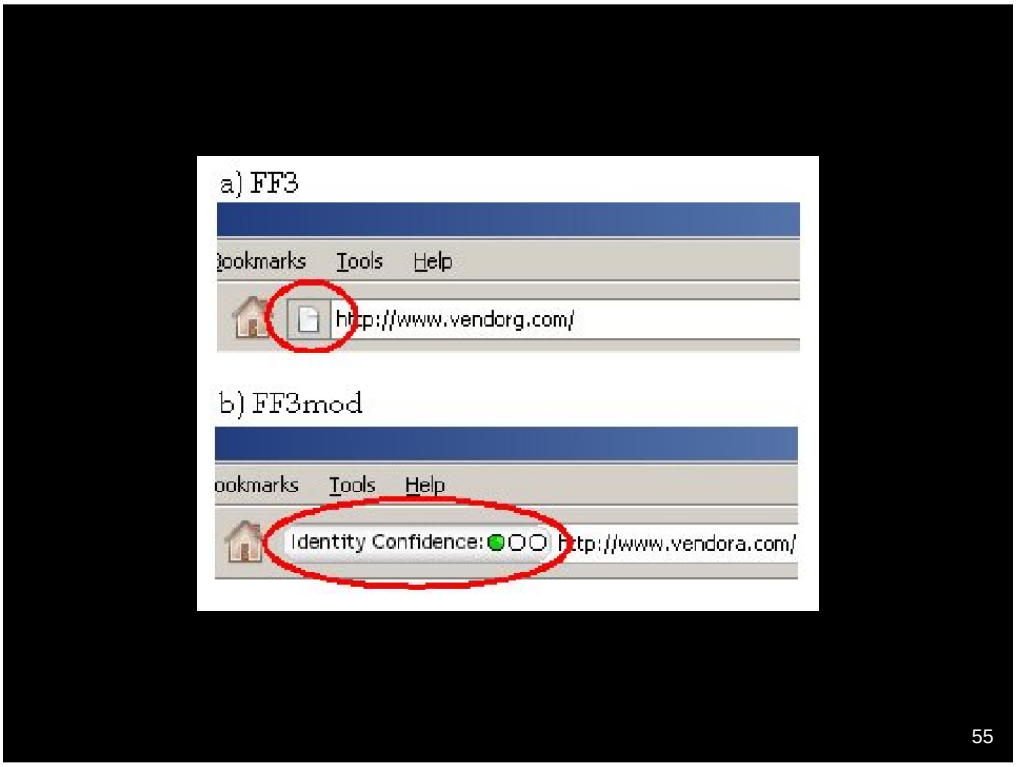
Jennifer Sobey, for her MA thesis at Carleton, examined browser cues that are associated with SSL certificates



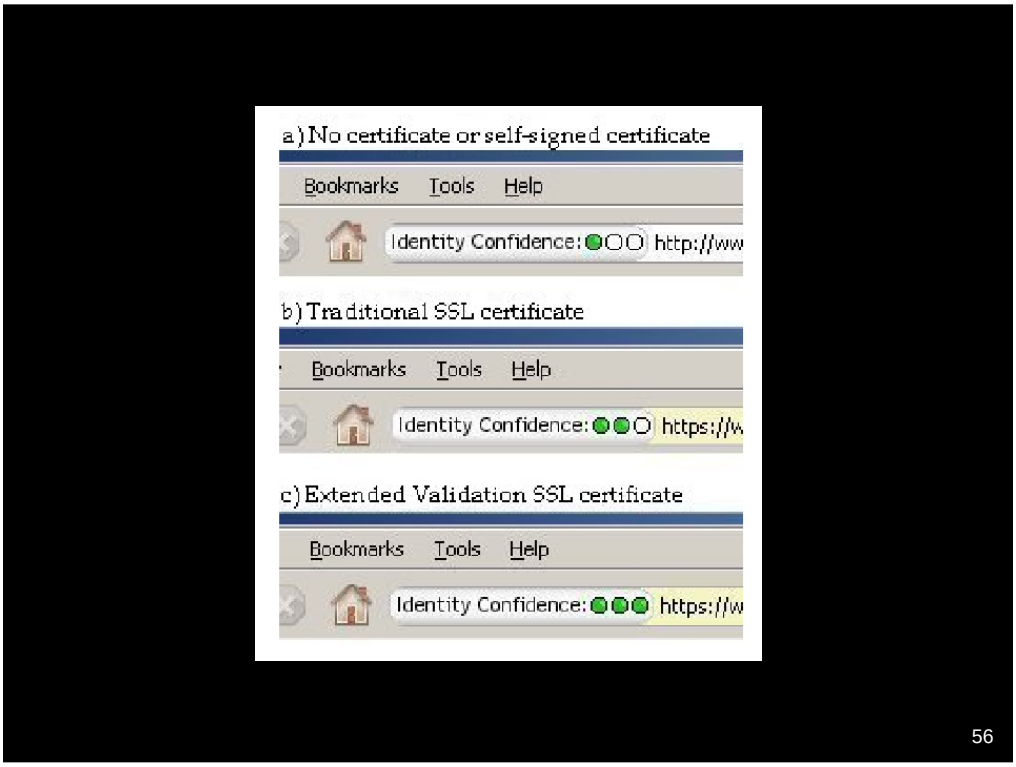
The latest browsers are adding support for Extended Validation Certificates. Here Internet Explorer turns the address bar green when there is an EV certificate.

Will users appreciate this?

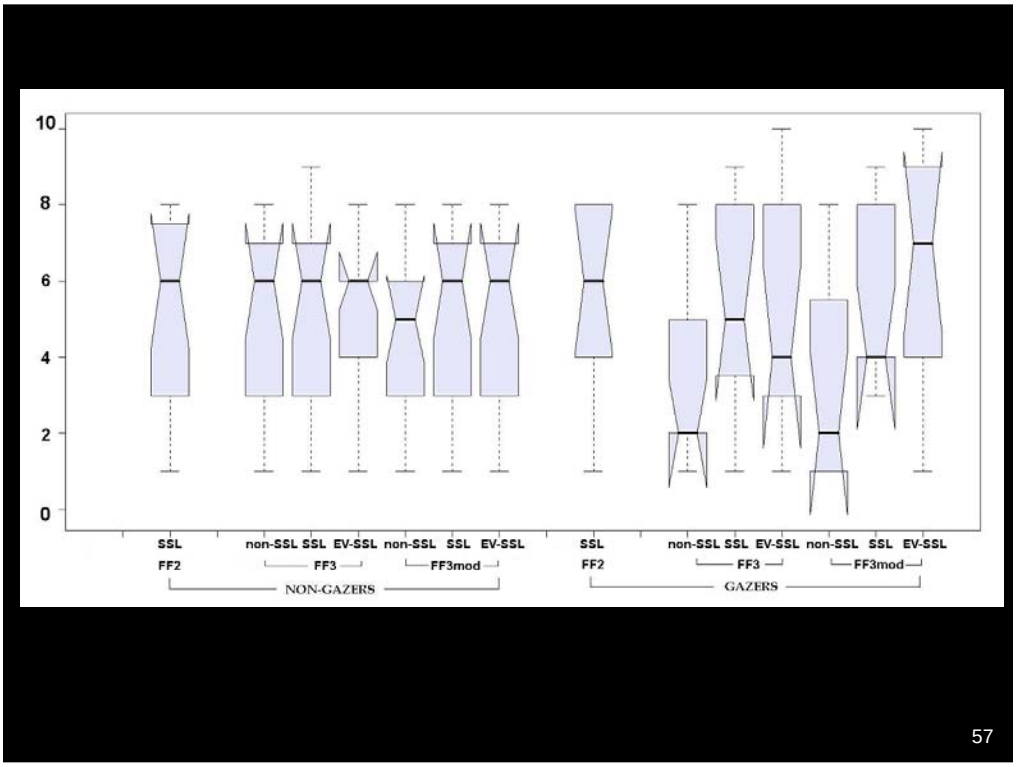
Will they even see it?



Jennifer modified the Firefox 3 browser during development and introduced her own Identity Confidence indicator.



The purpose was to show users information about the certificate type without them having to examine the certificate, or understand green and yellow address bars.



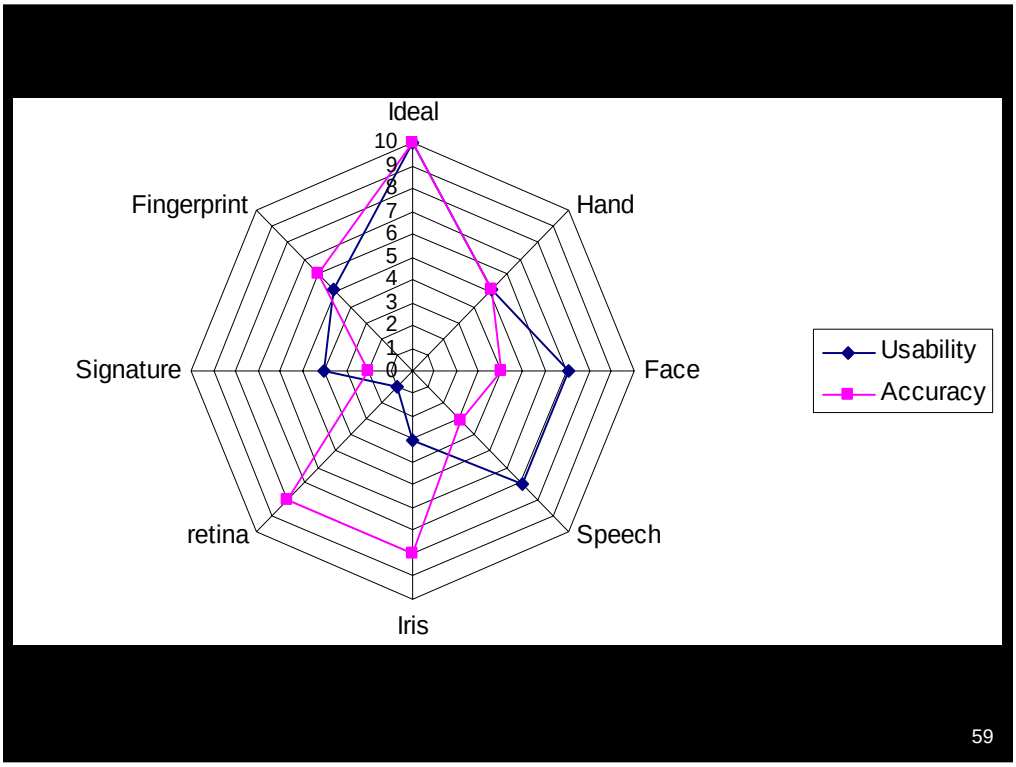
Using eye tracking, the results showed that about half the people never even looked at that part of the browser.

Of those that did, some noticed and appreciated the new indicators, and tended to rate their comfort in doing e-commerce less when there was no SSL certificate (one lit LED)

biometrics

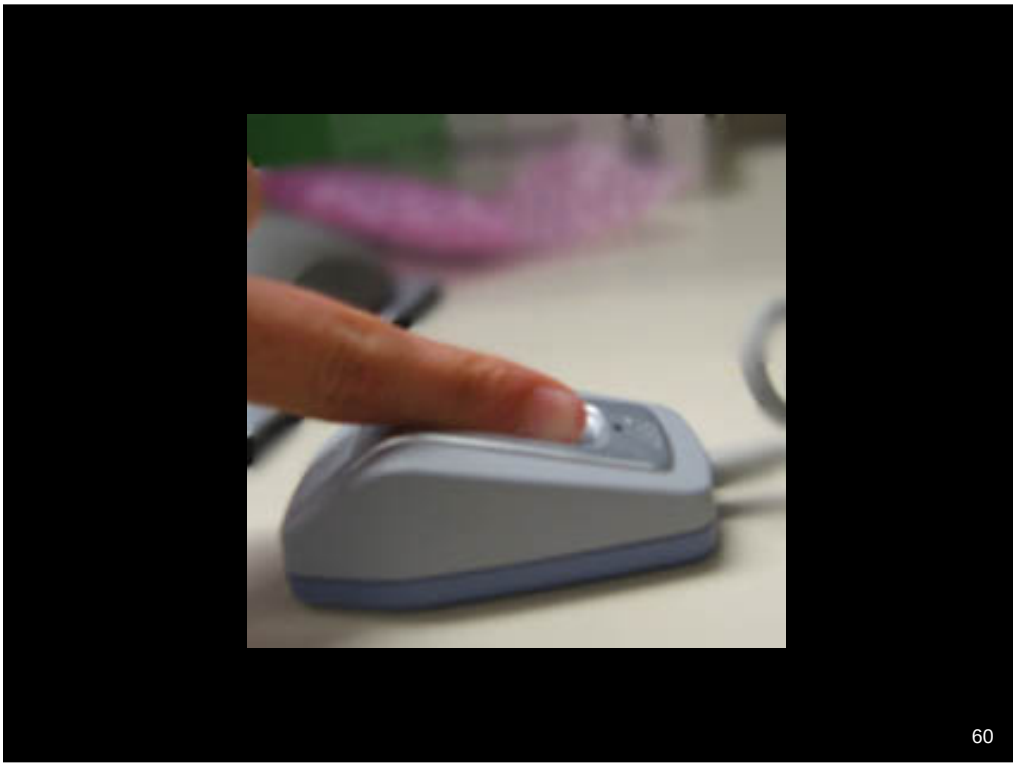
58

NEW TOPIC: biometrics



There is a trade-off between the usability and security of biometrics.

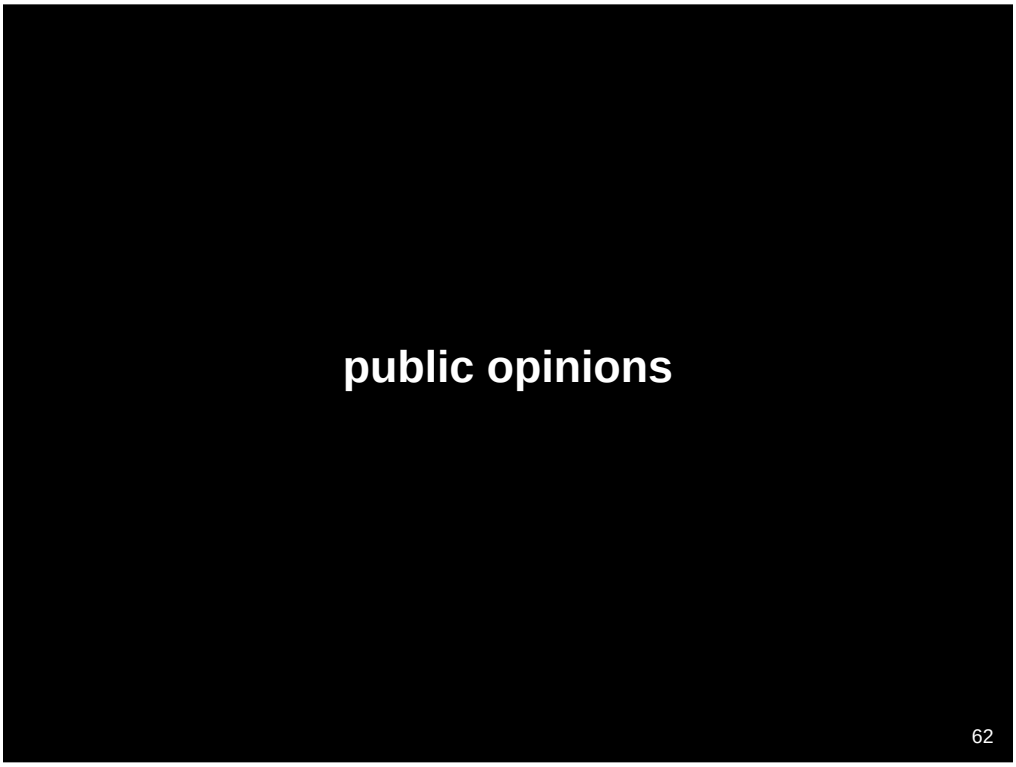
from Coventry book chapter



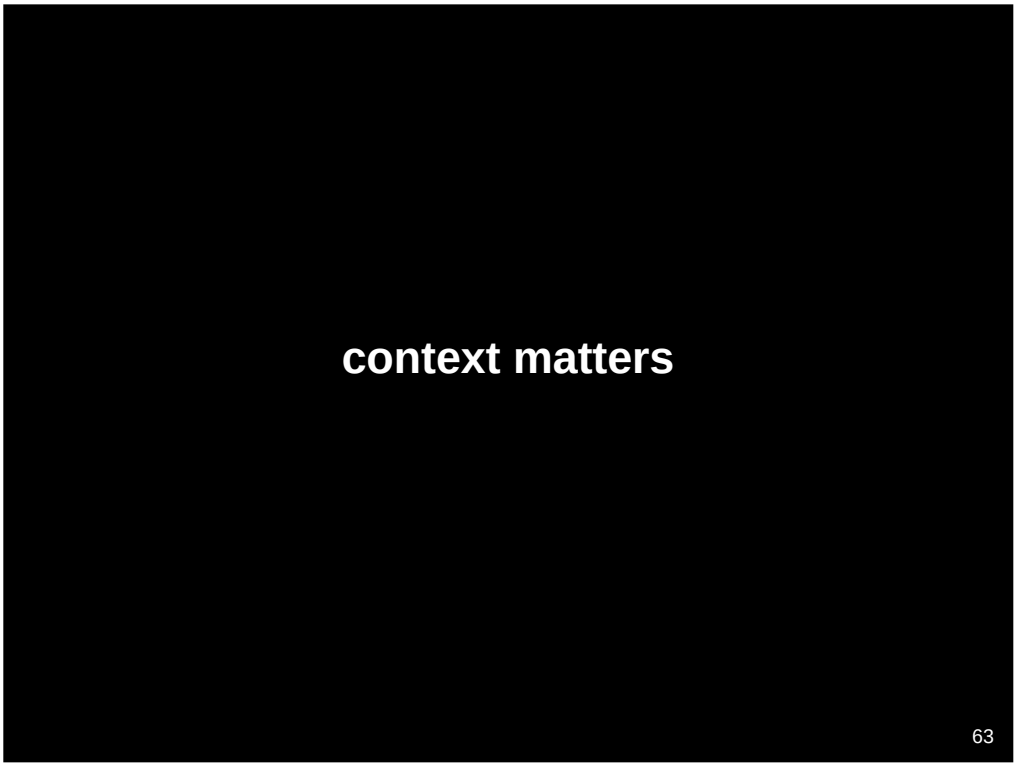
*** misconceptions about using scanners (rolling, wiping, tip-only, pressure)**

*** ergonomic issues with finger placement on scanners**

This person is trying to use an iris camera.



* security as an "enabling task" that gets in the way (Sasse)
* biometrics can be seen as unhygienic, stressful (Coventry)
* some fear of bodily harm to obtain biometric information (movies)
    * union at Pearson airport objecting to iris recognition due to infra-red light
* lack of understanding about biometric templates and storage mechanisms
* opinion polls show weak support and concerns (e.g., TNS/TRUSTe 2005)
    * more support in recent polls
* some cross-cultural differences (within Europe; US/Canada)



Context refers to the identity, place, time, and activity that is associated with using a biometric system.

Context matters.

For example, the acceptance of biometrics in a commercial context will likely be quite different from acceptance for border control or other government applications.

Biometric systems are showing up in a wide variety of contexts, meaning places, applications, authorities, importance, etc.

To most people, the biometrics systems may appear to be the same (e.g., a fingerprint reader that they touch), but the functions and purposes of the system can be very different. They are confused when they are asked to use a biometric for a convenience application (login to a laptop or pay for milk and bread), while the same biometric is used for a national security application (border crossing).

Context also matters on a large scale. This recent report looked at attitudes towards using biometrics to pay for goods when shopping. This chart shows that the attitudes differ a great deal around the world, with the most positive attitudes in Asia, and the least positive in the Americas.

Source.

"New Future in Store" Report for www.tnsglobal.com

4,600 online surveys with primary household shoppers during Jan-Feb 2008

Application Suitability

Elliott, Massie, & Sutton, *The perception of biometric technology: A survey*. 2007 IEEE Workshop on Automatic Identification Advanced Technologies.

TABLE IV. BIOMETRIC APPLICATION SUITABILITY, AGGREGATED OPINIONS

Application	Percentage	
	Yes	No
Identification of arrested people	92	7
Obtaining passports	91	8
Purchasing a gun	84	15
Obtaining a national identification card	82	17
Entering a government building	70	30
Obtaining a drivers license	68	29
Preventing welfare fraud	68	31
ID verification when using a credit card	67	32
Safeguarding medical records	67	32
Checking in for a flight	65	35
Scanning public places	62	37
Making an ATM transaction	61	38
Opening a bank account	58	42
Background check for employment	58	41
Voting in a national election	55	45
Logging into a computer at work	52	47
Payment authorization for online transaction	50	50
Securing a cell phone or PDA	47	53
Scanning for potential gamblers	36	64
Entering a public school	32	67
Logging into a computer at home	32	68
Time and attendance at work	30	70
Renting a vehicle	26	74

66

Context also refers to the purpose of using biometrics. This tables show the percentage of people who think that biometrics are suitable for different applications. Clearly, opinions about suitability differ depending on the application.

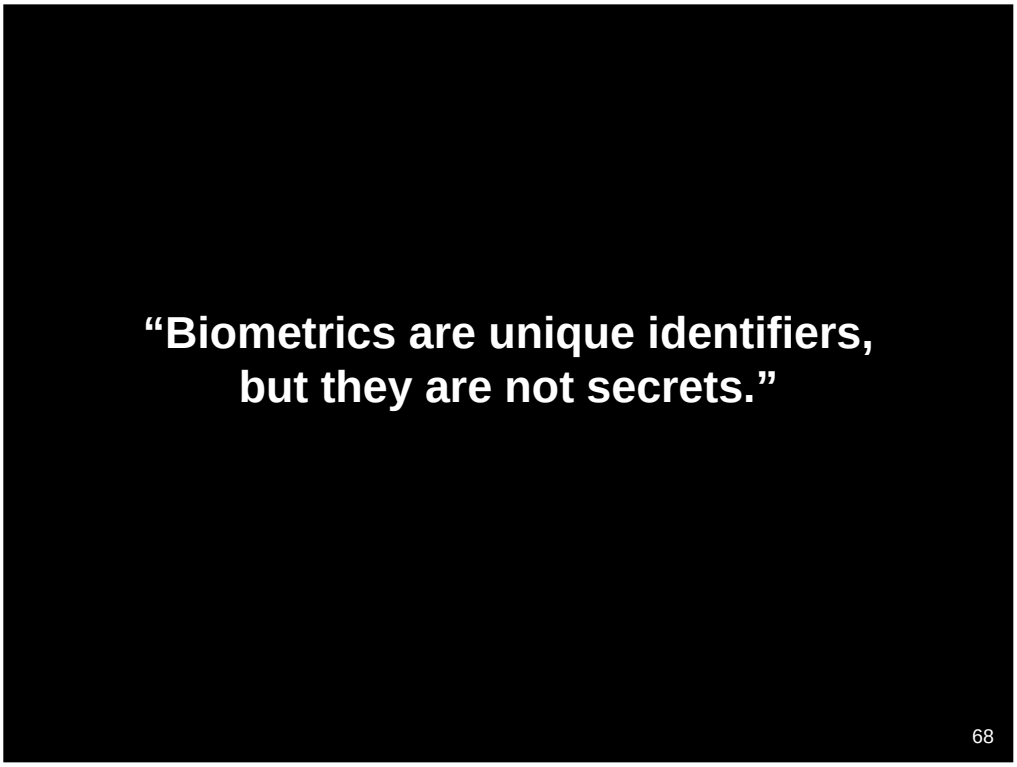
Context matters.

Concerns are often not with the biometric system, but with the back-end processes and policies

67

Biometrics are also used in a context of larger information and security systems. Biometric systems involve much more than gathering physical or behavioral characteristics. Research findings often show that peoples' concerns about biometrics are not with the measurement of human characteristics, but with the associated systems, processes, and polices.

Context matters.



This fundamental characteristic of biometrics should govern everything that we do, and we should not ignore it, but we often do. We can’t just accept it.

*** biometrics provides a universal, public identifier**

*** this leads to universal risk**

*** what is usually needed is a specific, secret identifier**

As a protest against his support for the increasing use of biometric data, the influential hacker group Chaos Computer Club published one of Wolfgang Schäuble's fingerprints in the March 2008 edition of its magazine Datenschleuder (Schäuble is the federal Minister of the Interior). The magazine also included the print on a film that readers could use to fool fingerprint readers.

They did this by collecting a latent fingerprint, because (remember the elephant) biometrics are not secret.

Why did this story get so much attention if this is a fundamental characteristic of biometrics? Why are adopters of biometric systems ignoring the non-secret nature of biometrics?

users make security “errors” because…

71

Conclusions…

systems ignore
human characteristics

72

unattainable cognitive tasks

73

insufficient knowledge

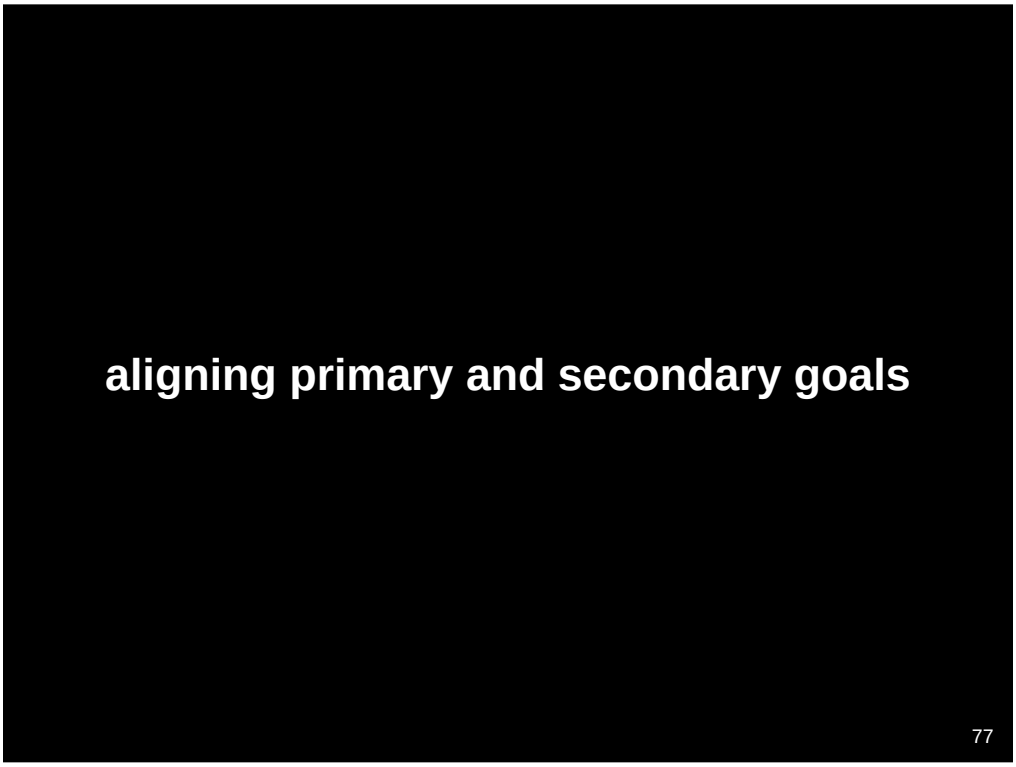
74

designs give no/wrong cues

75

I am arguing for a safety-critical approach to information security

Analyze the system as a whole, not just users, or technology, or operators



The users' primary goal is often in conflict with the secondary goal of maintaining good security. This leads to the belief that there must be a trade-off between usability and security.

“More and more people are coming to realise that security failures are often due to perverse incentives rather than to the lack of suitable technical protection mechanisms.” (Ross Anderson)

- **the person guarding the system is not the person who suffers when the security mechanisms fail**

Are users really the weakest link in the security chain?

79