بسم الله الرحمن الرحیم

Fundamentals of Secure Computing

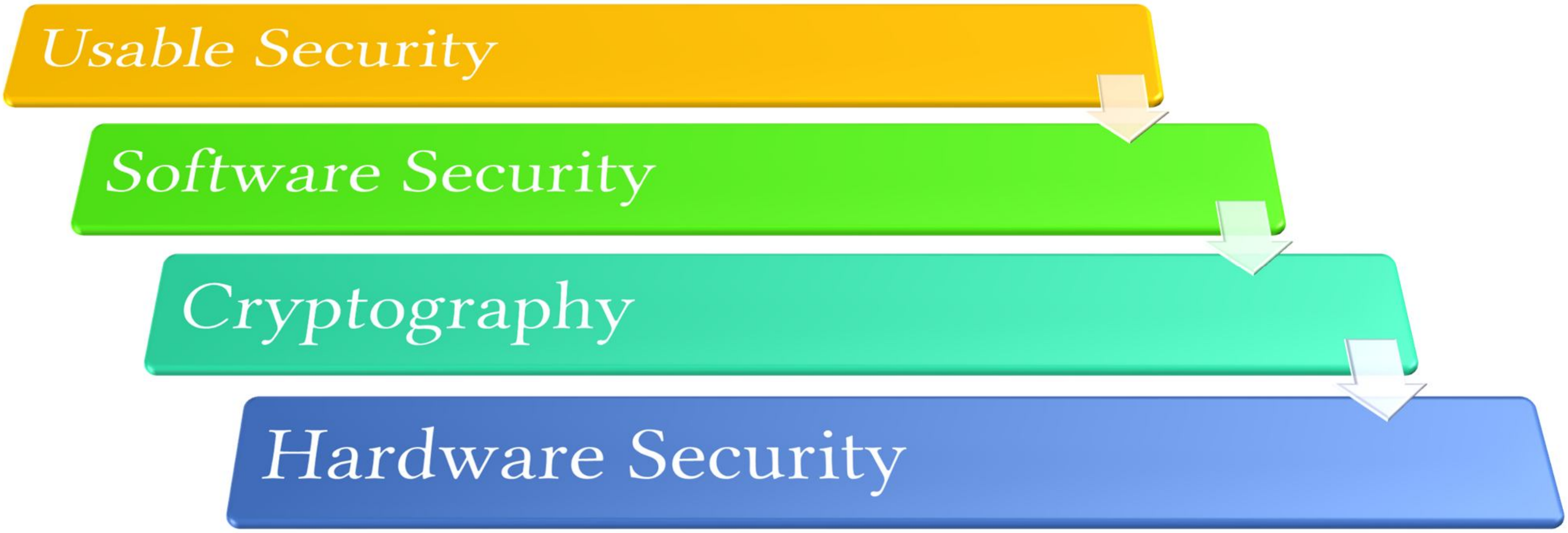
Ali Shakiba

Vali-e-Asr University of Rafsanjan

ali.shakiba@vru.ac.ir

Fall 2017

What are we going to learn in the class?



Usable Security

Software Security

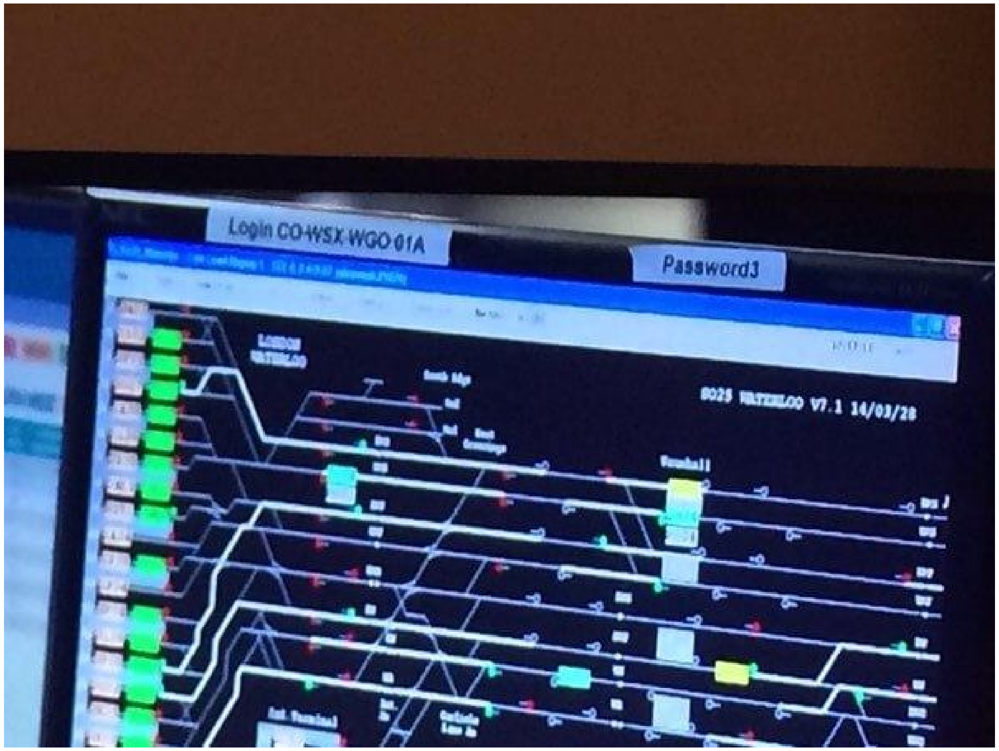
Cryptography

Hardware Security

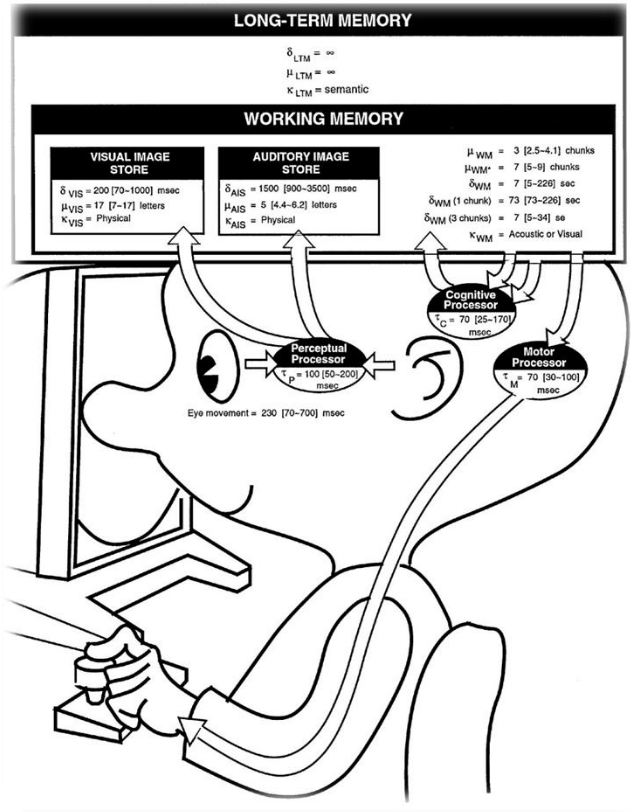
Usable Security?

Why did it happen?

another example, ...



Human Computer Interaction or HCI


LONG-TERM MEMORY
$\delta_{LTM} = \infty$
$\mu_{LTM} = \infty$
κ_{LTM} = semantic
WORKING MEMORY
VISUAL IMAGE STORE
δ_{VIS} = 200 [70~1000] msec
μ_{VIS} = 17 [7~17] letters
κ_{VIS} = Physical
AUDITORY IMAGE STORE
δ_{AIS} = 1500 [900~3500] msec
μ_{AIS} = 5 [4.4~6.2] letters
κ_{AIS} = Physical
μ_{WM} = 3 [2.5~4.1] chunks
μ_{WM^*} = 7 [5~9] chunks
δ_{WM} = 7 [5~226] sec
δ_{WM} (1 chunk) = 73 [73~226] sec
δ_{WM} (3 chunks) = 7 [5~34] se
κ_{WM} = Acoustic or Visual
Cognitive Processor
τ_C = 70 [25~170] msec
Perceptual Processor
τ_P = 100 [50~200] msec
Motor Processor
τ_M = 70 [30~100] msec
Eye movement = 230 [70~700] msec

Unfortunately, HCI is ignored in "Security Design", most of the time …

and the result is, ...

How to get a SECURE system +

What about “Privacy”?

So, we are going to study the "HCI" and its applications in "Cyber Security"

HCI Basics

- What's HCI?
- Usability
- Mental Models

Design

- Design Methodologies
- Case Study: SSL Warnings

Evaluation

- Qualitative Evaluation & Controlled Experiments
- Usability Studies
- Case Study: Phishing Emails

Guidelines for Usable Security

- Authority Guidelines
- Authorization & Communication Guidelines
- Interface Guidelines for Usable Security
- Case Study: Phishing Warnings

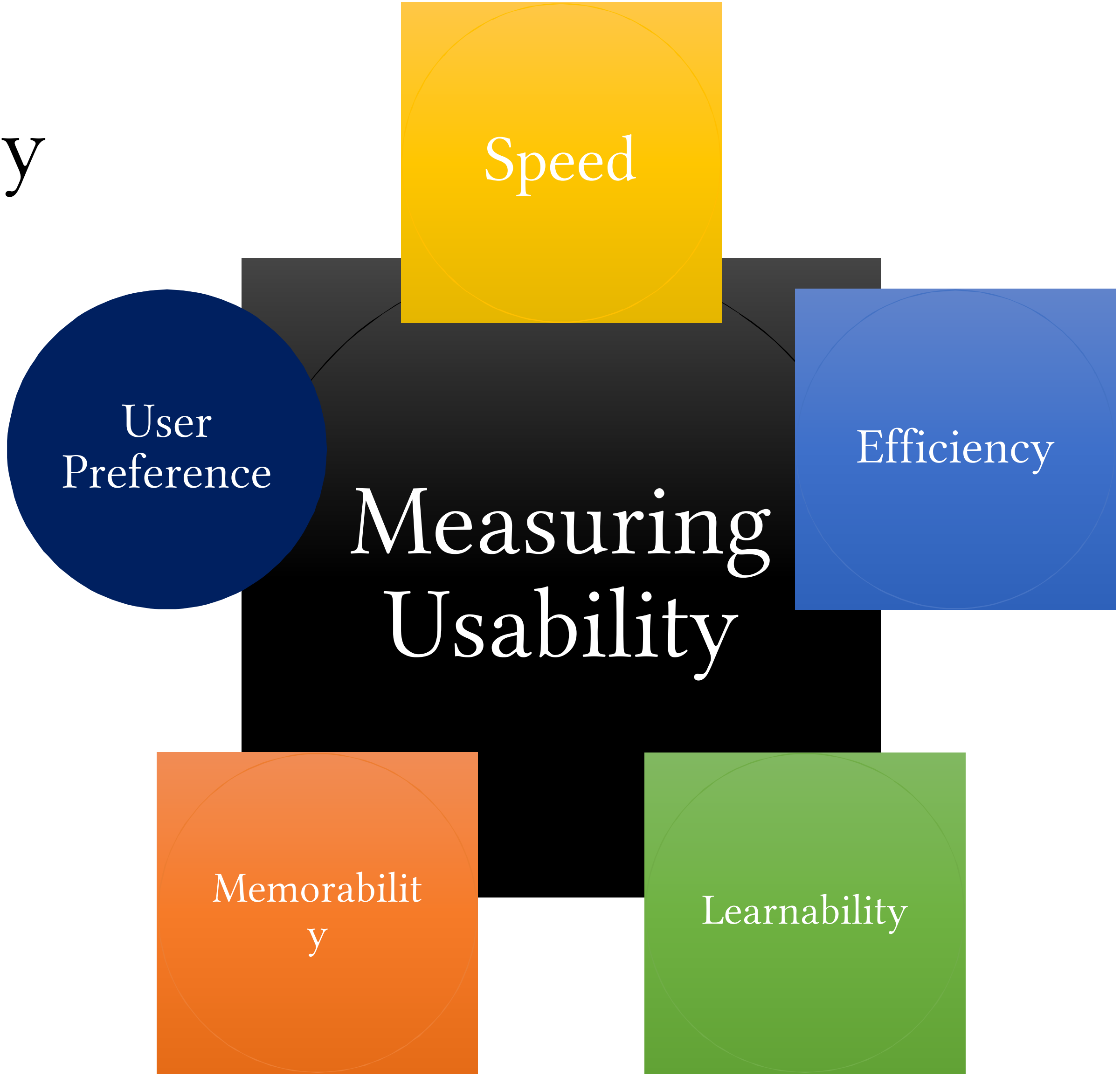
Usable Authentication

- Passwords & 2-factor Authentication
- Biometric Authentication
- Gesture-based Authentication
- Case Study: Smudgy Attacks

Usable Privacy

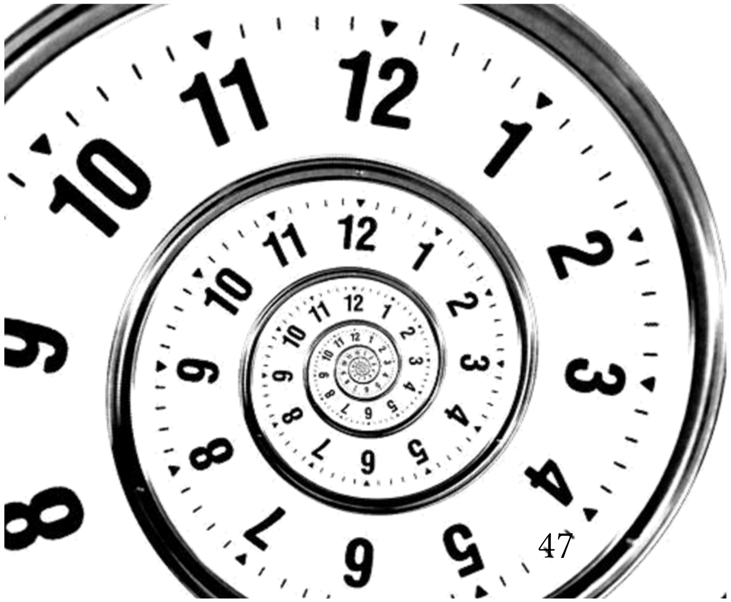
- Privacy Policies & User Understanding
- Informed Consent for Privacy
- Inferring personal Data & Policy

Usability


Speed
User Preference
Measuring Usability
Efficiency
Memorabilit
y
Learnability

Usability Measures: Speed

- how quickly can the task be accomplished
  - ignoring users' mistakes, i.e. the users act optimally



Usability Measures: Efficiency

- how many mistakes are made in accomplishing the task

Usability Measures: Learnability

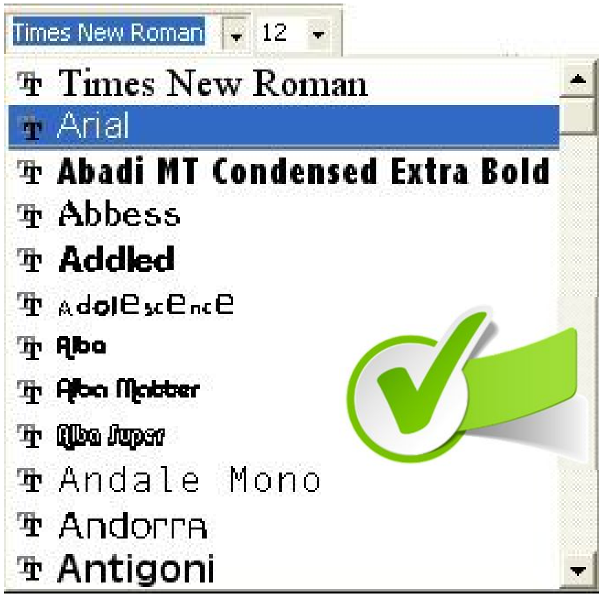
- how easy is it to learn to use the system

Usability Measures: Memorability

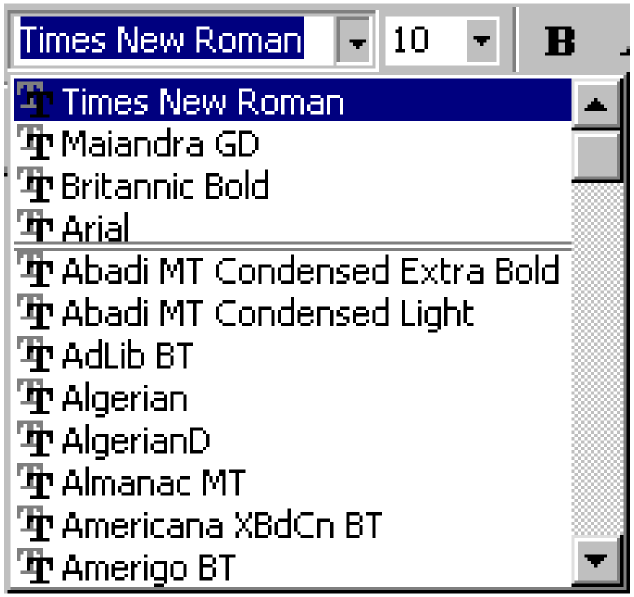
- once learned, how easy is it to remember how to use the system

Memorability Measure

font list with preview



font list without preview

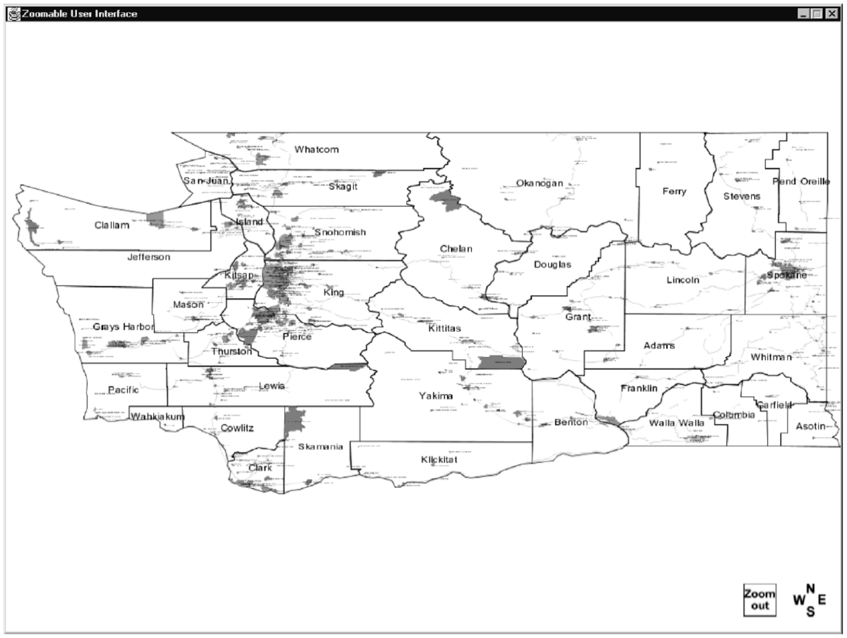


Usability Measures: User Preference

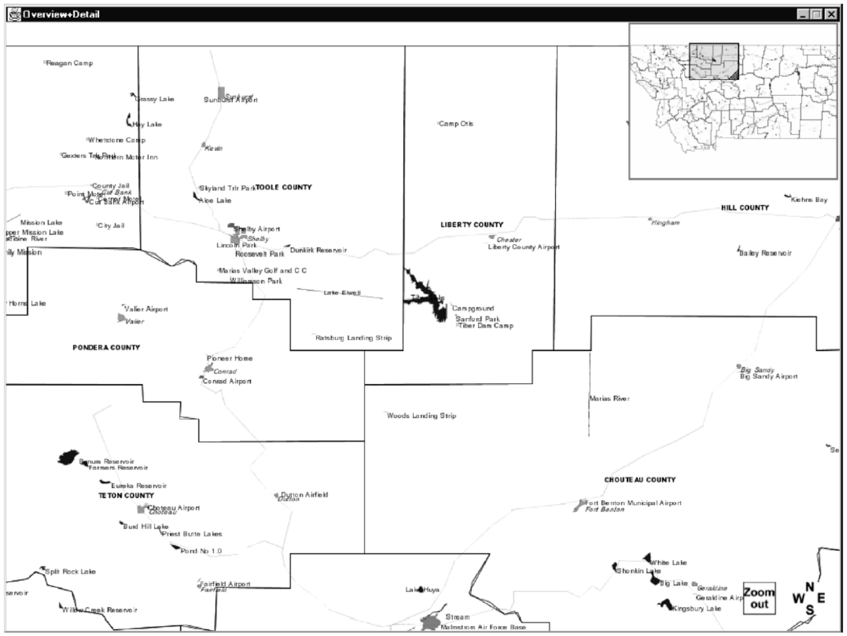
- what do users like most?

Usability Measures & User Preference

zooming + no overview interface



zooming + overview interface



User Preference ☑

Speed ☑ Efficiency ☑

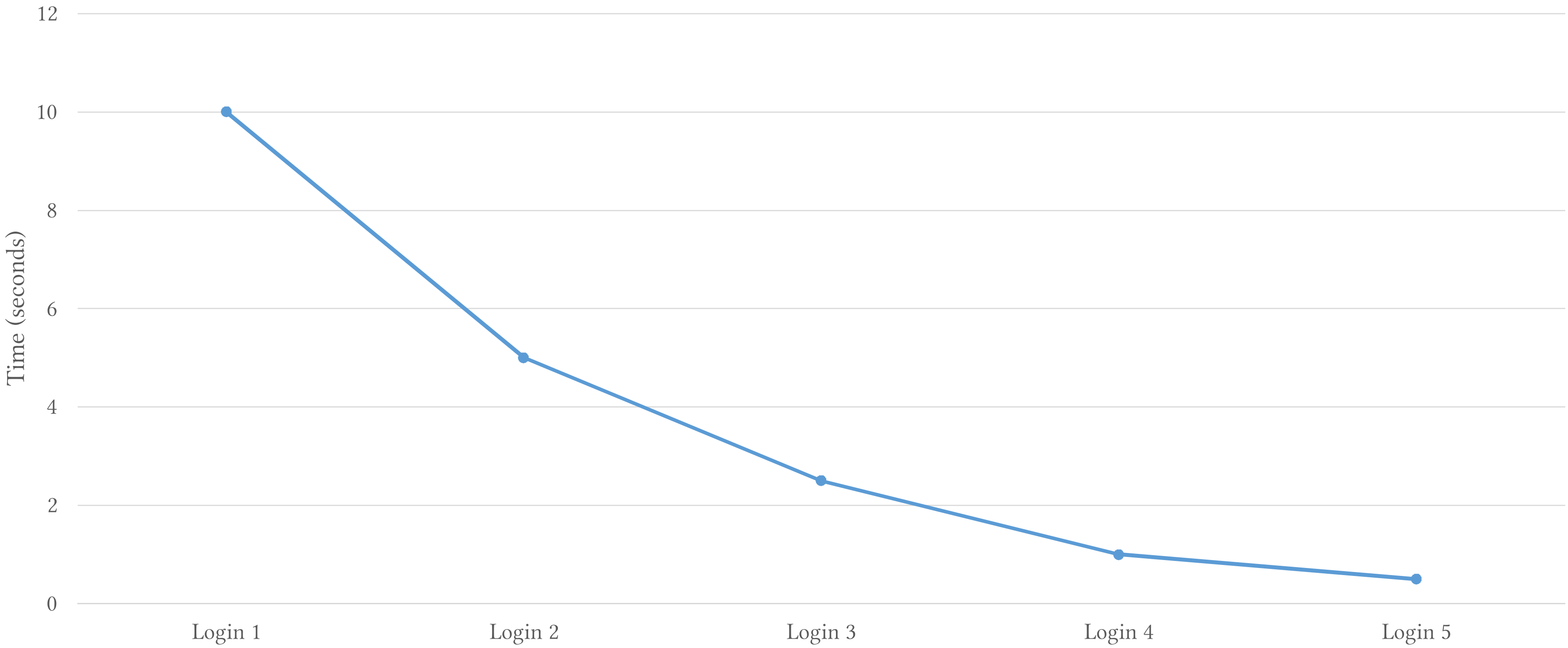
[HBP02] Kasper Hornbæk, Benjamin B. Bederson, and Catherine Plaisant. 2002. Navigation patterns and usability of zoomable user interfaces with and without an overview. *ACM Trans. Comput.-Hum. Interact.* 9, 4 (December 2002), 362-389.

How do we measure these factors?

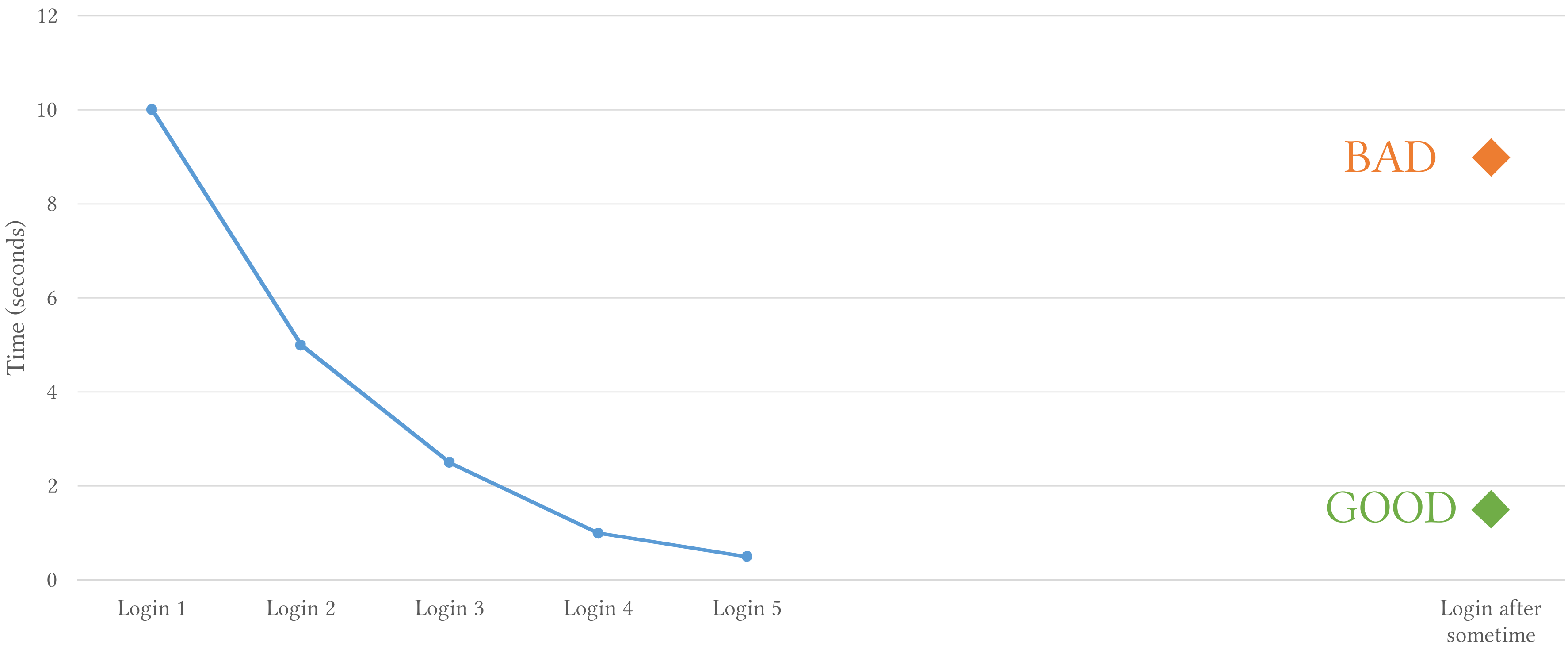
- speed
  - timing
- efficiency
  - counting errors

- learnability
  - ?
- memorability
  - ?
- user preferences
  - ?

Measuring Learnability



Measuring Memorability

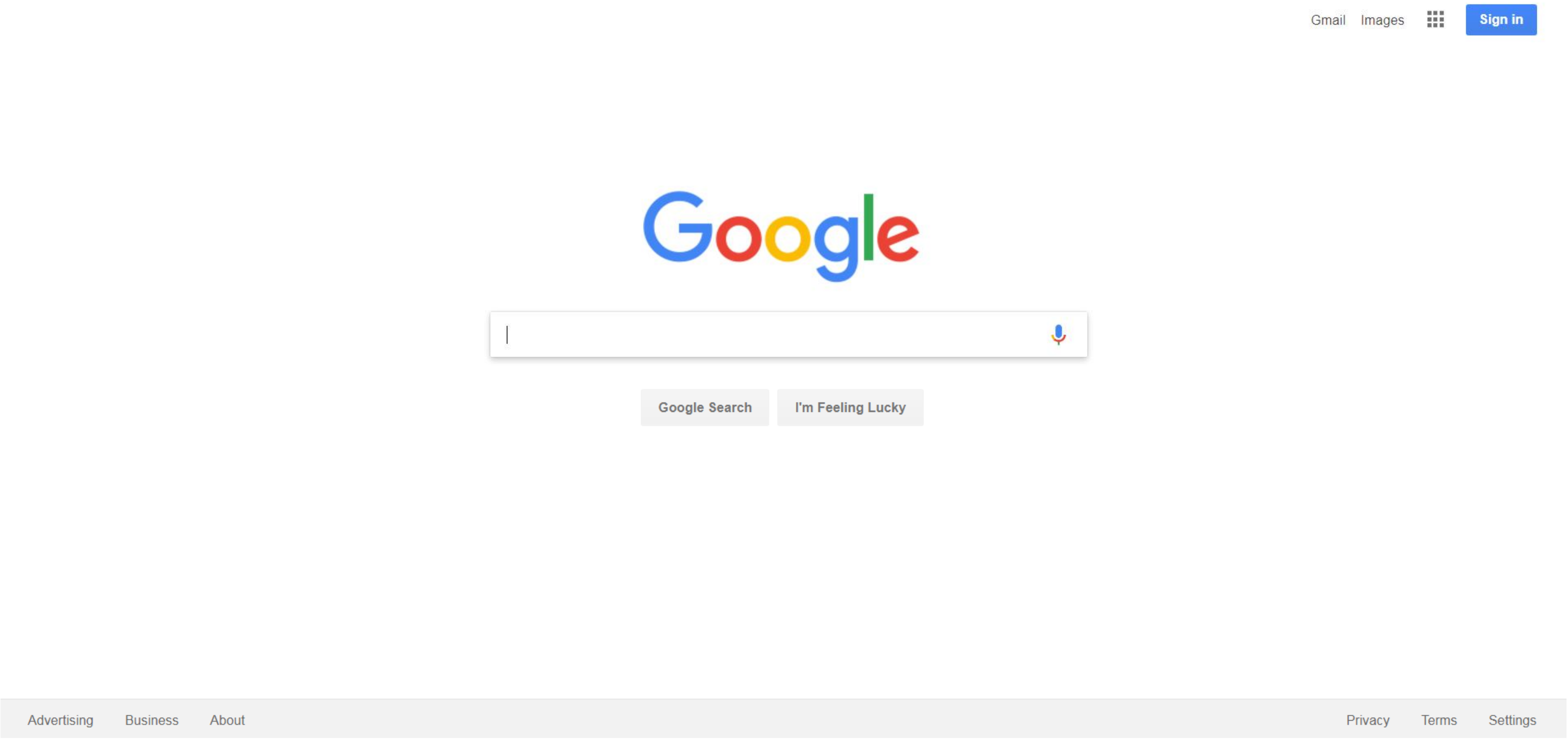


Measuring User Preference

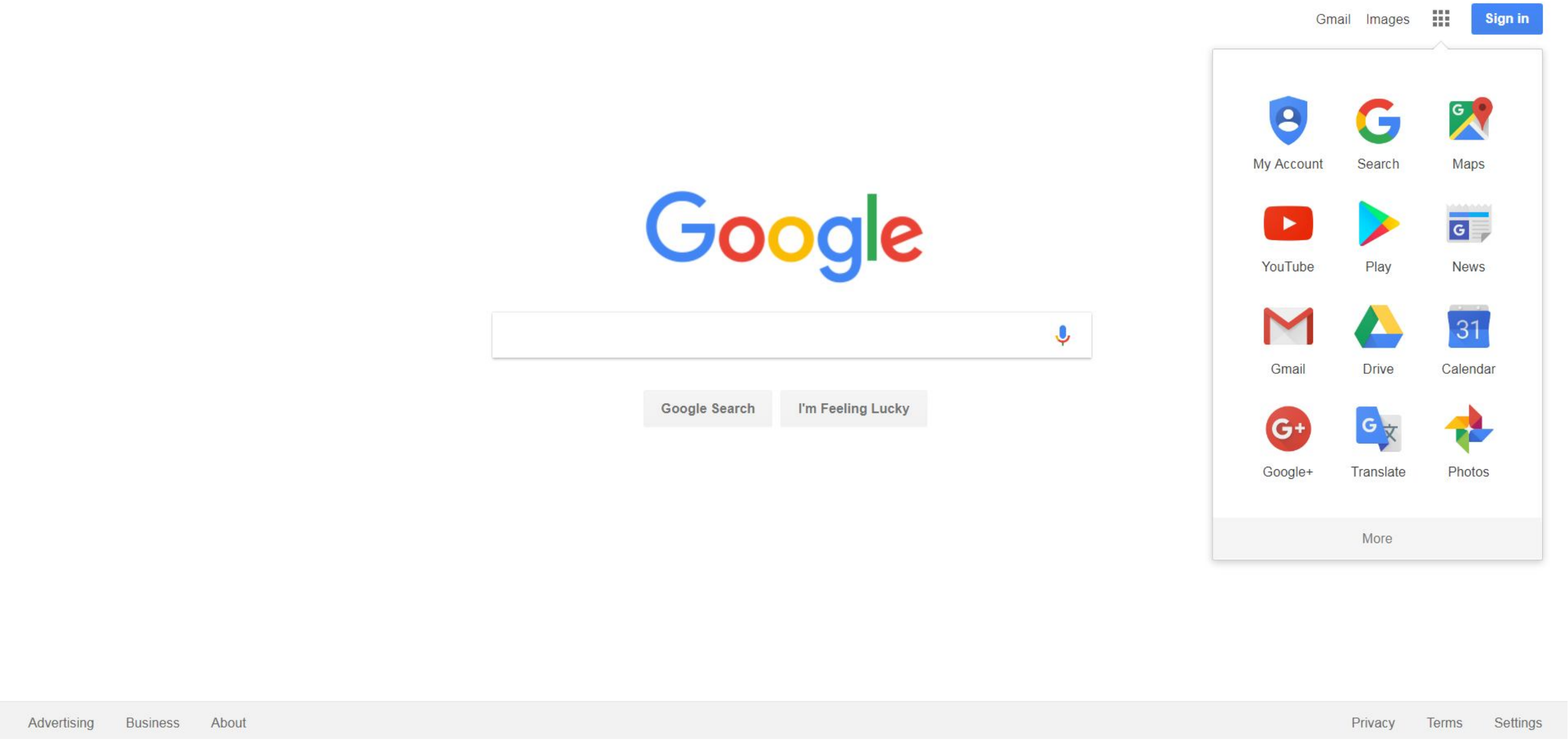
Tasks

- goals that users set out to accomplish when they are using a system
  - most important tasks & less important tasks

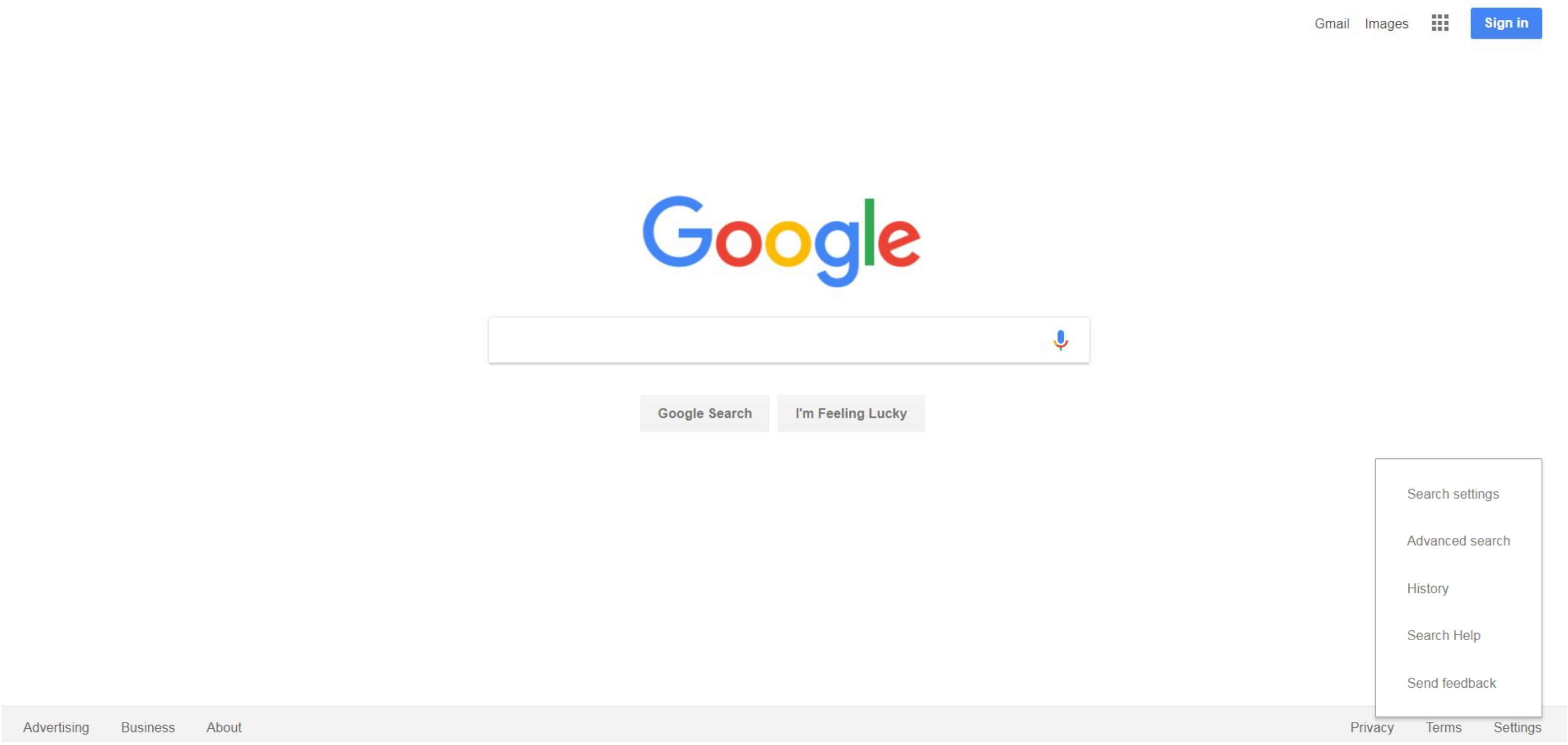
Example: Google.com



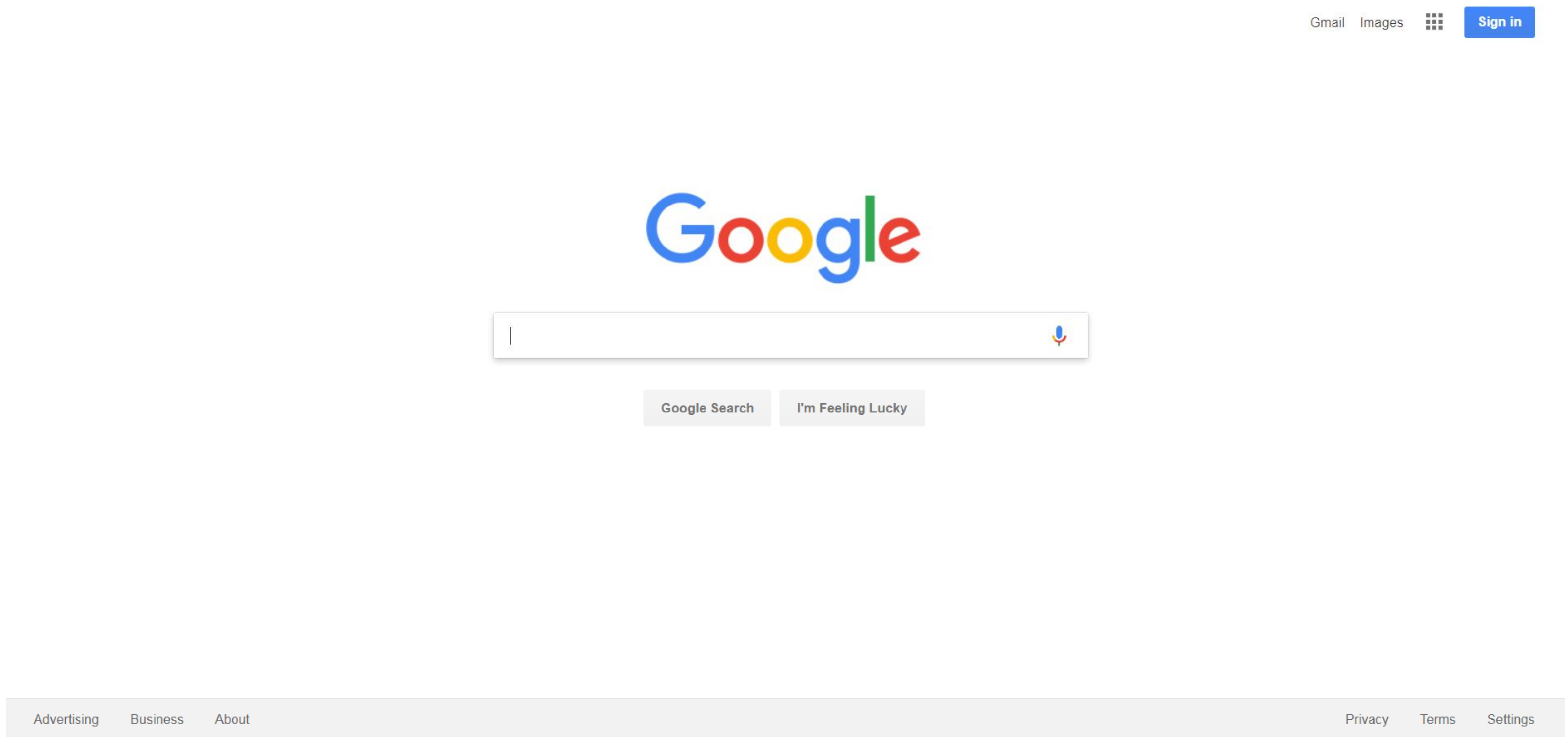
Example: Google.com (cont’d)



Example: Google.com (cont’d)

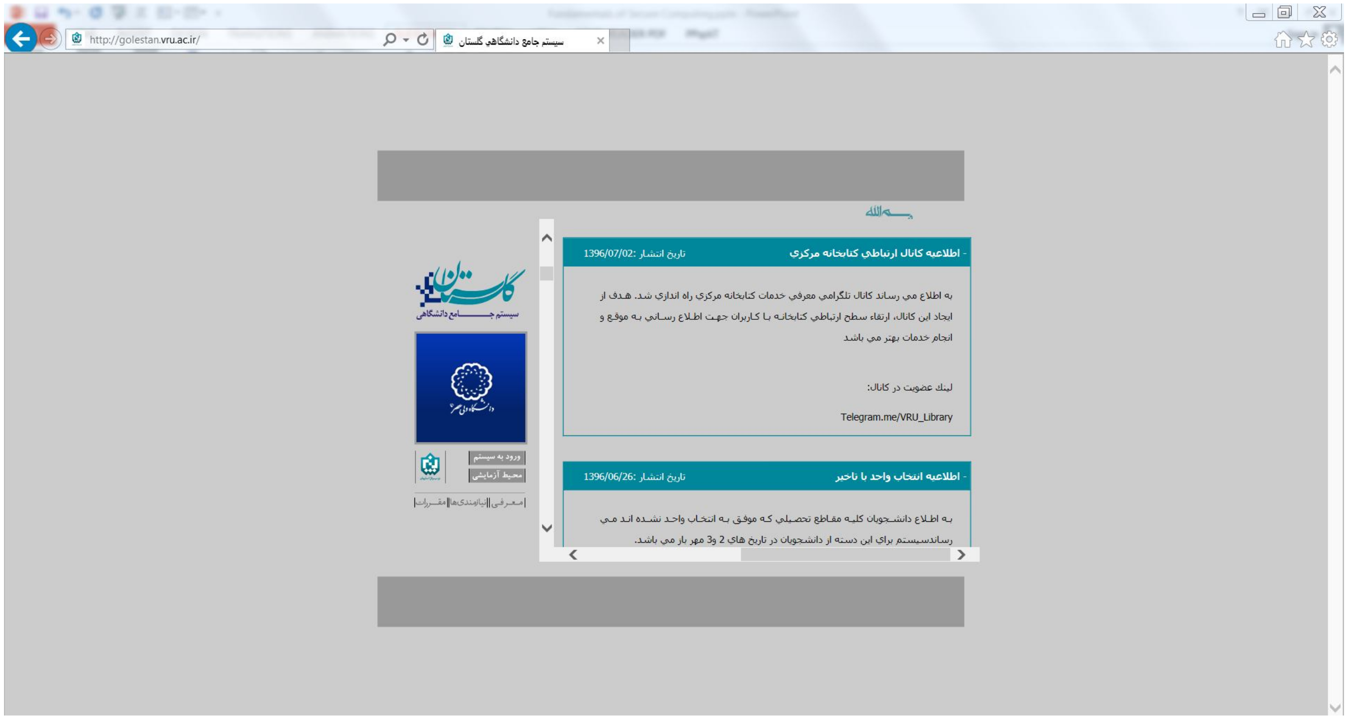


Example: Google.com (cont'd)



Tasks are goals users set out to accomplish in a system

Example: Log in to golestan.vru.ac.ir



- اطلاعيه كانال ارتباطي كتابخانه مركزي تاريخ انتشار :1396/07/02

به اطلاع مي رساند كانال تلگرامي معرفي خدمات كتابخانه مركزي راه اندازي شد. هدف از ايجاد اين كانال، ارتقاء سطح ارتباطي كتابخانه با كاربران جهت اطلاع رساني به موقع و انجام خدمات بهتر مي باشد

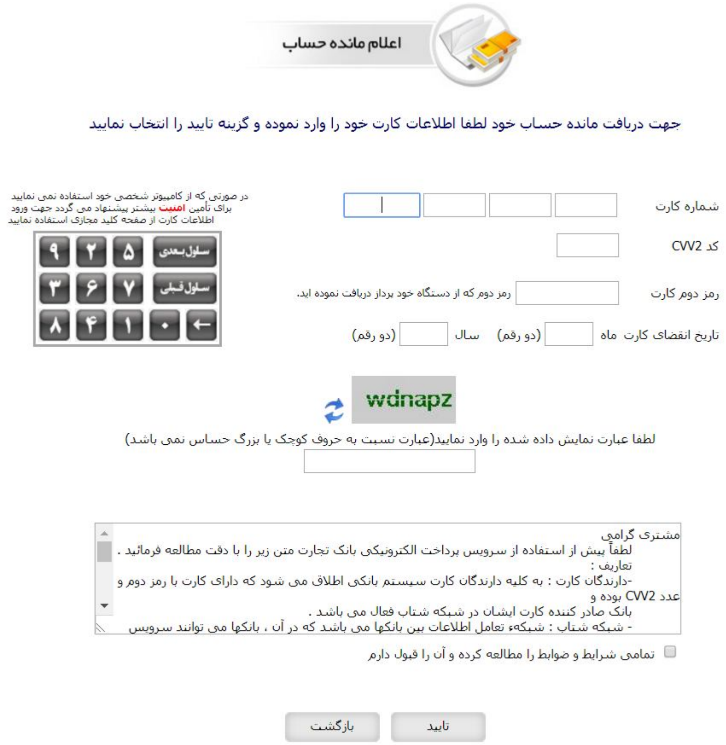
لينك عضويت در كانال:

Telegram.me/VRU_Library

- اطلاعيه انتخاب واحد با تاخير تاريخ انتشار :1396/06/26

به اطلاع دانشجويان كليه مقاطع تحصيلي كه موفق به انتخاب واحد نشده اند مي رساندسيستم براي اين دسته از دانشجويان در تاريخ هاي 2 و3 مهر باز مي باشد.

Example: Check the Bank Card Balance



اعلام مانده حساب

جهت دریافت مانده حساب خود لطفا اطلاعات کارت خود را وارد نموده و گزینه تایید را انتخاب نمایید

در صورتی که از کامپیوتر شخصی خود استفاده نمی نمایید
برای تأمین **امنیت** بیشتر پیشنهاد می گردد جهت ورود
اطلاعات کارت از صفحه کلید مجازی استفاده نمایید

شماره کارت

کد CVV2

رمز دوم کارت — رمز دوم که از دستگاه خود پرداز دریافت نموده اید.

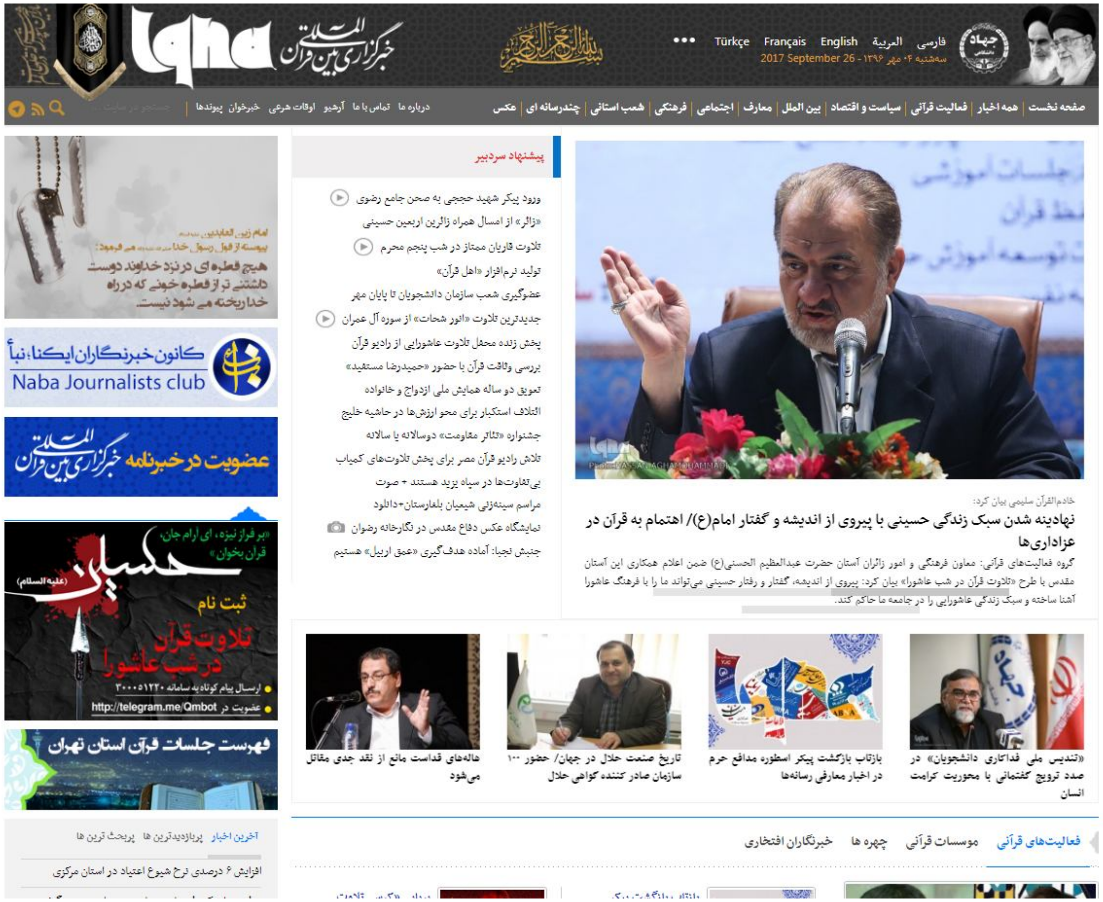
تاریخ انقضای کارت ماه (دو رقم) سال (دو رقم)

لطفا عبارت نمایش داده شده را وارد نمایید(عبارت نسبت به حروف کوچک یا بزرگ حساس نمی باشد)

مشتری گرامی
لطفاً پیش از استفاده از سرویس پرداخت الکترونیکی بانک تجارت متن زیر را با دقت مطالعه فرمائید .
تعاریف :
-دارندگان کارت : به کلیه دارندگان کارت سیستم بانکی اطلاق می شود که دارای کارت با رمز دوم و
عدد CVV2 بوده و
بانک صادر کننده کارت ایشان در شبکه شتاب فعال می باشد .
- شبکه شتاب : شبکهء تعامل اطلاعات بین بانکها می باشد که در آن ، بانکها می توانند سرویس

☐ تمامی شرایط و ضوابط را مطالعه کرده و آن را قبول دارم

Example: Read the Headlines


Iqna
خبرگزاری بین المللی قرآن
فارسی العربیة English Français Türkçe •••
سه‌شنبه ۰۴ مهر ۱۳۹۶ - 2017 September 26
صفحه نخست | همه اخبار | فعالیت قرآنی | سیاست و اقتصاد | بین الملل | معارف | اجتماعی | فرهنگی | شعب استانی | چندرسانه ای | عکس
درباره ما تماس با ما آرشیو اوقات شرعی خبرخوان پیوندها
کانون خبرنگاران ایکنا؛ نبأ
Naba Journalists club
عضویت در خبرنامه خبرگزاری بین المللی قرآن
فهرست جلسات قرآن استان تهران
فعالیت‌های قرآنی موسسات قرآنی چهره ها خبرنگاران افتخاری

امام زین العابدین (ع) پیوسته از قول رسول خدا (ص) می فرمود: هیچ قطره ای در نزد خداوند دوست داشتنی تر از قطره خونی که در راه خدا ریخته می شود نیست.

«بر فراز نیزه، ای ارام جان، قران بخوان»

حسین (علیه السلام)

ثبت نام تلاوت قرآن در شب عاشورا

- ارسال پیام کوتاه به سامانه ۳۰۰۰۵۱۲۲۰
- عضویت در http://telegram.me/Qmbot

خادم‌القرآن سلیمی بیان کرد:

نهادینه شدن سبک زندگی حسینی با پیروی از اندیشه و گفتار امام(ع)/ اهتمام به قرآن در عزاداری‌ها

گروه فعالیت‌های قرآنی: معاون فرهنگی و امور زائران آستان حضرت عبدالعظیم الحسنی(ع) ضمن اعلام همکاری این آستان مقدس با طرح «تلاوت قرآن در شب عاشورا» بیان کرد: پیروی از اندیشه، گفتار و رفتار حسینی می‌تواند ما را با فرهنگ عاشورا آشنا ساخته و سبک زندگی عاشورایی را در جامعه ما حاکم کند.

پیشنهاد سردبیر

- ورود پیکر شهید حججی به صحن جامع رضوی
- «زائر» از امسال همراه زائرین اربعین حسینی
- تلاوت قاریان ممتاز در شب پنجم محرم
- تولید نرم‌افزار «اهل قرآن»
- عضوگیری شعب سازمان دانشجویان تا پایان مهر
- جدیدترین تلاوت «انور شحات» از سوره آل عمران
- پخش زنده محفل تلاوت عاشورایی از رادیو قرآن
- بررسی وثاقت قرآن با حضور «حمیدرضا مستفید»
- تعویق دو ساله همایش ملی ازدواج و خانواده
- ائتلاف استکبار برای محو ارزش‌ها در حاشیه خلیج
- جشنواره «تئاتر مقاومت» دوسالانه یا سالانه
- تلاش رادیو قرآن مصر برای پخش تلاوت‌های کمیاب
- بی‌تفاوت‌ها در سپاه یزید هستند + صوت
- مراسم سینه‌زنی شیعیان بلغارستان+دانلود
- نمایشگاه عکس دفاع مقدس در نگارخانه رضوان
- جنبش نجبا: آماده هدف‌گیری «عمق اربیل» هستیم

«تندیس ملی فداکاری دانشجویان» در صدد ترویج گفتمانی با محوریت کرامت انسان

بازتاب بازگشت پیکر اسطوره مدافع حرم در اخبار معارفی رسانه‌ها

تاریخ صنعت حلال در جهان/ حضور ۱۰۰ سازمان صادر کننده گواهی حلال

هاله‌های قداست مانع از نقد جدی مقاتل می‌شود

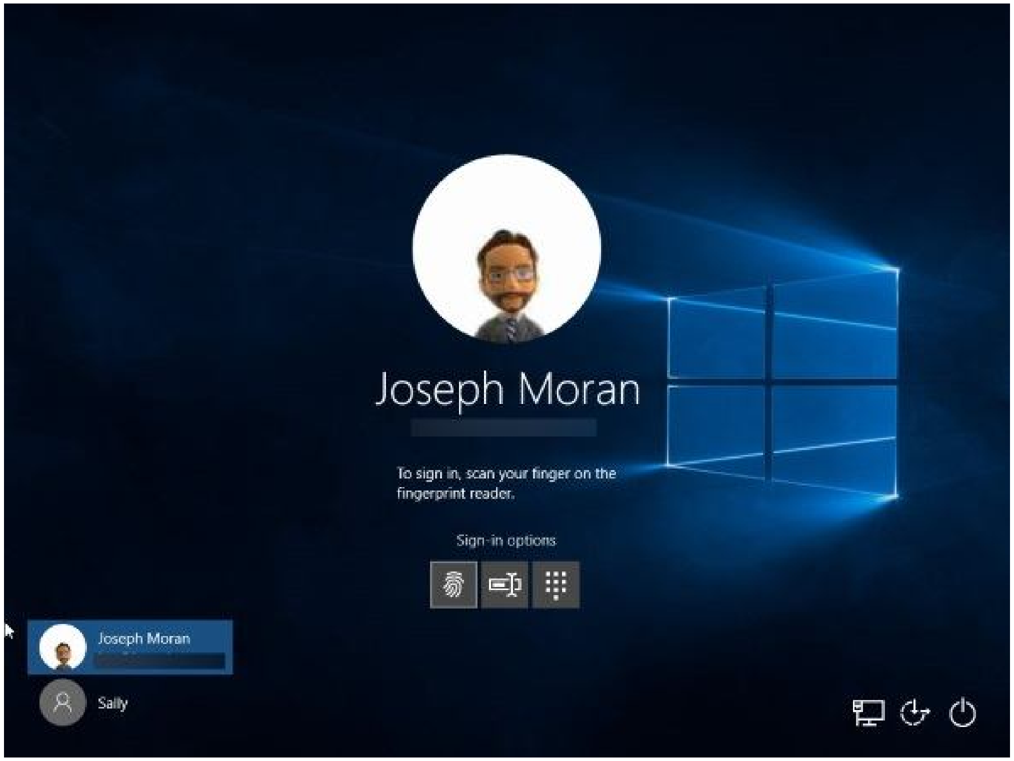
آخرین اخبار پربازدیدترین ها پربحث ترین ها

افزایش ۶ درصدی نرخ شیوع اعتیاد در استان مرکزی

Measuring the Usability of a Task

1. Speed
2. Efficiency
3. Learnability
4. Memorability
5. User Preference

Example: Windows Fingerprint Sign in



Joseph Moran

To sign in, scan your finger on the fingerprint reader.

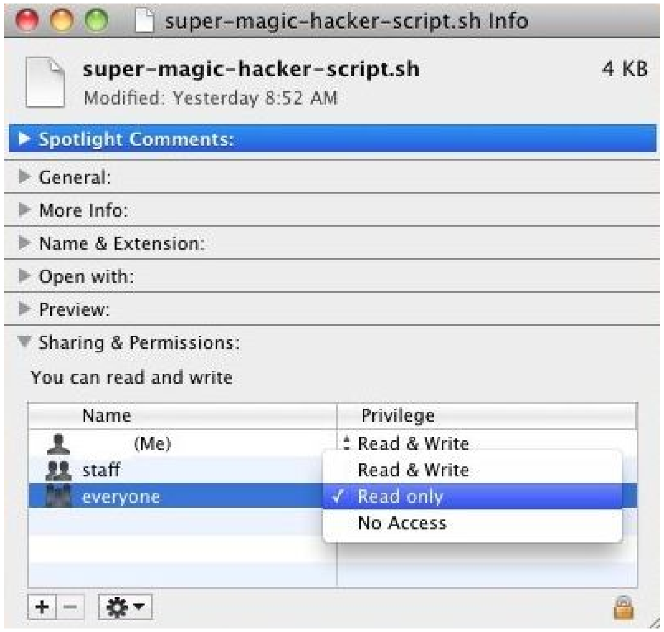
Common Errors in Task Creation

- Too leading or too descriptive
  - e.g. click on the username box at the upper right ofthe screen and enter your username. Then click the password box underneath itand enter your password and click submit …
- Specific questions
  - What is the 2nd headline in the website of the university?
- Directing users toward things you want to tell them, not what they want to know
  - What are the names of the website developers?

Comparing tasks between systems

- Task: “Giving people write access to a file”
  - Mode: command line vs. GUI

```
$ chmod +w super-magic-hacker-script.sh
```



super-magic-hacker-script.sh Info

super-magic-hacker-script.sh 4 KB
Modified: Yesterday 8:52 AM

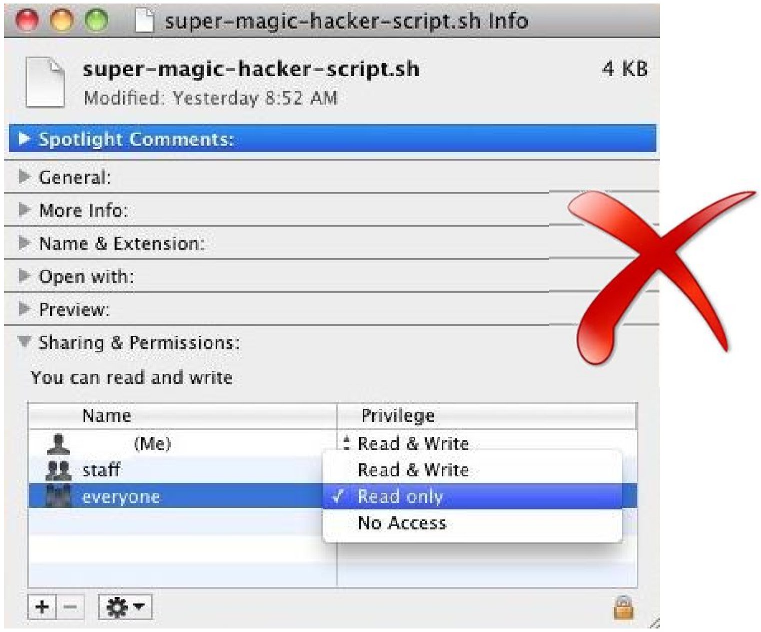
Sharing & Permissions:
You can read and write

Name	Privilege
(Me)	Read & Write
staff	Read & Write
everyone	✓ Read only

Comparing tasks between systems

- Task: “Giving people execute access to a file”
  - Mode: command line vs. GUI

```
$ chmod +x super-magic-hacker-script.sh
```



super-magic-hacker-script.sh Info

super-magic-hacker-script.sh 4 KB
Modified: Yesterday 8:52 AM

▶ Spotlight Comments:

▶ General:

▶ More Info:

▶ Name & Extension:

▶ Open with:

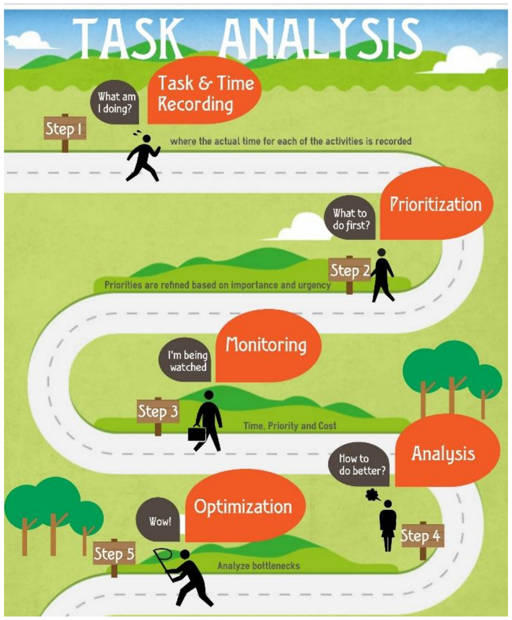
▶ Preview:

▼ Sharing & Permissions:

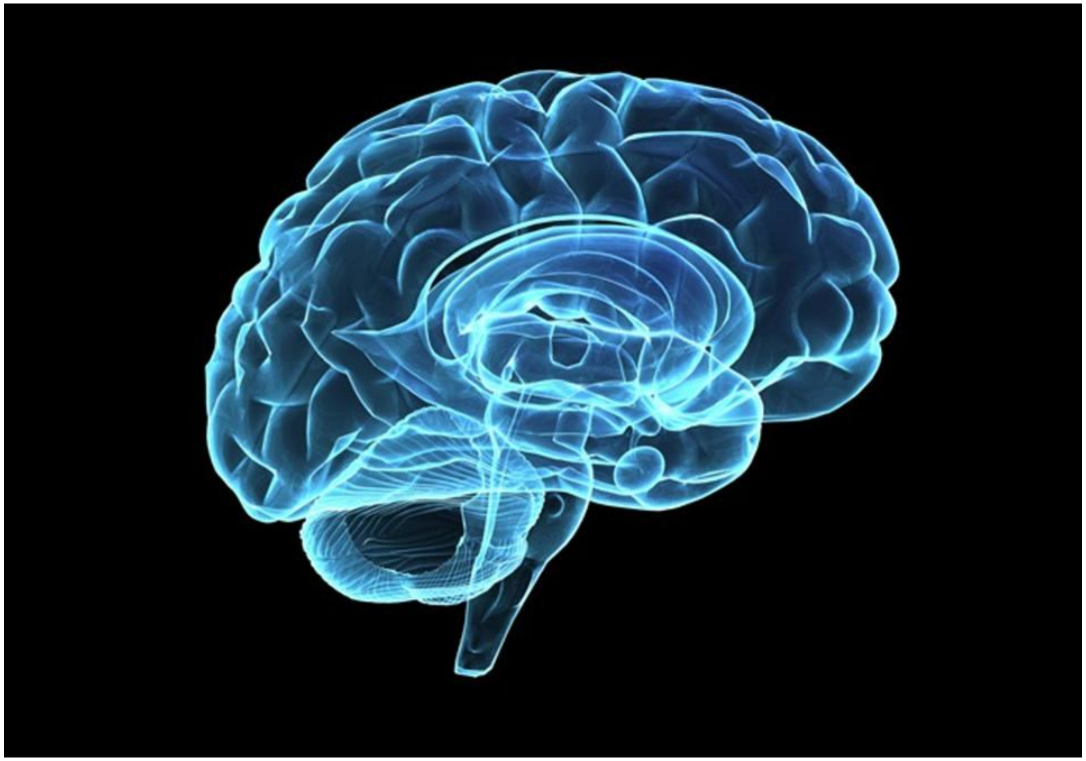
You can read and write

Name	Privilege
(Me)	Read & Write
staff	Read & Write
everyone	✓ Read only
	No Access

Tasks and Task Analysis



Memory



Working Memory – Short-term Memory

- George A. Miller (1956)
  - The magical number 7 ± 2.
  - The working memory can hold between 5 to 9 pieces of information.

- Revisions on this limit:
  - Broadbent (1975): 4-6
  - LeCompte (1999): 3

Common Practice: 4 ± 1

Chunking

oomgydliev

old veg me yo

video gym lo

i love my dog

3.14159265358979323846264338327950288 41
9716939937510582097494459230781640628 62
0899862803482534211706798214808651328 23
0664709384460955058223172535940812848 11
1745028410270193852110555964462294895 49
3038196442881097566593344612847564823 37
8678316527120190914564856692346034861 04
54326648213393607260249141273724587006
6063155881748815209209628292540917153 64
3678925903600113305305488204665213841 46
9519415116094330572703657595919530921 86
1173819326117931051185480744623799627 49
5673518857527248912279381830119491298 33
6733624406566430860213949463952247371 90
7021798609437027705392171762931767523 84
6748184676694051320005681271452635608 27
…

Chunking

3.141592653589793238462643383

↓

3.14 159265358979323846264338 3

↓

3.14 15 926 535 8979 323 846 264 3383

Ready for a test?

67890

Ready for a test?

983431312270	209
98 (34) 3131 2270	728
978012405531582	135
3728912	726
03758129	123456789101112
54856	2244668
24055	11223344
29607	12345
523	67890

Example: Information Chunking & Security

- The password must be at least eight characters long, and can contain letters, numerals, and punctuation.
- It cannot contain spaces.
- It must contain at least one alpha character [a-z; A-Z].
- It cannot contain your login ID.
- The first eight characters cannot be the same as your previous password.
- Passwords are treated as case sensitive.

1. password
2. 12345
3. 12345678
4. abc123
5. qwerty
6. monkey
7. letmein
8. dragon
9. 111111
10. baseball

Password Memory

- Create a password with chunks
  - 17#08#09Vr16#06#12as

- Research reveals that people's ability to remember
  - 7 character long password: ~ 50%
  - 4-chunk password: ~ 76%

Mental Models

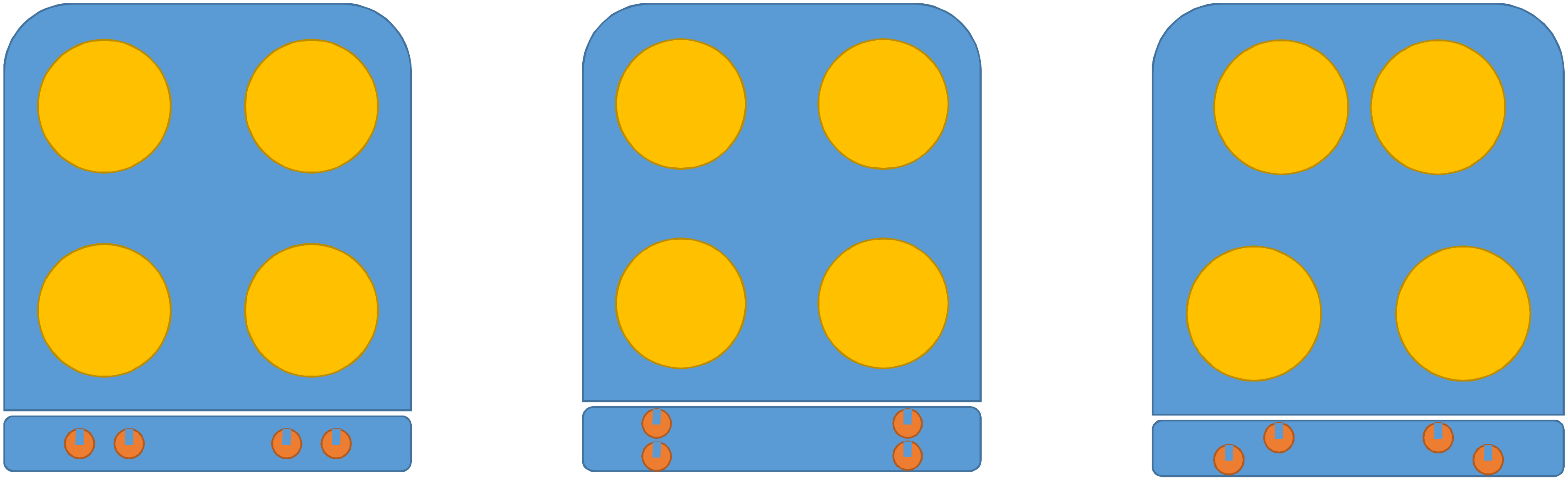
- let us understand how users perceive systems

Mental Models

- playing factors into developing mental models
    - affordances
        - things within a system that show a user how they are supposed to be used
        - important components: **mapping**, **visibility**, and **feedback**

Affordances: 1- Mapping

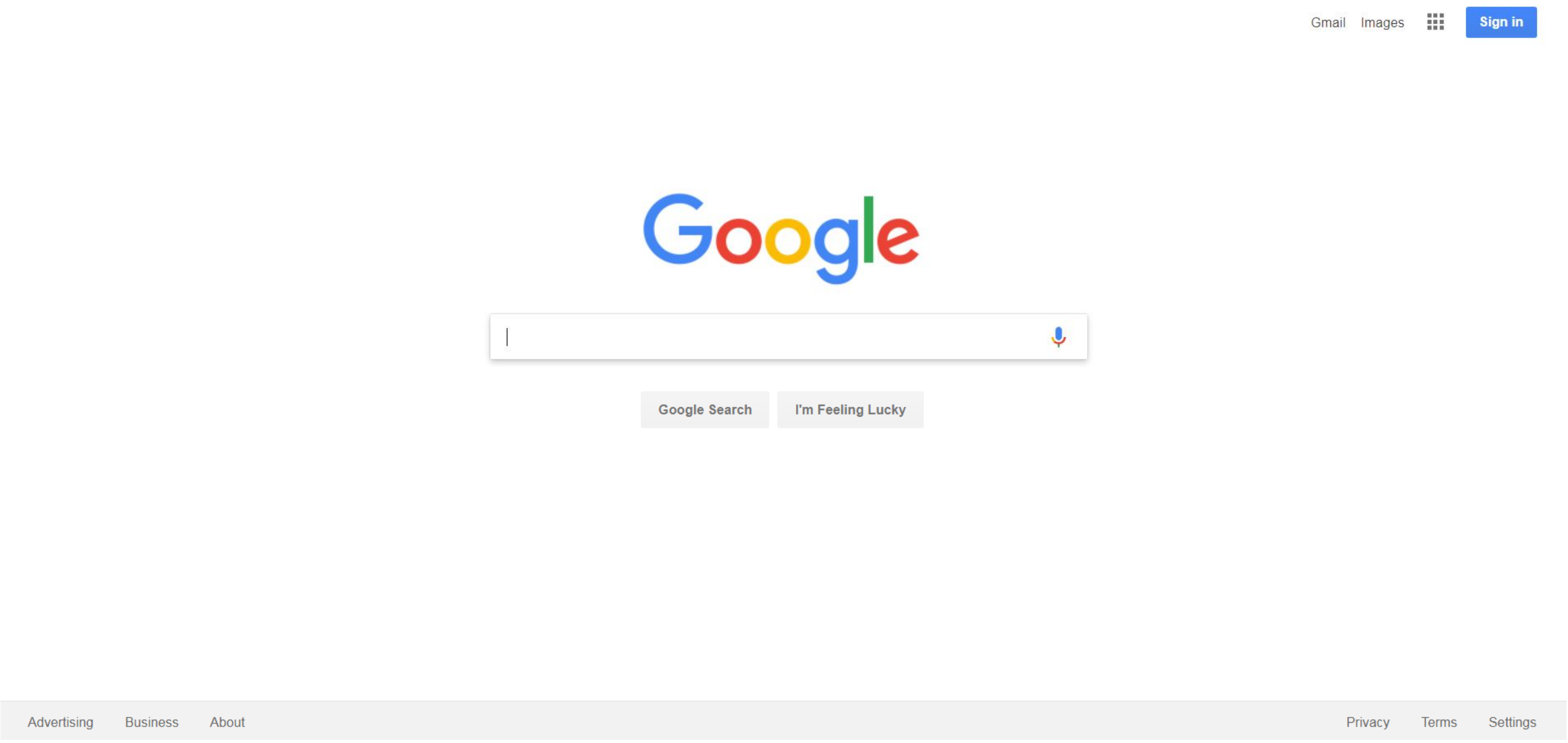
How certain functionalities will map to something that you see.



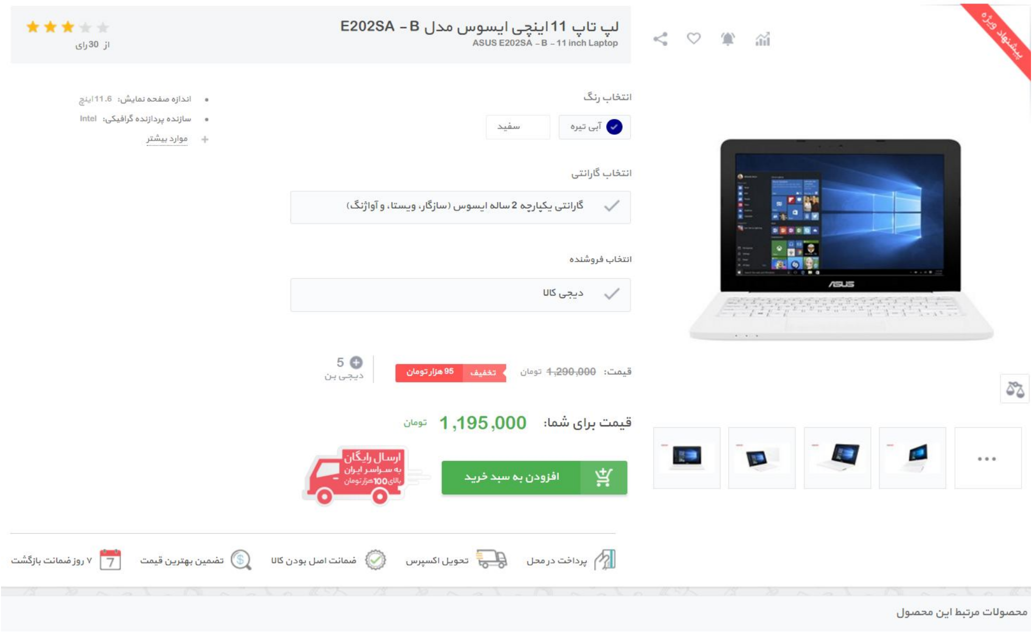
Affordances: 1- Mapping

How certain functionalities will map to something that you see.

Affordances: 2- Visibility



Affordances: 3- Feedback



پیشنهاد ویژه

لپ تاپ 11 اینچی ایسوس مدل E202SA - B
ASUS E202SA - B - 11 inch Laptop

★★★☆☆
از 30 رای

انتخاب رنگ

● ✓ آبی تیره | سفید

- اندازه صفحه نمایش: 11.6 اینچ
- سازنده پردازنده گرافیکی: Intel
- + موارد بیشتر

انتخاب گارانتی

✓ گارانتی یکپارچه 2 ساله ایسوس (سازگار، ویستا، و آواژنگ)

انتخاب فروشنده

✓ دیجی کالا

قیمت: ~~1,290,000~~ تومان تخفیف 95 هزار تومان

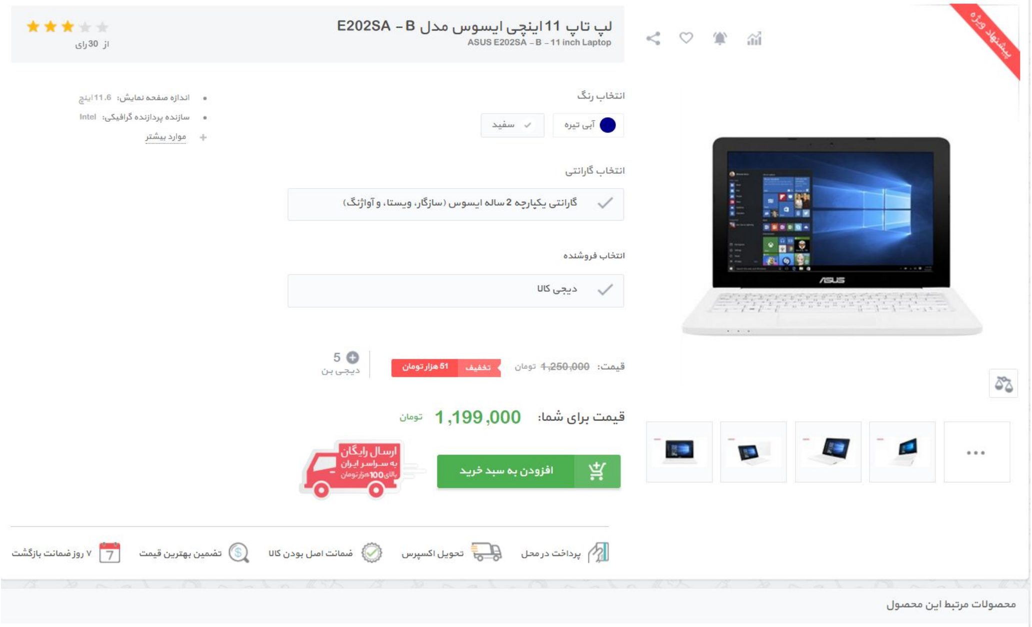
5 دیجی بن

قیمت برای شما: 1,195,000 تومان

افزودن به سبد خرید

پرداخت در محل | تحویل اکسپرس | ضمانت اصل بودن کالا | تضمین بهترین قیمت | ۷ روز ضمانت بازگشت

محصولات مرتبط این محصول



پیشنهاد ویژه

لپ تاپ 11 اینچی ایسوس مدل E202SA - B
ASUS E202SA - B - 11 inch Laptop

★★★☆☆
از 30 رای

انتخاب رنگ

● آبی تیره | ✓ سفید

- اندازه صفحه نمایش: 11.6 اینچ
- سازنده پردازنده گرافیکی: Intel
- + موارد بیشتر

انتخاب گارانتی

✓ گارانتی یکپارچه 2 ساله ایسوس (سازگار، ویستا، و آواژنگ)

انتخاب فروشنده

✓ دیجی کالا

قیمت: ~~1,250,000~~ تومان تخفیف 51 هزار تومان

5 دیجی بن

قیمت برای شما: 1,199,000 تومان

افزودن به سبد خرید

پرداخت در محل | تحویل اکسپرس | ضمانت اصل بودن کالا | تضمین بهترین قیمت | ۷ روز ضمانت بازگشت

محصولات مرتبط این محصول

Mental Models

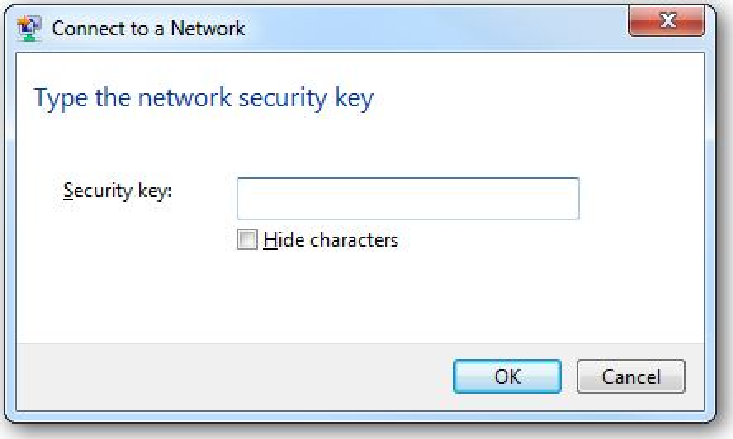
- playing factors into developing mental models
    - affordances
        - things within a system that show a user how they are supposed to be used
        - important components: **mapping**, **visibility**, and **feedback**
    - constraints

Constraints

how a system can prevent us from doing things that we should not and how the design of it can encourage us to do things the right way

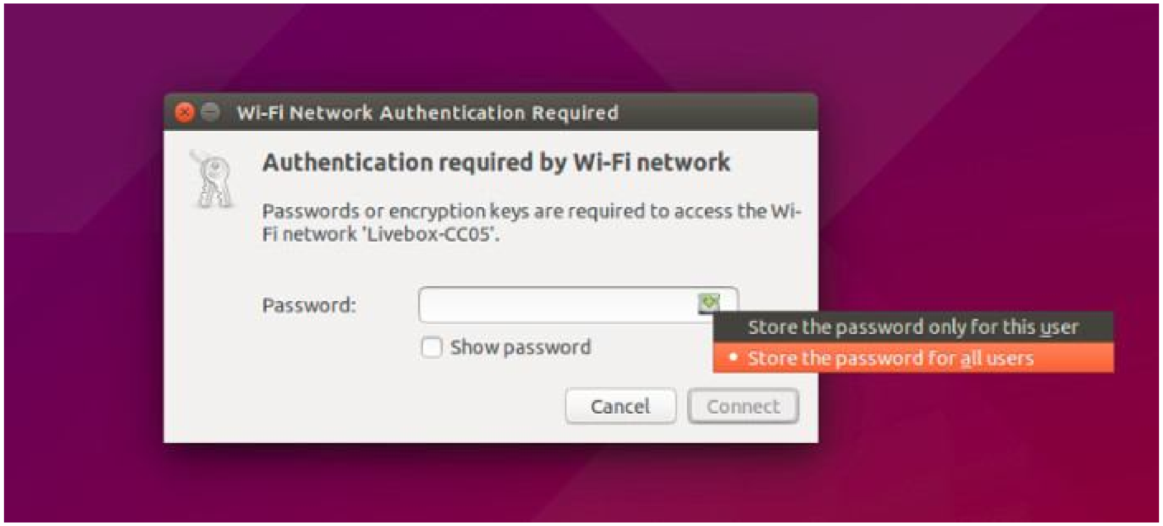
Constraints

how a system can prevent us from doing things that we should not and how the design of it can encourage us to do things the right way



Connect to a Network

Type the network security key



Wi-Fi Network Authentication Required

Authentication required by Wi-Fi network

Passwords or encryption keys are required to access the Wi-Fi network 'Livebox-CC05'.

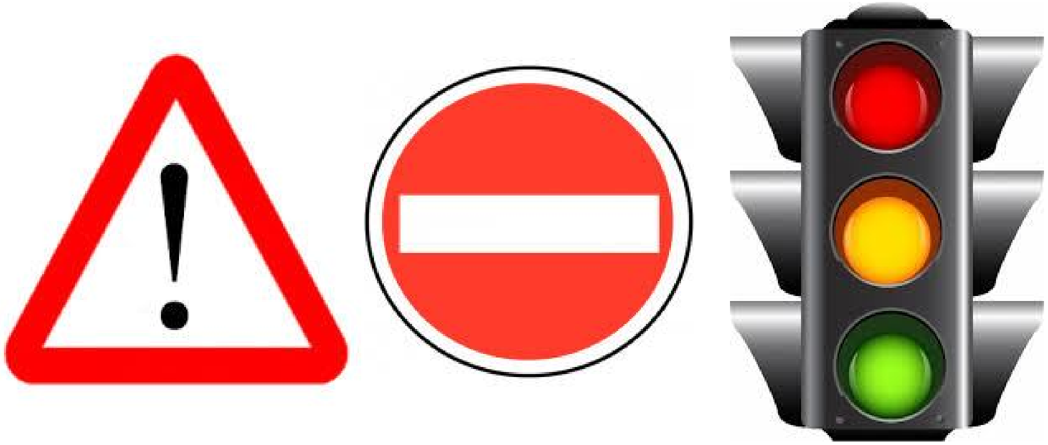
Password:
□ Show password
Store the password only for this user
● Store the password for all users
Cancel
Connect

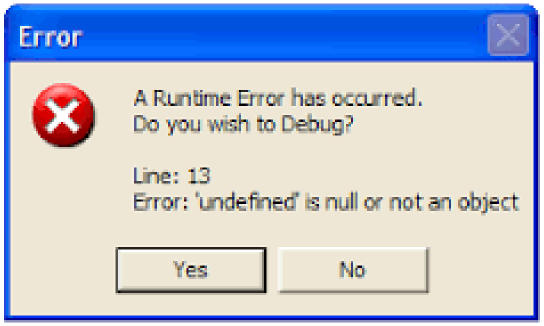
Mental Models

- playing factors into developing mental models
    - affordances
        - things within a system that show a user how they are supposed to be used
        - important components: **mapping**, **visibility**, and **feedback**
    - constraints
    - conventions

Conventions

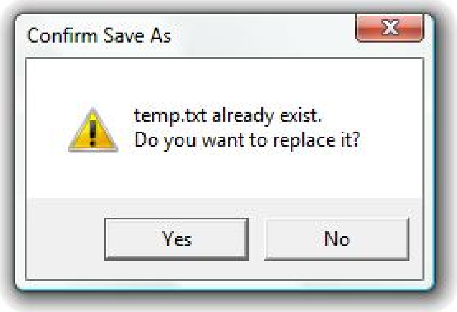
describe a common understanding of what something means



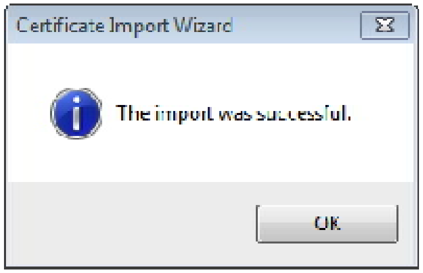


A Runtime Error has occurred.
Do you wish to Debug?

Line: 13
Error: 'undefined' is null or not an object



temp.txt already exist.
Do you want to replace it?



The import was successful.

Mental Models

- Labels
- Affordances
- Constraints
- Mappings
- Conventions

Assignment

- find at least **six security or privacy** interface element that you love or hate and share it with us. It could be a login screen, authentication mechanism, an option for sending secure email, a privacy setting interface, etc. It should NOT be an entire application or software program. In the discussion, you must:
    1. Provide a screen shot of the interface element.
    2. Describe what you think is great or terrible about the interface. This MUST be justified by and connected to the principles of usability we have discussed. It is not enough to say you love it or hate it. Tell us why is has good or bad usability using the things we have learned.

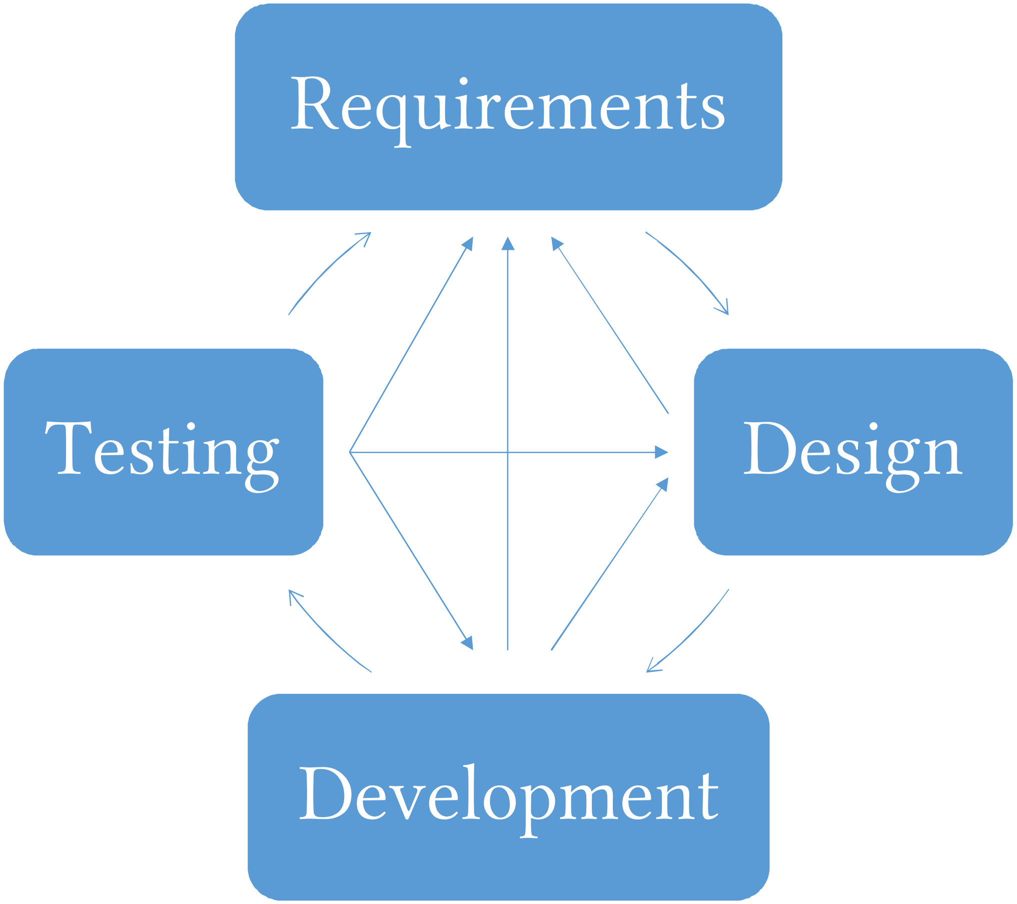
You will evaluate it, too.

1. Plagiarizing immediately results in 0 points for a question. Plagiarism is copying someone's words that are not your own, for example, by inserting an answer from a blog on the Web or Wikipedia.
2. The best answers are concise and to the point. A lot of words and a rambling response will fail to get your point across and confuse the student evaluating your answers.
3. You need to evaluate at least 5 of your classmates.
4. The reviews are anonymous.

Design Process

- where do ideas come from?
- many processes:
  - iterative design
  - system centered design
  - user centered design
  - participatory design
  - design centered design

Iterative Design



System Centered Design

- what can be built easily on this platform?
- what can I create from the available tools?
- what do I as a programmer find interesting to work on?

User Centered Design

- design is based upon a user's
  - abilities & real needs
  - context
  - work
  - tasks

Golden Rule of Interface Design
"Know the User"

Did you remember this?

User Centered Design

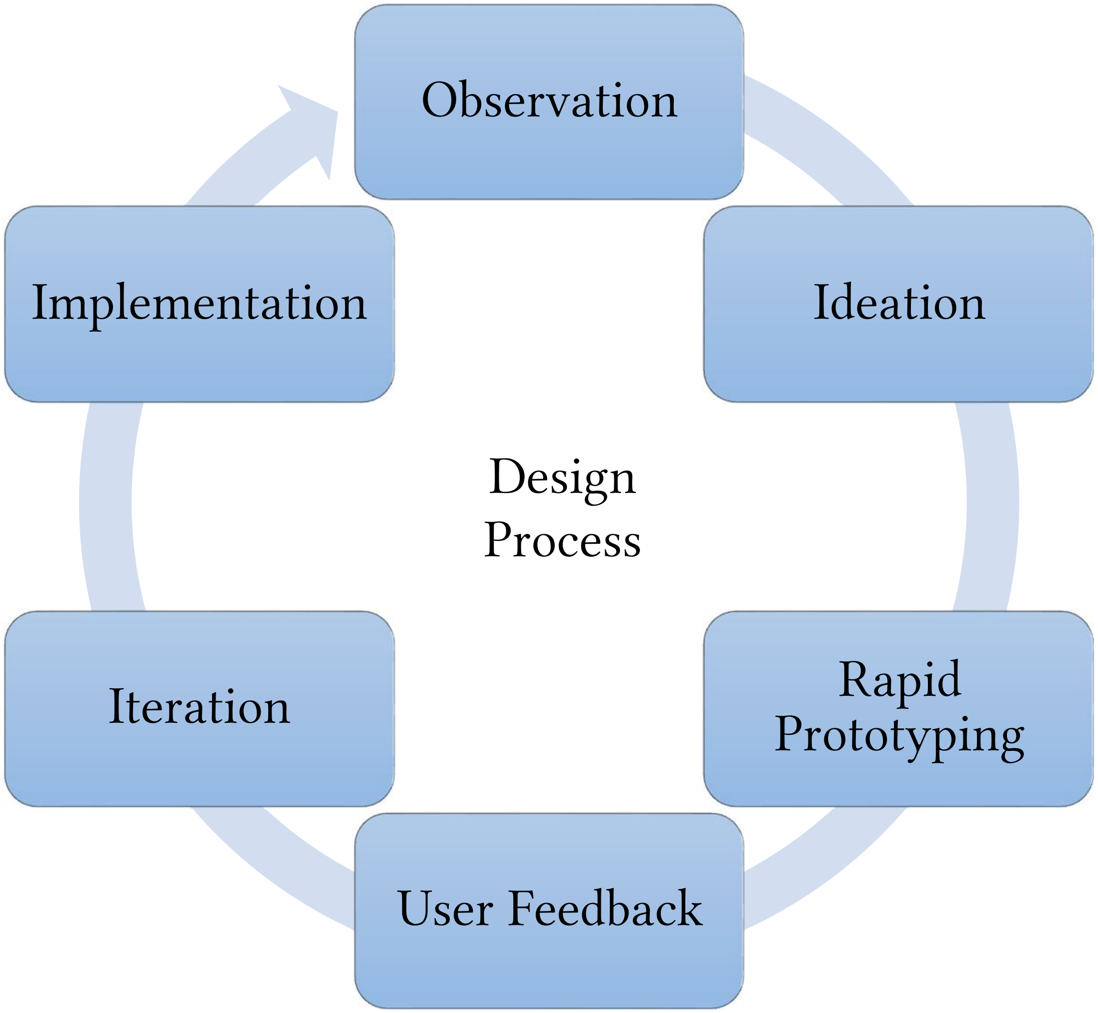
- design is based upon a user’s
  - abilities & real needs
  - context
  - work
  - tasks

Golden Rule of Interface Design
“Know the User”

Participatory Design

- problem
  - wrong intuitions
  - interviews & etc. are not precise
  - designer cannot know the user sufficiently well to answer all issues that come up during the design
- solution
  - designers should have access to pool of representative users
    - the END users, not their managers

Brainstorming



Designer Centered Design

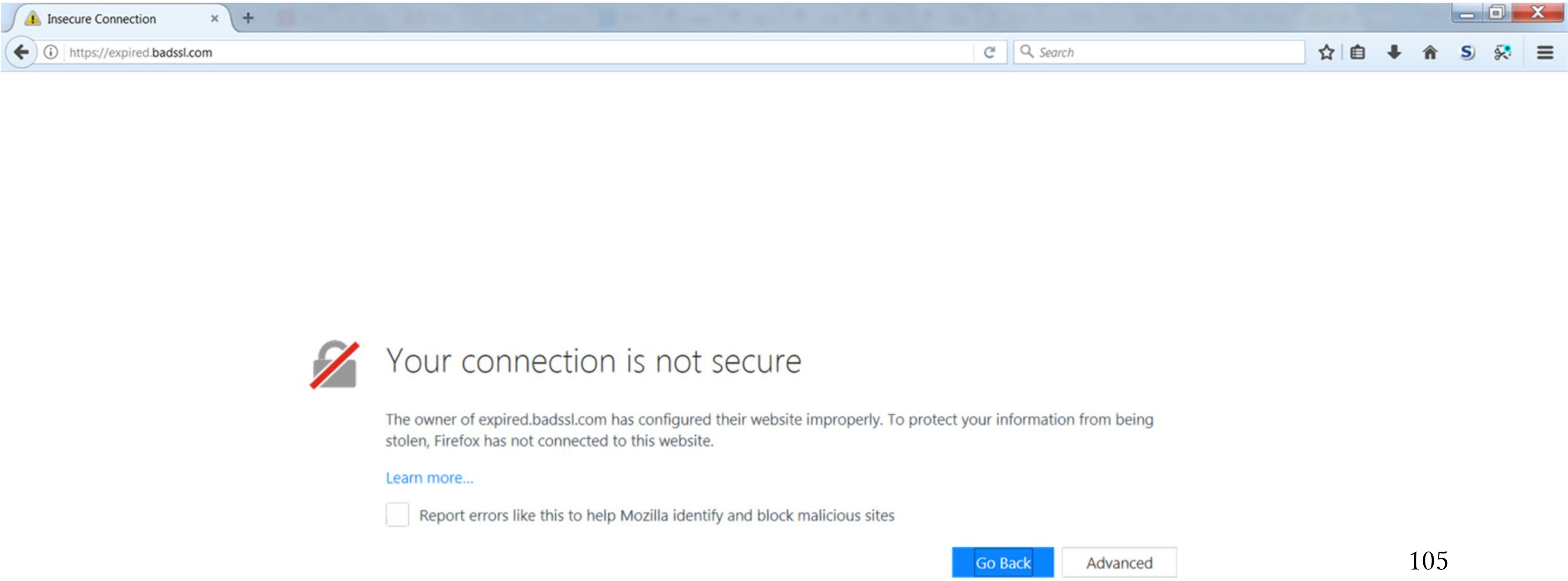
“It isn’t the consumers’ job to know what they want.”
--- Steve Jobs

Conclusions

- users can give a lot of valuable insights for design
  - tasks
  - context
  - needs
- support designers coming up with ideas
- iterate to build better systems

Example: Usability of Firefox's Untrusted Connection Error

https://expired.badssl.com/



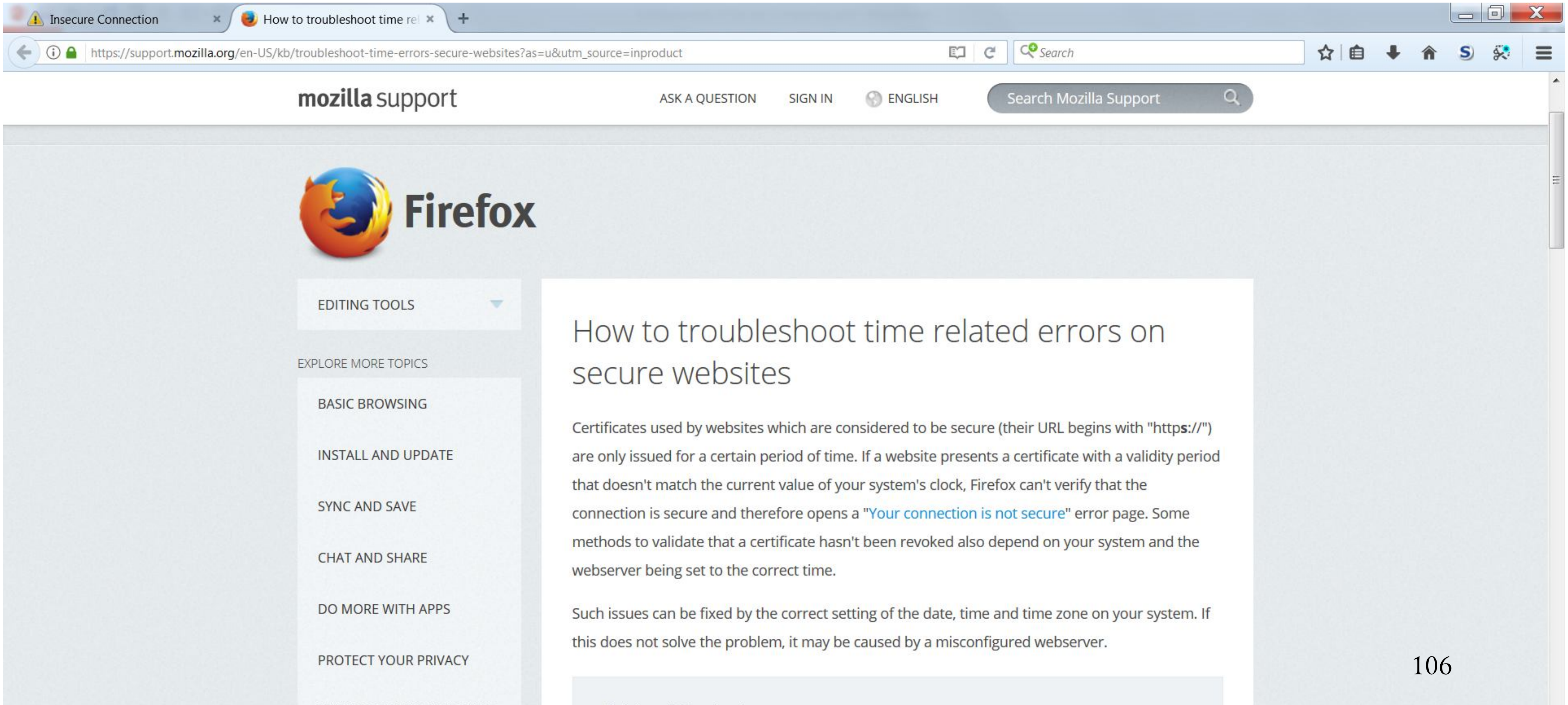
Your connection is not secure

The owner of expired.badssl.com has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

Learn more...

□ Report errors like this to help Mozilla identify and block malicious sites

If one clicks on “Learn More”

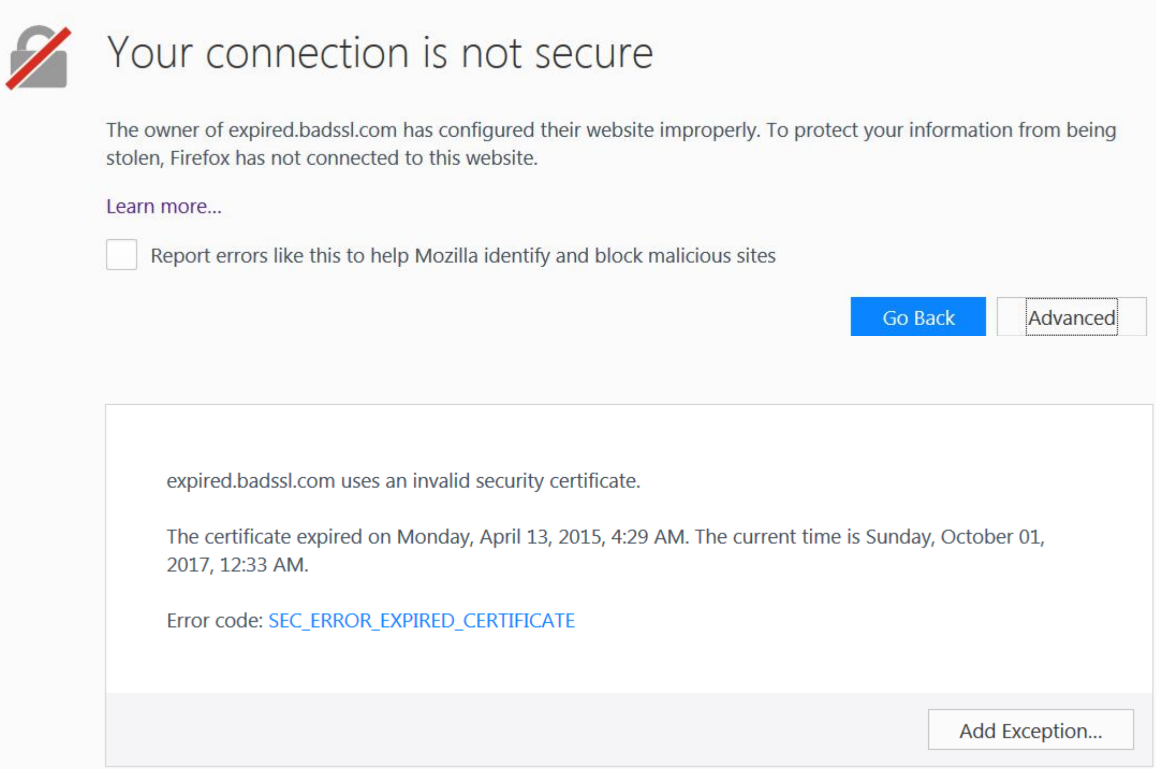


How to troubleshoot time related errors on secure websites

Certificates used by websites which are considered to be secure (their URL begins with "https://") are only issued for a certain period of time. If a website presents a certificate with a validity period that doesn't match the current value of your system's clock, Firefox can't verify that the connection is secure and therefore opens a "Your connection is not secure" error page. Some methods to validate that a certificate hasn't been revoked also depend on your system and the webserver being set to the correct time.

Such issues can be fixed by the correct setting of the date, time and time zone on your system. If this does not solve the problem, it may be caused by a misconfigured webserver.

or clicking on "Advanced"



Your connection is not secure

The owner of expired.badssl.com has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

Learn more...

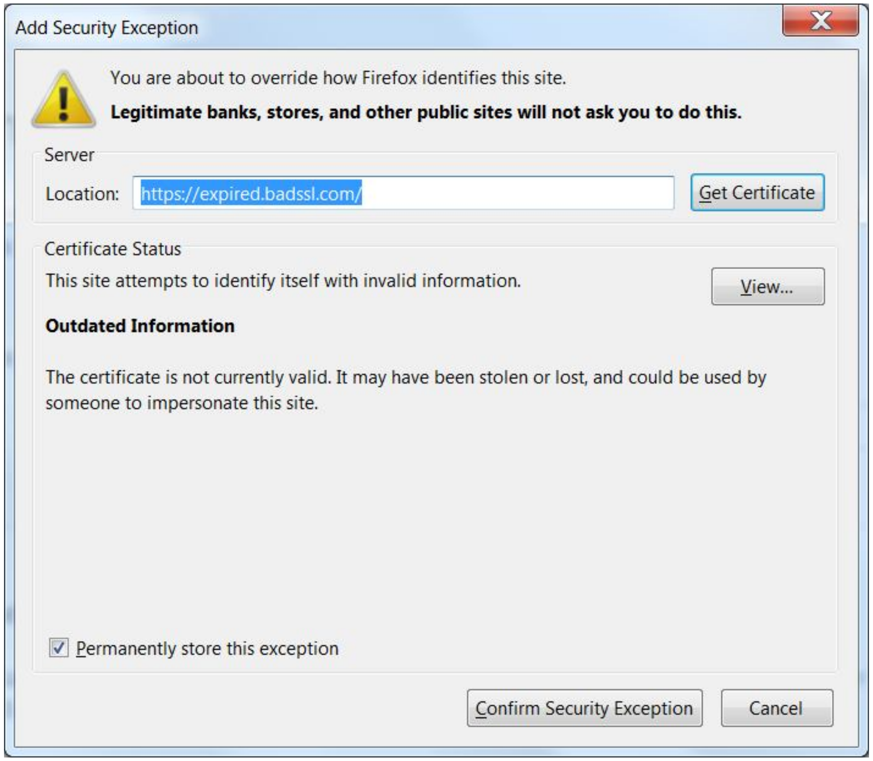
□ Report errors like this to help Mozilla identify and block malicious sites

expired.badssl.com uses an invalid security certificate.

The certificate expired on Monday, April 13, 2015, 4:29 AM. The current time is Sunday, October 01, 2017, 12:33 AM.

Error code: SEC_ERROR_EXPIRED_CERTIFICATE

Adding Exception



Add Security Exception

You are about to override how Firefox identifies this site.

Legitimate banks, stores, and other public sites will not ask you to do this.

Server

Location: https://expired.badssl.com/

Certificate Status

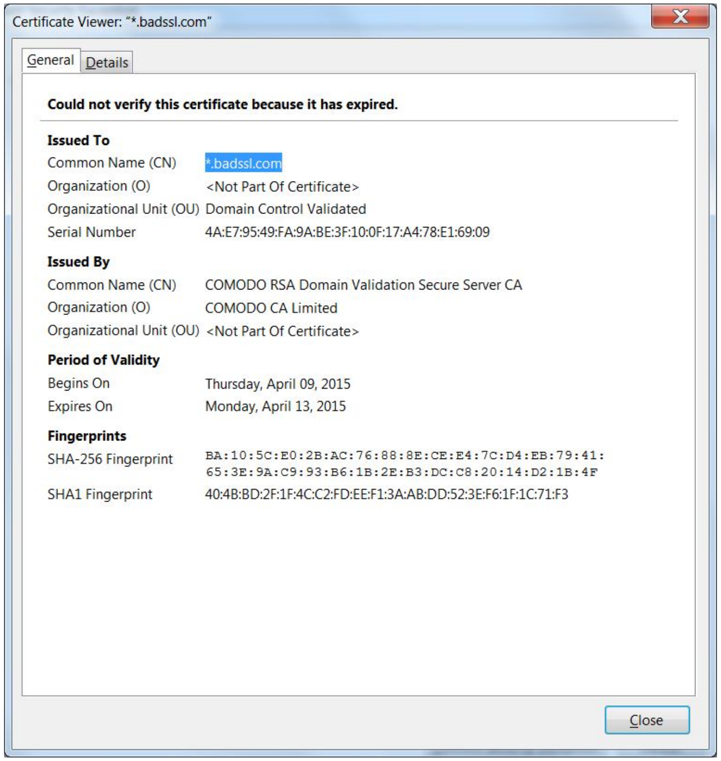
This site attempts to identify itself with invalid information.

Outdated Information

The certificate is not currently valid. It may have been stolen or lost, and could be used by someone to impersonate this site.

☑ Permanently store this exception

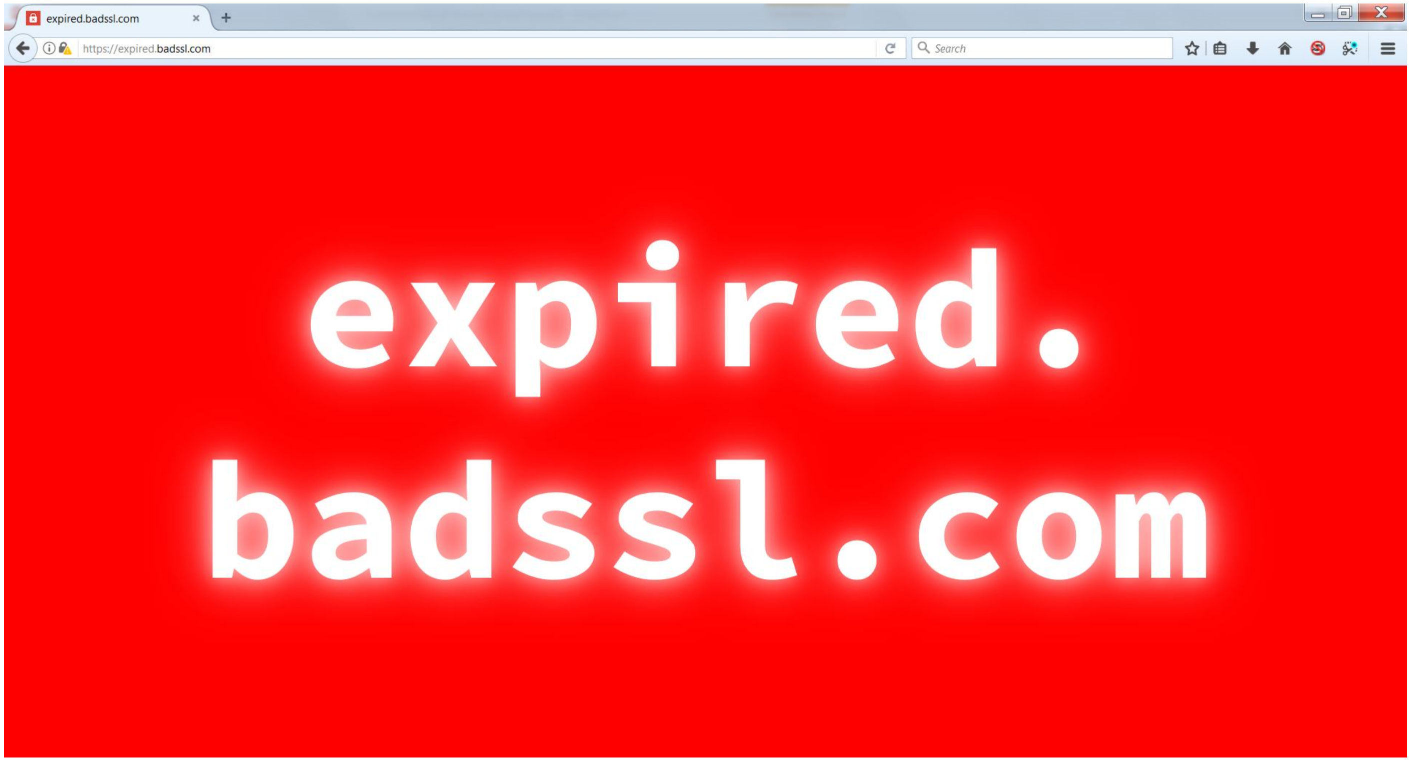
Viewing the Certificate



Could not verify this certificate because it has expired.

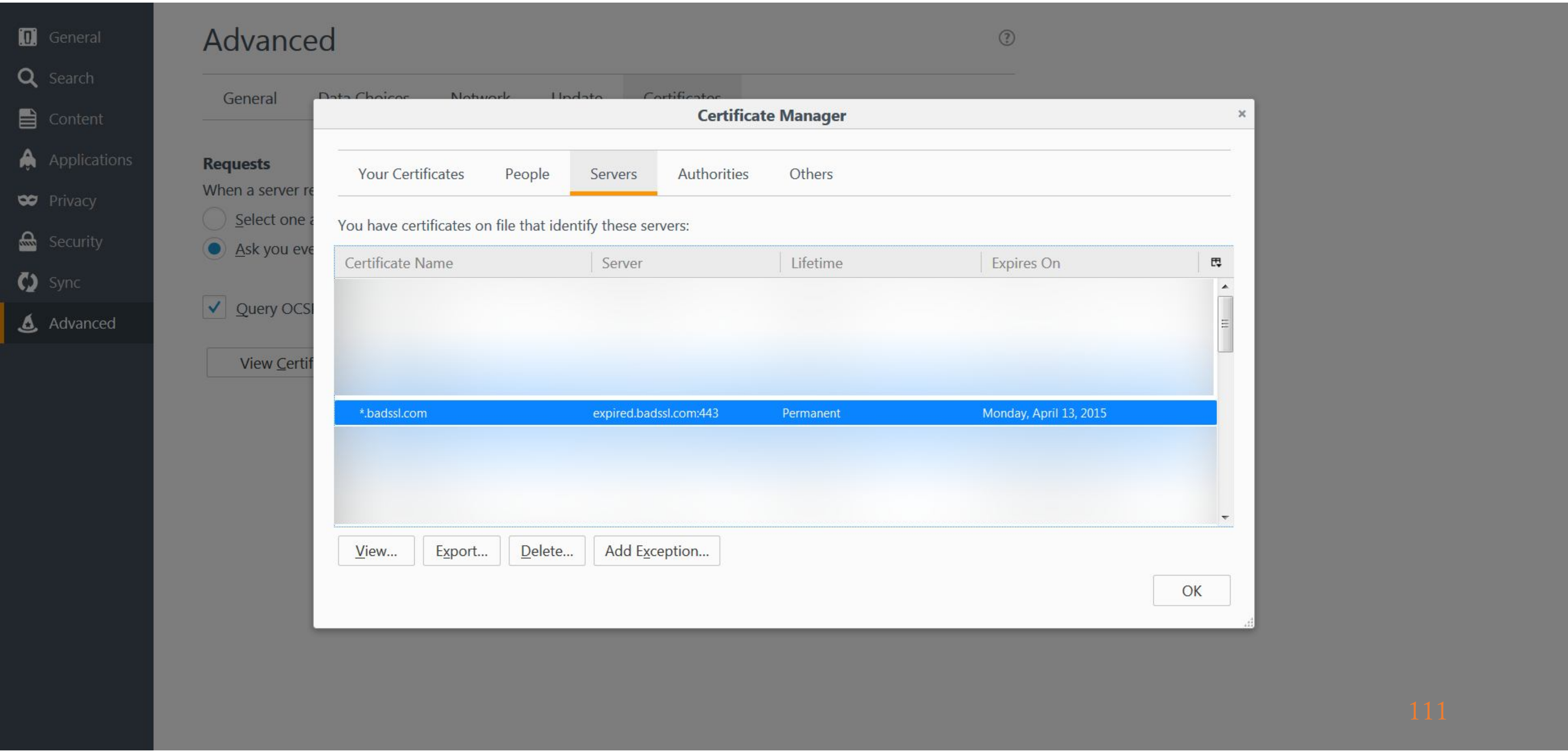
Issued To	
Common Name (CN)	*.badssl.com
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	Domain Control Validated
Serial Number	4A:E7:95:49:FA:9A:BE:3F:10:0F:17:A4:78:E1:69:09
Issued By	
Common Name (CN)	COMODO RSA Domain Validation Secure Server CA
Organization (O)	COMODO CA Limited
Organizational Unit (OU)	<Not Part Of Certificate>
Period of Validity	
Begins On	Thursday, April 09, 2015
Expires On	Monday, April 13, 2015
Fingerprints	
SHA-256 Fingerprint	BA:10:5C:E0:2B:AC:76:88:8E:CE:E4:7C:D4:EB:79:41: 65:3E:9A:C9:93:B6:1B:2E:B3:DC:C8:20:14:D2:1B:4F
SHA1 Fingerprint	40:4B:BD:2F:1F:4C:C2:FD:EE:F1:3A:AB:DD:52:3E:F6:1F:1C:71:F3

Confirming Security Exception



expired.
badssl.com

Removing the Certificate Exception



Certificate Manager

You have certificates on file that identify these servers:

Certificate Name	Server	Lifetime	Expires On
*.badssl.com	expired.badssl.com:443	Permanent	Monday, April 13, 2015

Lessons

- user knows something bad is happening, however not what.
- user has good general strategies (worry more about sites with sensitive info).
- error message relies on a lot of information users don’t understand.

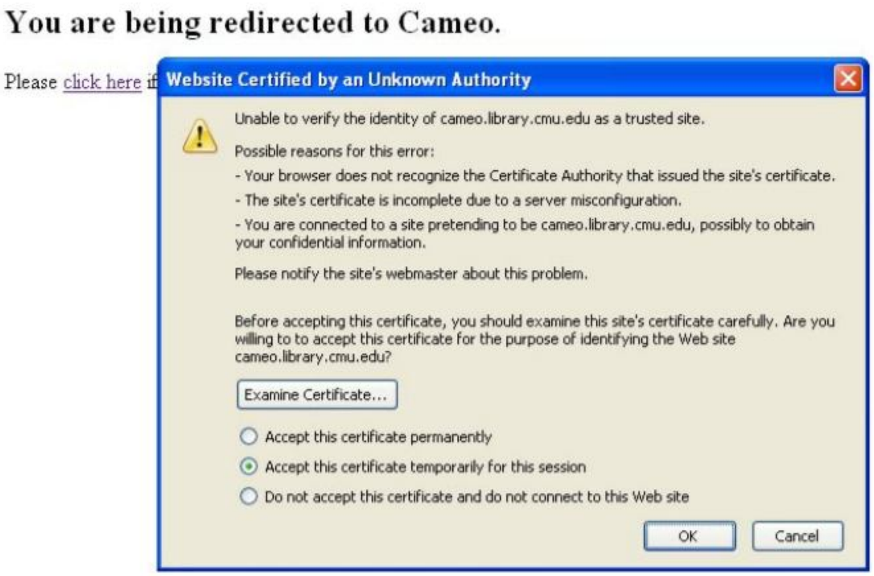
How could we improve this?

Case Study: SSL Warnings

We will study the following paper:

> Joshua Sunshine, Serge Egelman, Hazim Almuhimedi, Neha Atri, and Lorrie Faith Cranor. 2009. **Crying wolf: an empirical study of SSL warning effectiveness**. In *Proceedings of the 18th conference on USENIX security symposium* (SSYM'09). USENIX Association, Berkeley, CA, USA, 399-416.

Warnings Studied:



You are being redirected to Cameo.

Please click here if

Website Certified by an Unknown Authority

Unable to verify the identity of cameo.library.cmu.edu as a trusted site.

Possible reasons for this error:

- Your browser does not recognize the Certificate Authority that issued the site's certificate.

- The site's certificate is incomplete due to a server misconfiguration.

- You are connected to a site pretending to be cameo.library.cmu.edu, possibly to obtain your confidential information.

Please notify the site's webmaster about this problem.

Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to to accept this certificate for the purpose of identifying the Web site cameo.library.cmu.edu?

Examine Certificate...

○ Accept this certificate permanently

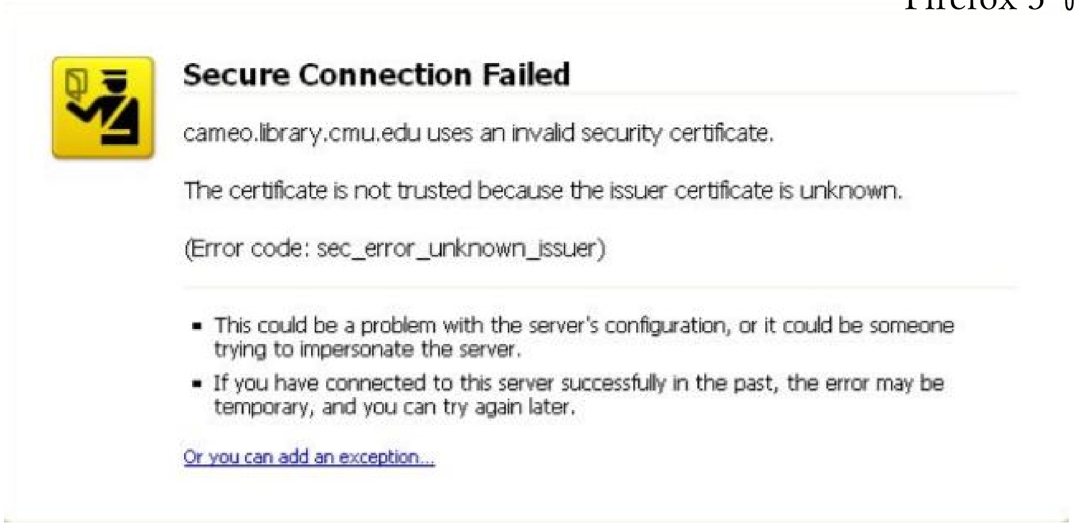
● Accept this certificate temporarily for this session

○ Do not accept this certificate and do not connect to this Web site

OK Cancel

Firefox 2 ☝

Firefox 3 ☟



Secure Connection Failed

cameo.library.cmu.edu uses an invalid security certificate.

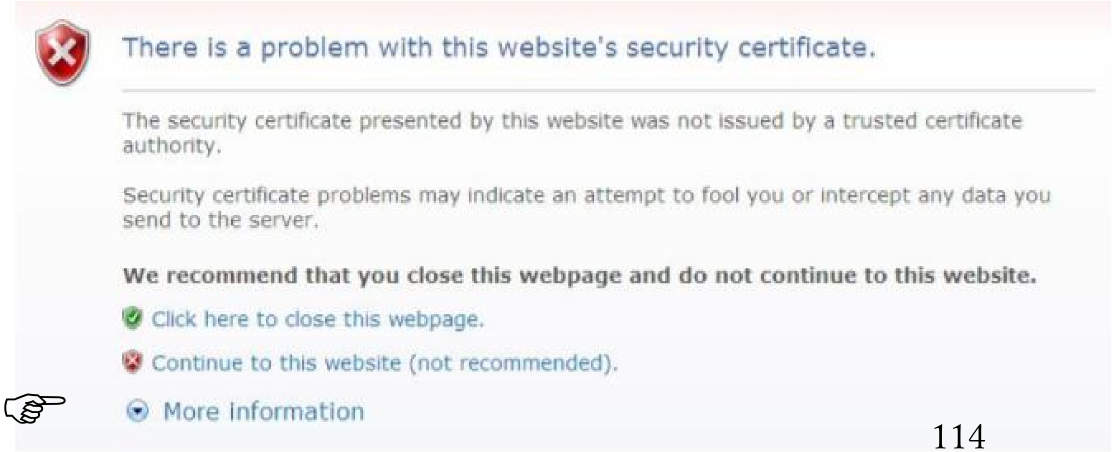
The certificate is not trusted because the issuer certificate is unknown.

(Error code: sec_error_unknown_issuer)

- This could be a problem with the server's configuration, or it could be someone trying to impersonate the server.
- If you have connected to this server successfully in the past, the error may be temporary, and you can try again later.

Or you can add an exception...

Internet Explorer 7 ☞



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

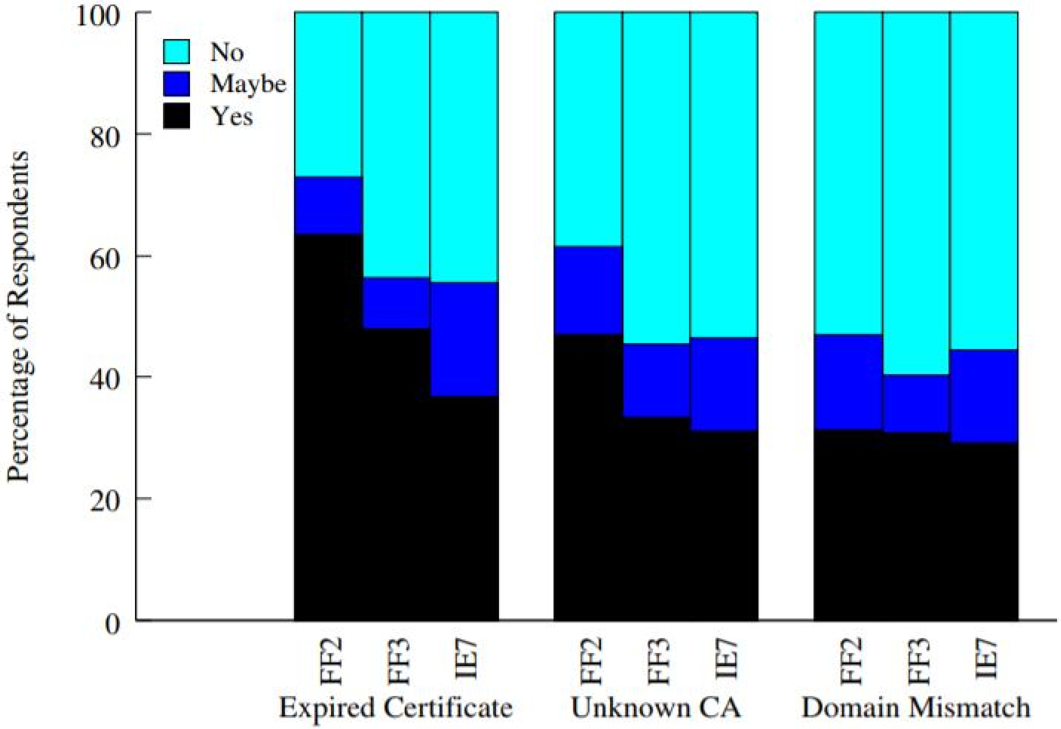
We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

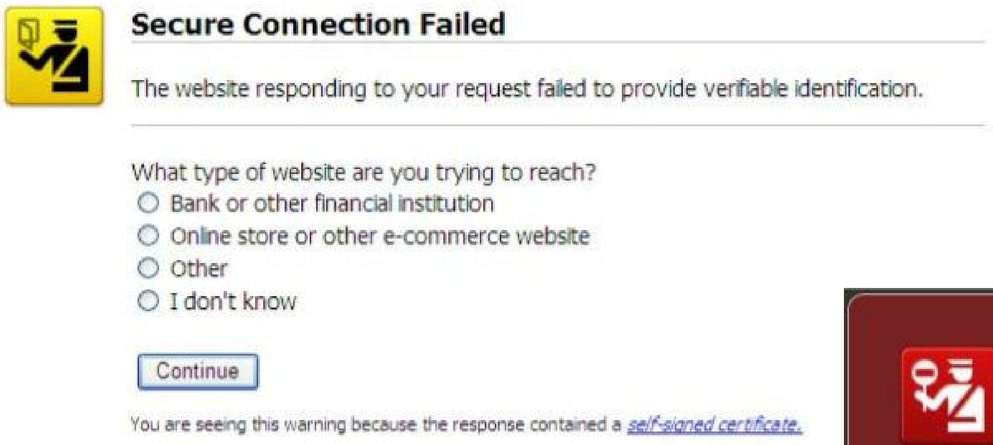
Responses to the question: “If you saw this message, would you attempt to continue to the website?”



Comments of People who Continued …

- “I use a Mac so nothing bad would happen.”
- “Since I use FreeBSD, rather than Windows, not much [risk].”
- “On my Linux box, nothing significantly bad would happen.”

Redesigned Warnings



Secure Connection Failed

The website responding to your request failed to provide verifiable identification.

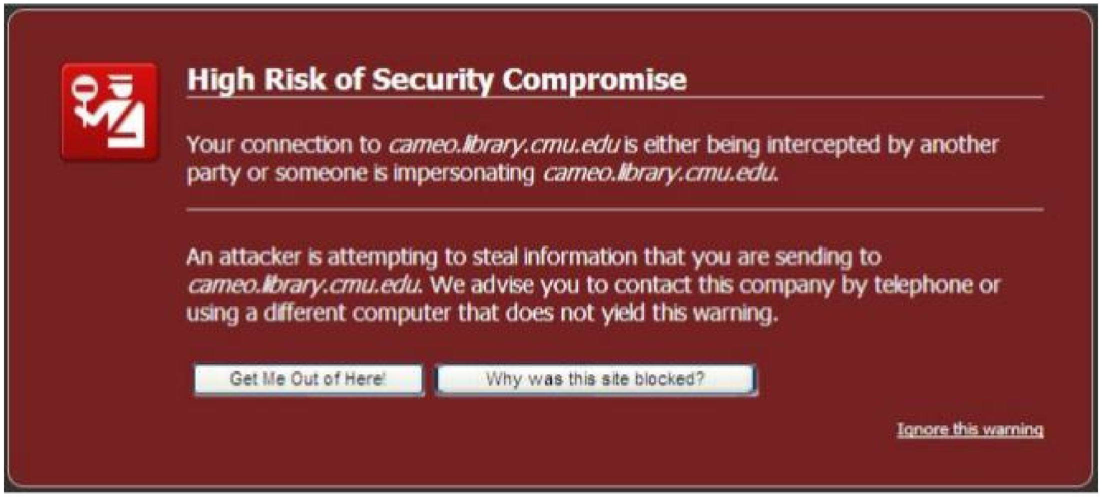
What type of website are you trying to reach?

○ Bank or other financial institution
○ Online store or other e-commerce website
○ Other
○ I don't know

You are seeing this warning because the response contained a self-signed certificate.

Page 1 ☝

Page 2 ☟

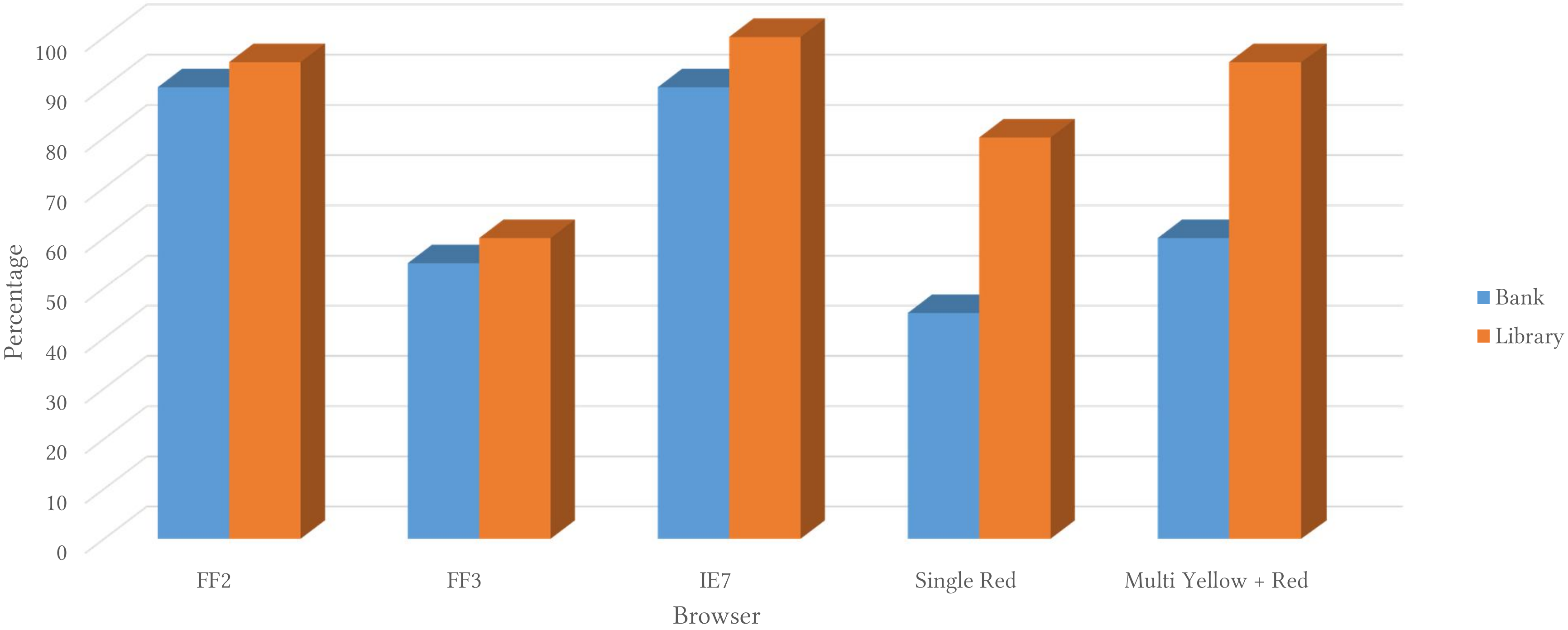


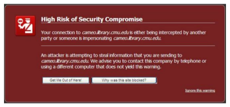
High Risk of Security Compromise

Your connection to *cameo.library.cmu.edu* is either being intercepted by another party or someone is impersonating *cameo.library.cmu.edu*.

An attacker is attempting to steal information that you are sending to *cameo.library.cmu.edu*. We advise you to contact this company by telephone or using a different computer that does not yield this warning.

Users Ignoring Warnings

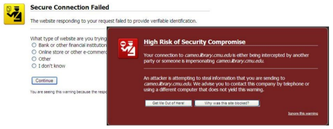




High Risk of Security Compromise

Your connection to *cameo.library.cmu.edu* is either being intercepted by another party or someone is impersonating *cameo.library.cmu.edu*.

An attacker is attempting to steal information that you are sending to *cameo.library.cmu.edu*. We advise you to contact this company by telephone or using a different computer that does not yield this warning.



Secure Connection Failed

The website responding to your request failed to provide verifiable identification.

What type of website are you trying

○ Bank or other financial institution

○ Online store or other e-commerc

○ Other

○ I don't know

You are seeing this warning because the respo

High Risk of Security Compromise

Your connection to *cameo.library.cmu.edu* is either being intercepted by another party or someone is impersonating *cameo.library.cmu.edu*.

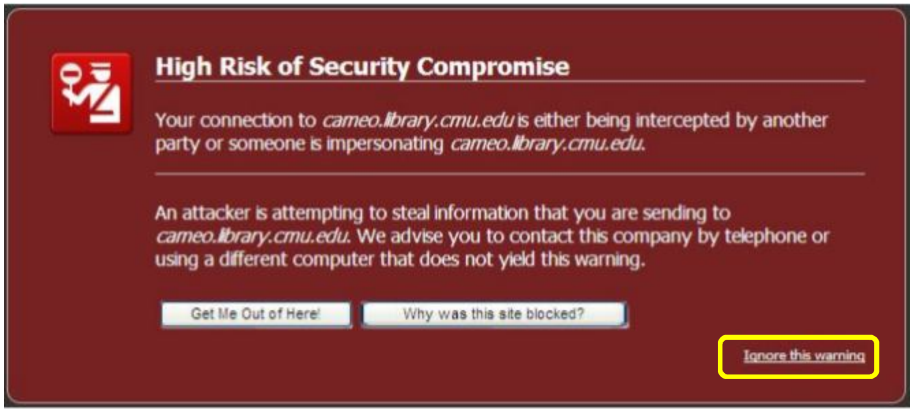
An attacker is attempting to steal information that you are sending to *cameo.library.cmu.edu*. We advise you to contact this company by telephone or using a different computer that does not yield this warning.

Users who logged in

Condition	Read	Didn't Read	Understood	Didn't Understand
FF2	20%	70%	35%	55%
FF3	10%	45%	20%	35%
IE7	20%	70%	40%	50%
Single Red Page	20%	25%	20%	25%
Multi Yellow Red Pages	40%	20%	35%	25%

Lessons

- different interfaces can have major impacts on the security behavior of users.
- what do we want users to do?
- what do they need to understand to do that?
- how can we make it more natural for them to do the “right” thing?



High Risk of Security Compromise

Your connection to *cameo.library.cmu.edu* is either being intercepted by another party or someone is impersonating *cameo.library.cmu.edu*.

An attacker is attempting to steal information that you are sending to *cameo.library.cmu.edu*. We advise you to contact this company by telephone or using a different computer that does not yield this warning.

Assignments

Evaluation

- how to **evaluate** the usability of systems
  - a critical component of building usable systems for security
  - how usable your system is
  - identify specific problems with the usability

- often, evaluations are large-scale and expensive
  - there are options that are easy to do on your own that follow good guidelines

- Systems can be evaluated
  - **quantitatively** (with numbers) or ,
  - **qualitatively** (through experience and description)

The main goal of evaluation

The goal of evaluation is ultimately to identify usability problems so the interface can be refined and improved.

Qualitative Evaluation

Cognitive Walkthrough

- requirements
  - description or prototype of interface
  - task description
  - list of actions to complete task
  - user background

- what you look for?
  - will users know to perform the action?
  - will users see the control?
  - **will users know the control does what they want?**
  - will users understand the feedback?

Demo of Cognitive Analysis of Mobile Authentication System

Heuristic Analysis

- follow “rules of thumb” or suggestions about good design
- can be done by experts / designers, fast & easy
- may miss problems users would catch

What are these “rules of thumb”?

Nielsen’s Heuristics

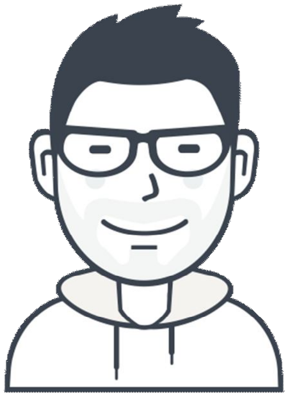
- simple & natural dialog
- speak the user language
- minimize user memory load
- consistency
- feedback
- clearly marked exits
- shortcuts
- prevent errors
- good error messages
- provide help & documentation

Demo of Nielsen's Heuristics for Mobile Authentication System

Personas

- a fictitious user representing a class of users
- reference point for design & analysis
- has a goal or goals they want to accomplish
    - in general or in the system

Persona: Ali



wants encryption but in a simple, low-effort way.

Undergraduate Student

- 20 years old
- Literature Major
- Cultural Activist
- Savvy computer user, but not expert

Goals

wants easy to use email & social media tools that are encrypted to protect his privacy

About Ali

Ali is an undergraduate student of literature at the Vali-e-Asr university of Rafsanjan. He enjoys playing tennis & watching movies. He always carries his smart phone which is an android phone. He also has a laptop. His mobile phone is constantly connected to the Internet through the carrier's data connection. He is always worried that his activities are monitored by his parents.

Demo of Using Personas for Analysis of the Mobile Authentication System

Conclusion

- qualitative evaluation can provide insights into the usability of a system without measurements or timing
- various levels of complexity
- can be quick & inexpensive, but may miss insights users provide

Running Controlled Experiments

Controlled Experiment

- state a lucid, testable hypothesis
- identify independent & dependent variables
- design the experimental protocol
- choose the user population
- run some pilot participants
- fix the experimental protocol
- run the experiment
- perform statistical analysis
- draw conclusions
- communicate results

Demo: Compare the Gesture-based Authentication on Android Phones with Password-based Authentication

State a Lucid, Testable Hypothesis

mobile phone login with gesture is faster than with password entry

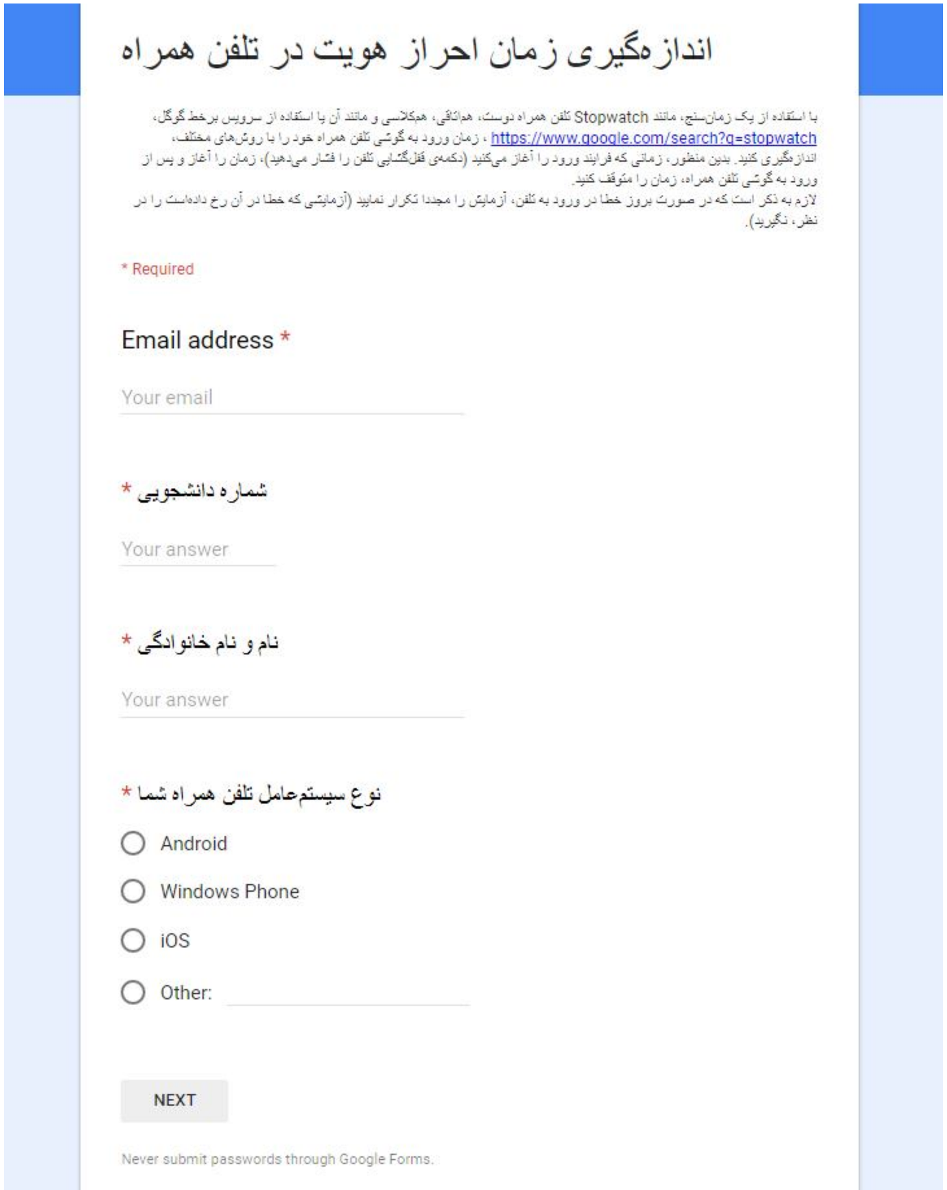
Choose the Variables

- manipulate one or more **independent** variables (the thing you change)
  - login method
- observe effect on one or more **dependent** variables (the thing that you measure)
  - time to login

Design the Experimental Protocol

- choose tasks
- between or within subjects?
    - between subjects
        - each subject runs one condition
    - within subjects
        - each subject runs several conditions

https://goo.gl/forms/abtZzg0mfiiGew6v2



اندازه‌گیری زمان احراز هویت در تلفن همراه

با استفاده از یک زمان‌سنج، مانند Stopwatch تلفن همراه دوست، هم‌اتاقی، همکلاسی و مانند آن یا استفاده از سرویس برخط گوگل،
https://www.google.com/search?q=stopwatch ، زمان ورود به گوشی تلفن همراه خود را با روش‌های مختلف،
اندازه‌گیری کنید. بدین منظور، زمانی که فرایند ورود را آغاز می‌کنید (دکمه‌ی قفل‌گشایی تلفن را فشار می‌دهید)، زمان را آغاز و پس از
ورود به گوشی تلفن همراه، زمان را متوقف کنید.
لازم به ذکر است که در صورت بروز خطا در ورود به تلفن، آزمایش را مجددا تکرار نمایید (آزمایشی که خطا در آن رخ داده‌است را در
نظر، نگیرید).

* Required

Email address *

Your email

شماره دانشجویی *

Your answer

نام و نام خانوادگی *

Your answer

نوع سیستم‌عامل تلفن همراه شما *

○ Android

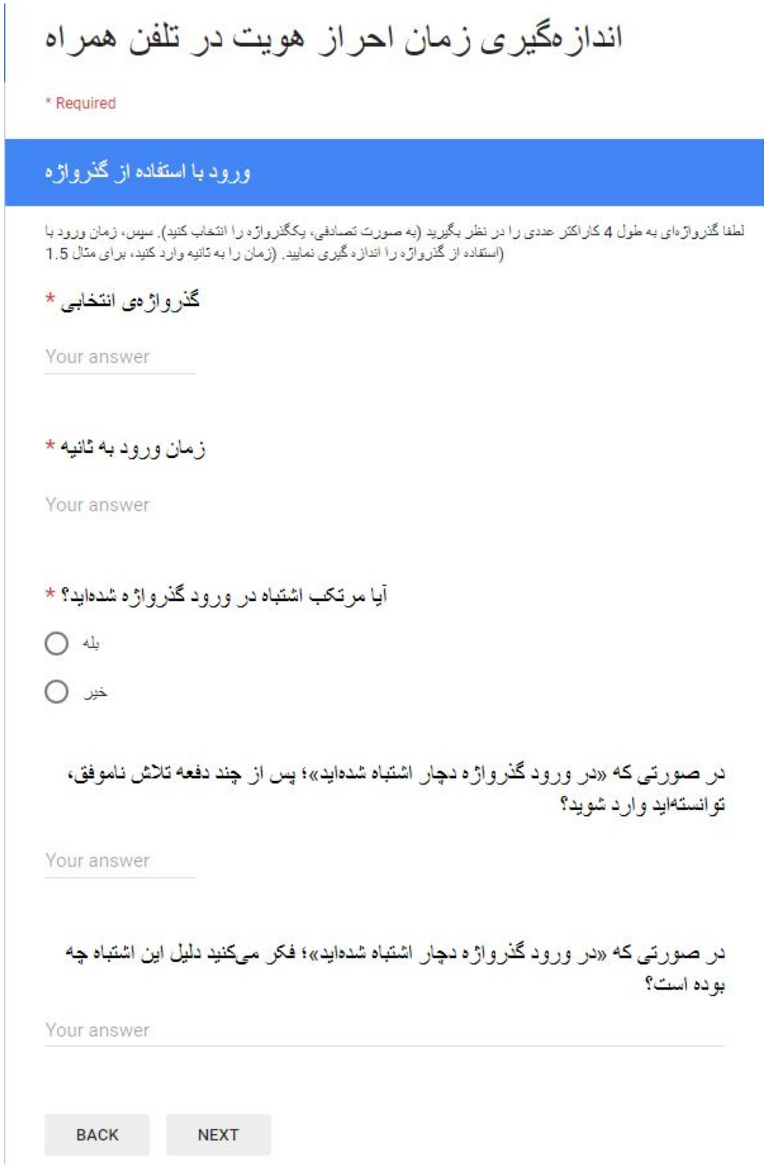
○ Windows Phone

○ iOS

○ Other: ____

Never submit passwords through Google Forms.

https://goo.gl/forms/abtZzg0mfiiGew6v2



اندازه‌گیری زمان احراز هویت در تلفن همراه

* Required

ورود با استفاده از گذرواژه

لطفا گذرواژه‌ای به طول 4 کاراکتر عددی را در نظر بگیرید (به صورت تصادفی، یکگذرواژه را انتخاب کنید). سپس، زمان ورود با استفاده از گذرواژه را اندازه گیری نمایید. (زمان را به ثانیه وارد کنید، برای مثال 1.5)

گذرواژه‌ی انتخابی *

Your answer

زمان ورود به ثانیه *

Your answer

آیا مرتکب اشتباه در ورود گذرواژه شده‌اید؟ *

○ بله

○ خیر

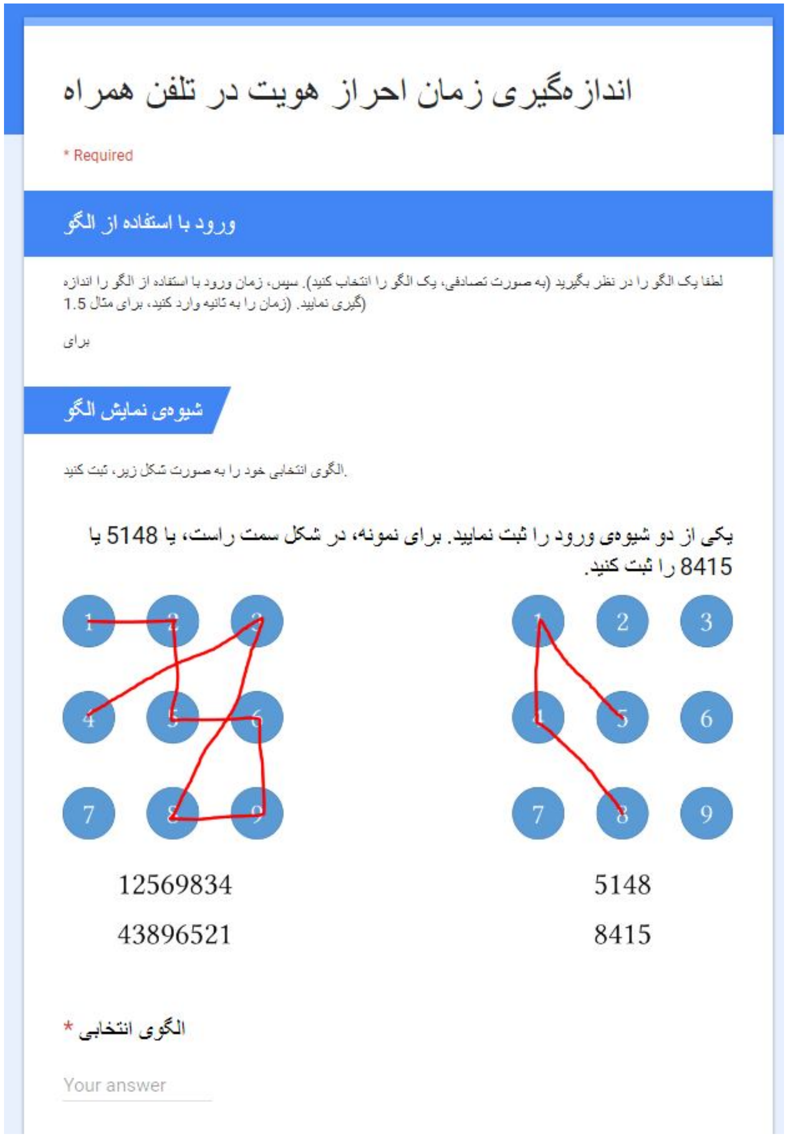
در صورتی که «در ورود گذرواژه دچار اشتباه شده‌اید»؛ پس از چند دفعه تلاش ناموفق، توانسته‌اید وارد شوید؟

Your answer

در صورتی که «در ورود گذرواژه دچار اشتباه شده‌اید»؛ فکر می‌کنید دلیل این اشتباه چه بوده است؟

Your answer

https://goo.gl/forms/abtZzg0mfiiGew6v2



اندازه‌گیری زمان احراز هویت در تلفن همراه

* Required

ورود با استفاده از الگو

لطفا یک الگو را در نظر بگیرید (به صورت تصادفی، یک الگو را انتخاب کنید). سپس، زمان ورود با استفاده از الگو را اندازه
گیری نمایید. (زمان را به ثانیه وارد کنید، برای مثال 1.5

برای

شیوه‌ی نمایش الگو

الگوی انتخابی خود را به صورت شکل زیر، ثبت کنید.

یکی از دو شیوه‌ی ورود را ثبت نمایید. برای نمونه، در شکل سمت راست، یا 5148 یا
8415 را ثبت کنید.

12569834

43896521

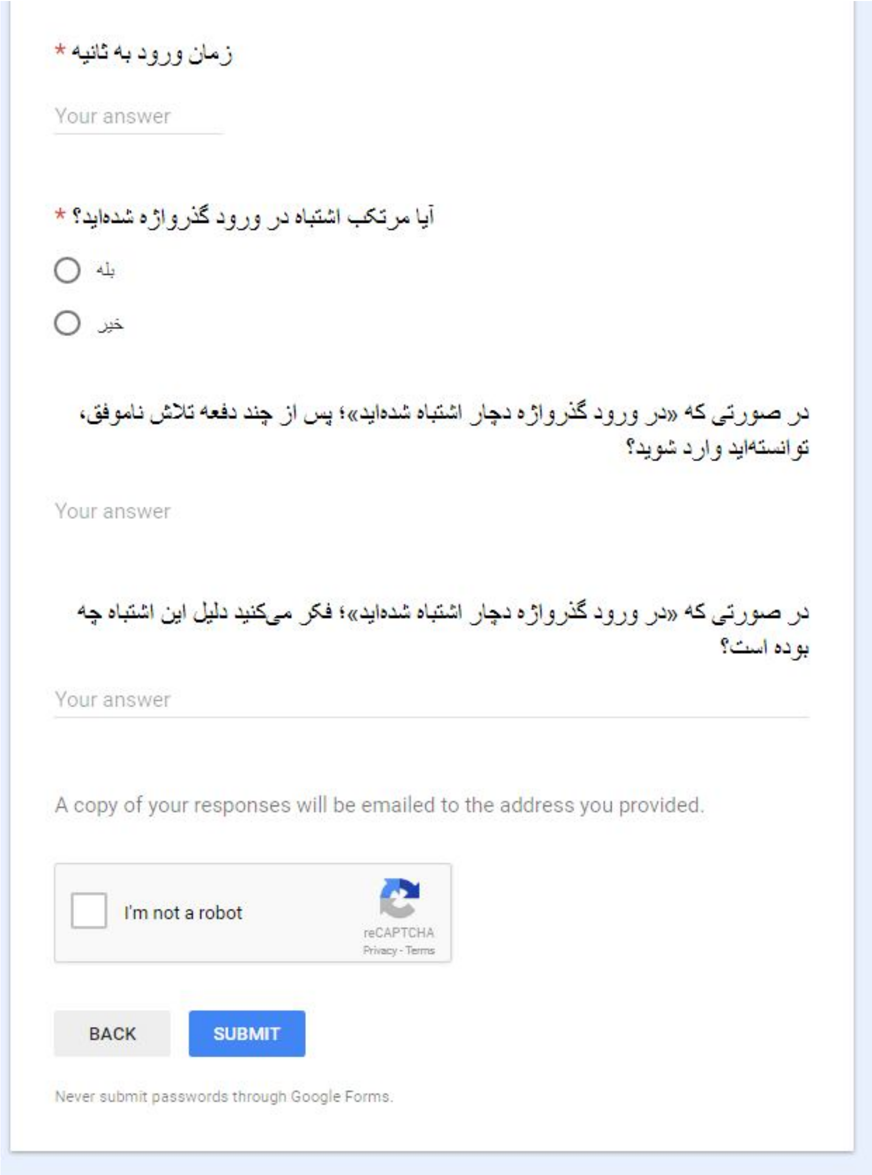
5148

8415

الگوی انتخابی *

Your answer

https://goo.gl/forms/abtZzg0mfiiGew6v2



زمان ورود به ثانیه *

Your answer

آیا مرتکب اشتباه در ورود گذرواژه شده‌اید؟ *

○ بله

○ خیر

در صورتی که «در ورود گذرواژه دچار اشتباه شده‌اید»؛ پس از چند دفعه تلاش ناموفق،
توانسته‌اید وارد شوید؟

Your answer

در صورتی که «در ورود گذرواژه دچار اشتباه شده‌اید»؛ فکر می‌کنید دلیل این اشتباه چه
بوده است؟

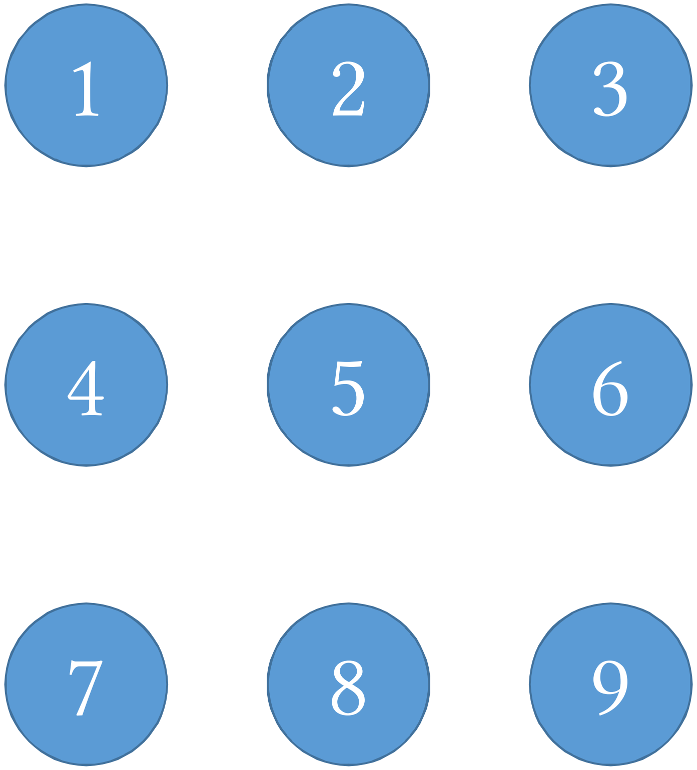
Your answer

A copy of your responses will be emailed to the address you provided.

□ I'm not a robot

Never submit passwords through Google Forms.

Gesture Coding Rules



1 2 3

4 5 6

7 8 9

Run the experiment

- run a pilot study
- have a checklist of steps, so all users are the same
- collect data

Analysis

- statistical comparison (e.g. t-test)
- report results

Now, it's your turn ...

- go & fill the form at https://goo.gl/forms/abtZzg0mfiiGew6v2
  - every student needs to do the experiment with **10 different** passwords & **10 different** gestures, interleavingly.
  - to measure the timing, ask your friends for help :-)

- and next week, I'll show you the analysis & communicate the result.

How to Run a Usability Study?

Evaluating Usability

- run a *usability study* to judge how an interface facilitates tasks with respect to the aspects of usability
  - speed, efficiency, learnability, memorability, and user preferences

Testing Usability of Security

- security is rarely the task users set out to accomplish
- good security is a seamless part of the task

Usability Study Process

- define tasks (and their importance)
- developing questionnaires

Selecting Tasks

- what are the most important things a user would do with this interface?
- present it as a task, not a question
  - good: create an itinerary from Rafsanjan to Tehran, departing October, 8th & returning October, 15th.
  - bad: how many flights are available from Rafsanjan to Tehran, departing on October, 8th & arriving on October, 15th.
  - users come to plan itineraries, not to count them.

Selecting Tasks (cont’d)

- be specific
  - good: find the calories, vitamins, and minerals in 1 mL of apple juice.
  - bad: find nutrition information.
  - users shouldn’t have to be creative to figure out what you want them to do.
- don’t give instructions
  - good: using Google map, find a street view of the city hall of Kerman.
  - bad: go to maps.google.com and type “city hall of Kerman” in the search box. Then, click on “search maps”. Using the zooming toolbox on the left, click on the person to see the street view, if it is available.
  - You aren’t testing anything if you give step by step instructions.

Selecting Tasks (cont’d)

- don’t be vague or provide tiny insignificant tasks
  - good: using Google map, find a close up view that just shows the block of the Kerman’s city hall.
  - bad: zoom in on a Google map.
  - users don’t come up to the site to zoom. Zooming is something that needs to be done as part of a real task.

Selecting Tasks (cont'd)

- choose representative tasks that reflect the most important things a user would do with the interface.
  - good: for Google, tasks could include a web search, a map search with directions, changing the language, conducting an advanced search, etc.
  - bad: do 5 basic web searches for different things.
  - repeated tasks do not provide new insights.

Security Tasks

- security is almost never a task!
- good tasks for a banking web site
  - check account balance
  - make a transfer
- bad tasks for a banking web site
  - login to your account

Pre-Test Questionnaires

- learn any relevant background about the subjects
    - age, gender, education level, experience with this kind of websites, experience with this site in particular, etc.
    - perhaps more specific questions based on the site, e.g. color blindness, if the user has children, etc.

Post-Test Questionnaires

- have users provide feedback on the interface
    - Overall, I found this interface/website
        - (difficult) 1 2 3 4 5 (easy)
    - Finding directions on a map was
        - (difficult) 1 2 3 4 5   6 7 8 9 10 (easy)
- can rate multiple features for each question

Evaluation

- users are given a list of tasks & asked to perform each task
- interaction with the user is governed by different observation protocols
    - silent observer
    - think aloud
    - constructive interaction

Interview

- ask users to give you feedback
- easier for the user than writing it down
- they will tell you things that you never thought to ask

Reporting

- after the evaluation, report your results
- summarize the experiences of the users
- emphasize your insights with specific examples or quotes
- offer suggestions for improvement for tasks that were difficult to perform

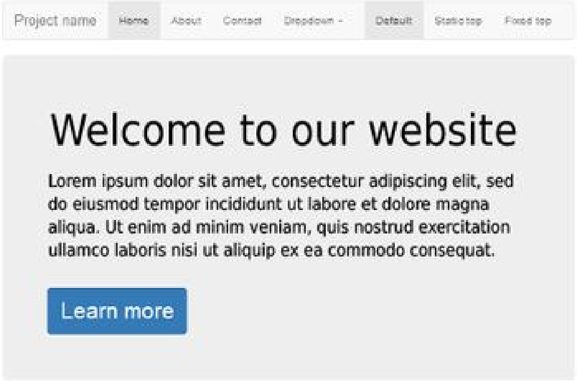
Lessons

- what parts of an application are easy and hard to use
- how usable is the site for each task
- what improvements can be made to improve the usability
- for security, can you make it more seamless?

Assignment

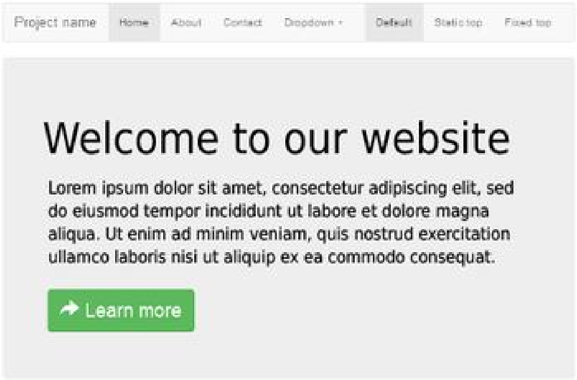
- Design a controlled experiment on the interface you have designed for SSL warnings.
- Evaluate the design of security elements of the first assignment.

A/B Testing



Welcome to our website

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.



Welcome to our website

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

Click rate: 52 %

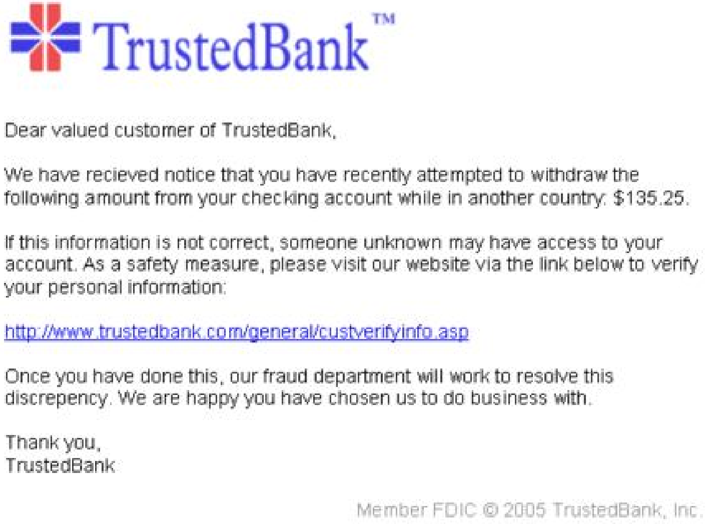
72 %

Case Study: Phishing Warnings

- it is based on the following paper
  - S. Egelman et. al., *“You've been warned: an empirical study of the effectiveness of web browser phishing warnings,”* in ACM SIGCHI Conference on Human Factors in Computing Systems, 2008, pp. 1065-1074.

What's Phishing?

- Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.



TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

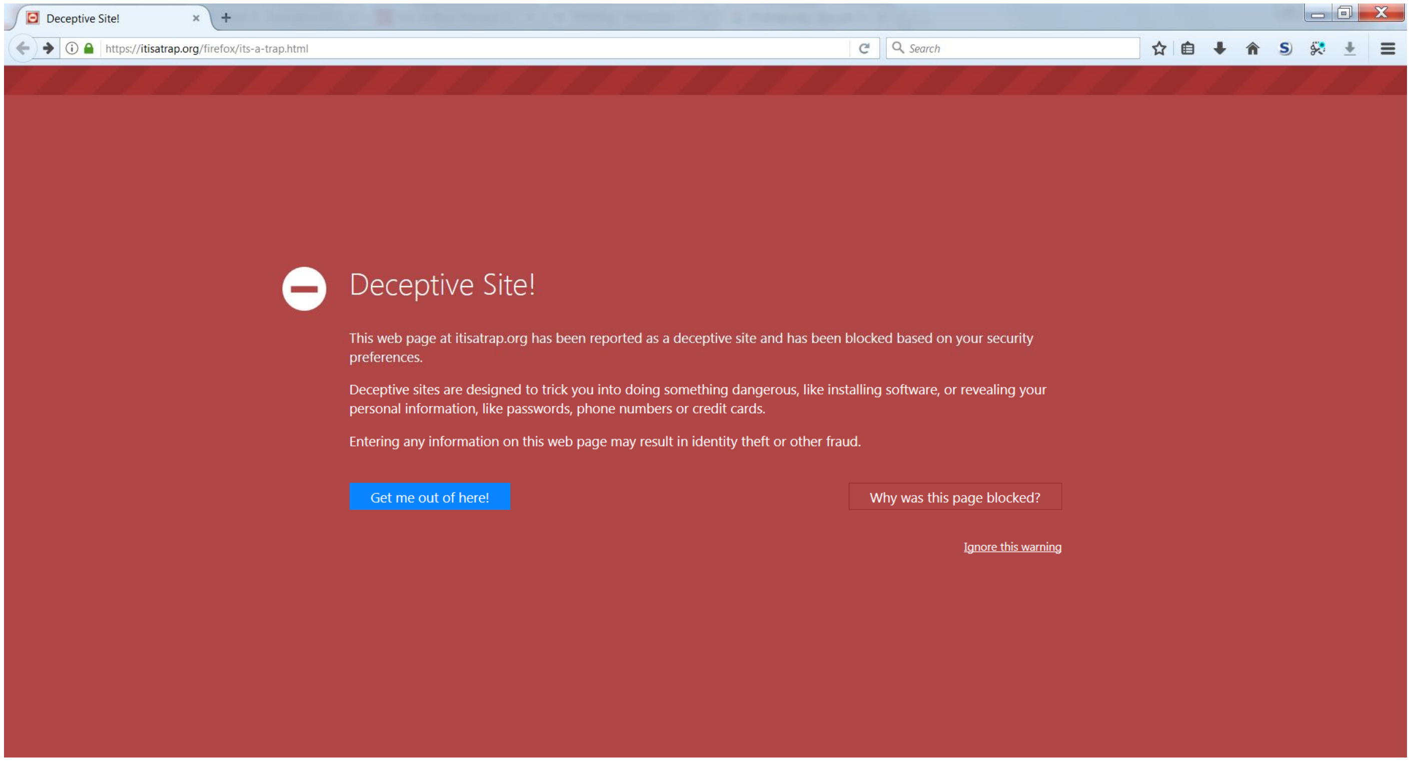
http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

https://itisatrap.org/firefox/its-a-trap.html



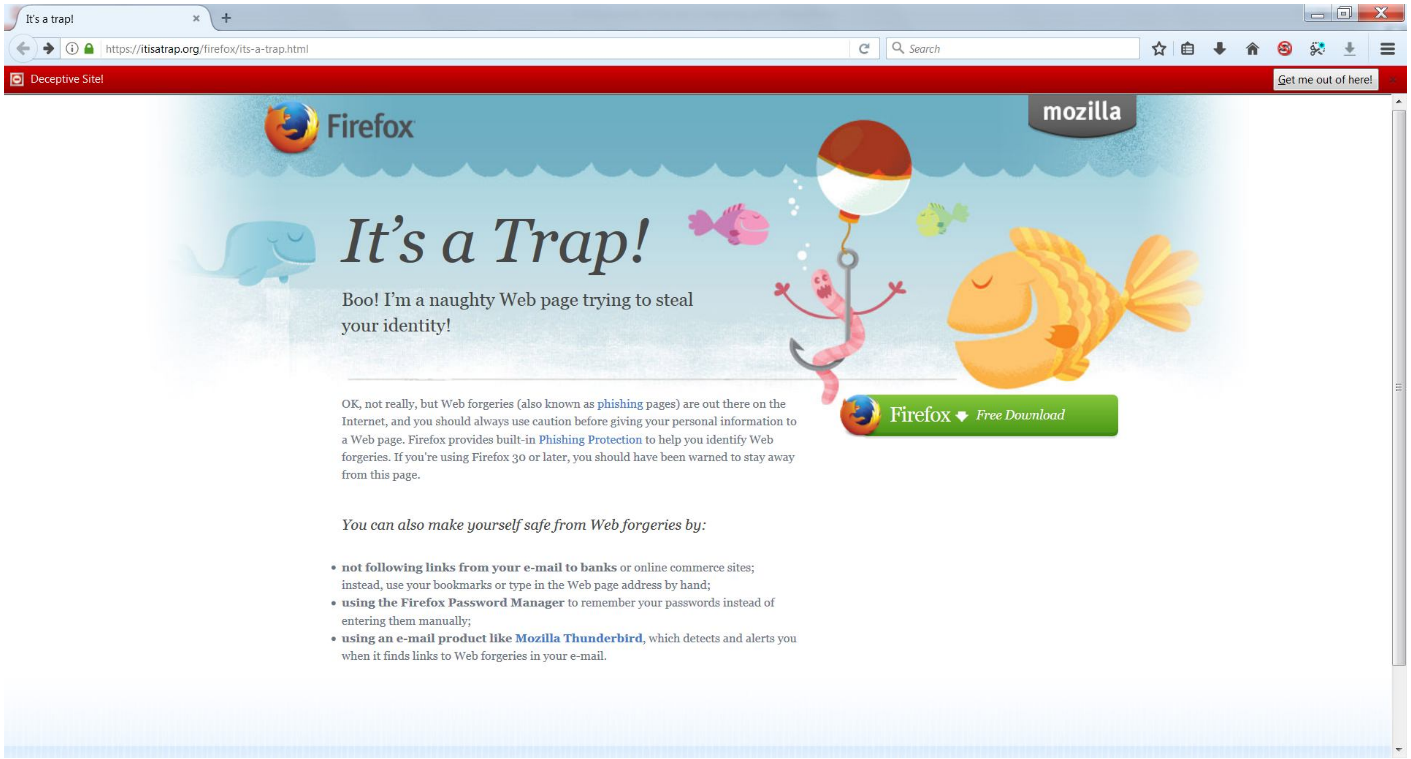
Deceptive Site!

This web page at itisatrap.org has been reported as a deceptive site and has been blocked based on your security preferences.

Deceptive sites are designed to trick you into doing something dangerous, like installing software, or revealing your personal information, like passwords, phone numbers or credit cards.

Entering any information on this web page may result in identity theft or other fraud.

https://itisatrap.org/firefox/its-a-trap.html



It's a Trap!

Boo! I'm a naughty Web page trying to steal your identity!

OK, not really, but Web forgeries (also known as phishing pages) are out there on the Internet, and you should always use caution before giving your personal information to a Web page. Firefox provides built-in Phishing Protection to help you identify Web forgeries. If you're using Firefox 30 or later, you should have been warned to stay away from this page.

You can also make yourself safe from Web forgeries by:

- **not following links from your e-mail to banks** or online commerce sites; instead, use your bookmarks or type in the Web page address by hand;
- **using the Firefox Password Manager** to remember your passwords instead of entering them manually;
- **using an e-mail product like Mozilla Thunderbird**, which detects and alerts you when it finds links to Web forgeries in your e-mail.

Case Study: Phishing Warnings

- it is based on the following paper
    - S. Egelman et. al., *“You've been warned: an empirical study of the effectiveness of web browser phishing warnings,”* in ACM SIGCHI Conference on Human Factors in Computing Systems, 2008, pp. 1065-1074.

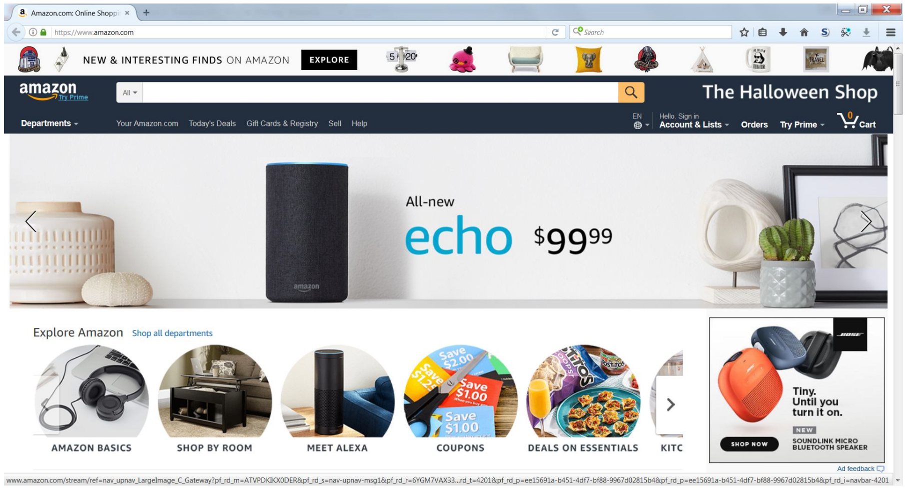
Measures of Usability

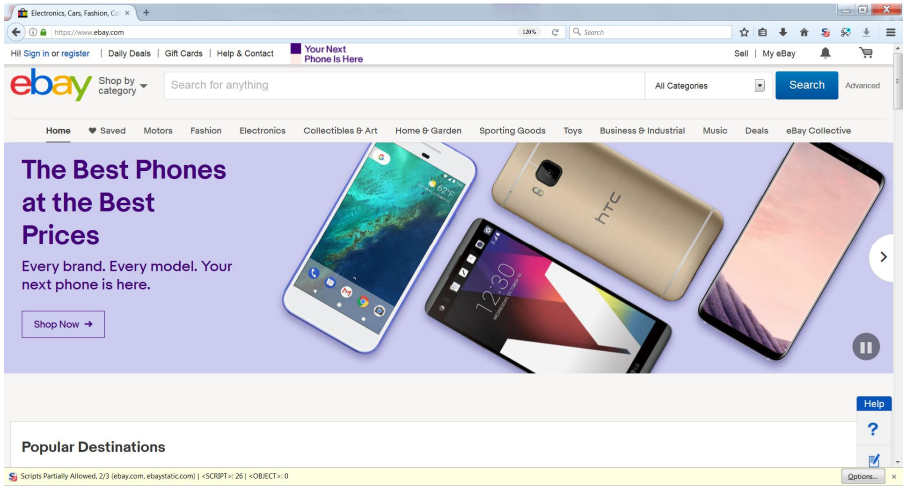
- Speed
- Efficiency
- Learnability
- Memorability
- User prefrences

Measures of Usability

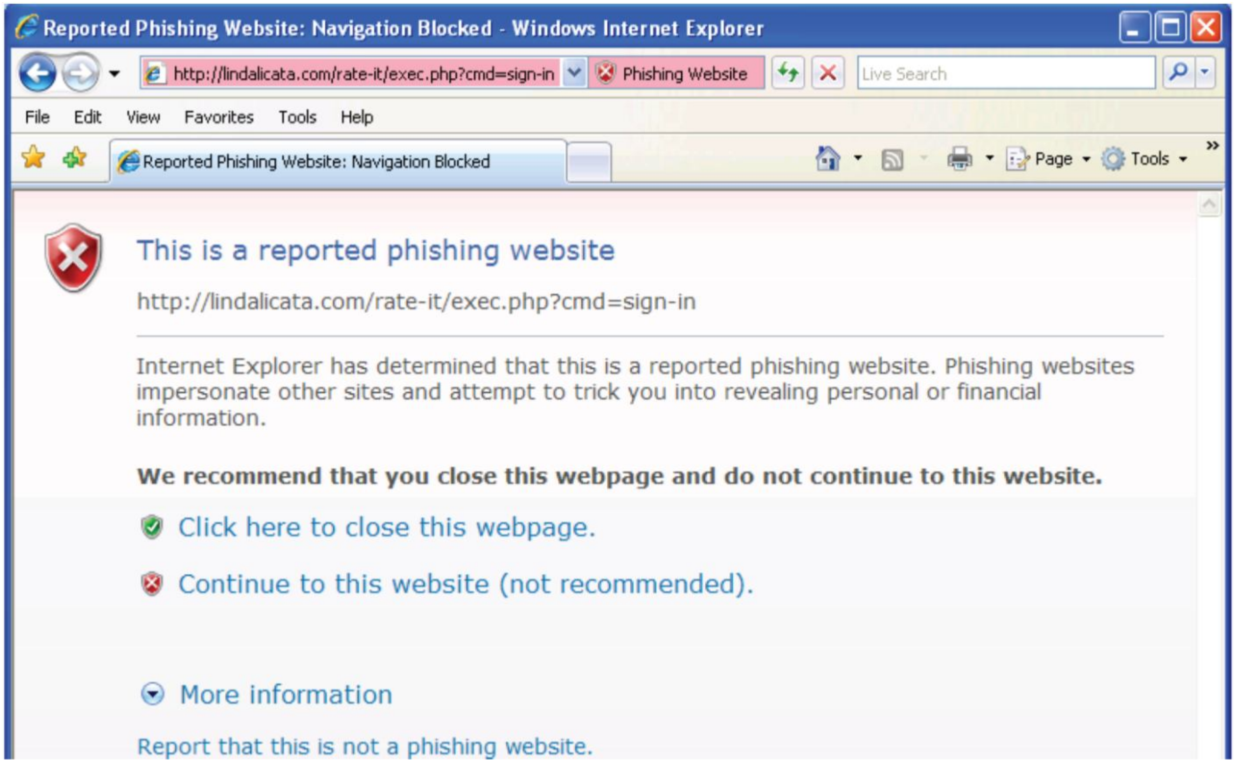
- Speed
- Efficiency
- Learnability
- Memorability
- User prefrences

Two Phishings





IE Active Phishing Warning



Reported Phishing Website: Navigation Blocked - Windows Internet Explorer
http://lindalicata.com/rate-it/exec.php?cmd=sign-in
Phishing Website
Live Search
File
Edit
View
Favorites
Tools
Help
Reported Phishing Website: Navigation Blocked
Page
Tools

This is a reported phishing website

http://lindalicata.com/rate-it/exec.php?cmd=sign-in

Internet Explorer has determined that this is a reported phishing website. Phishing websites impersonate other sites and attempt to trick you into revealing personal or financial information.

We recommend that you close this webpage and do not continue to this website.

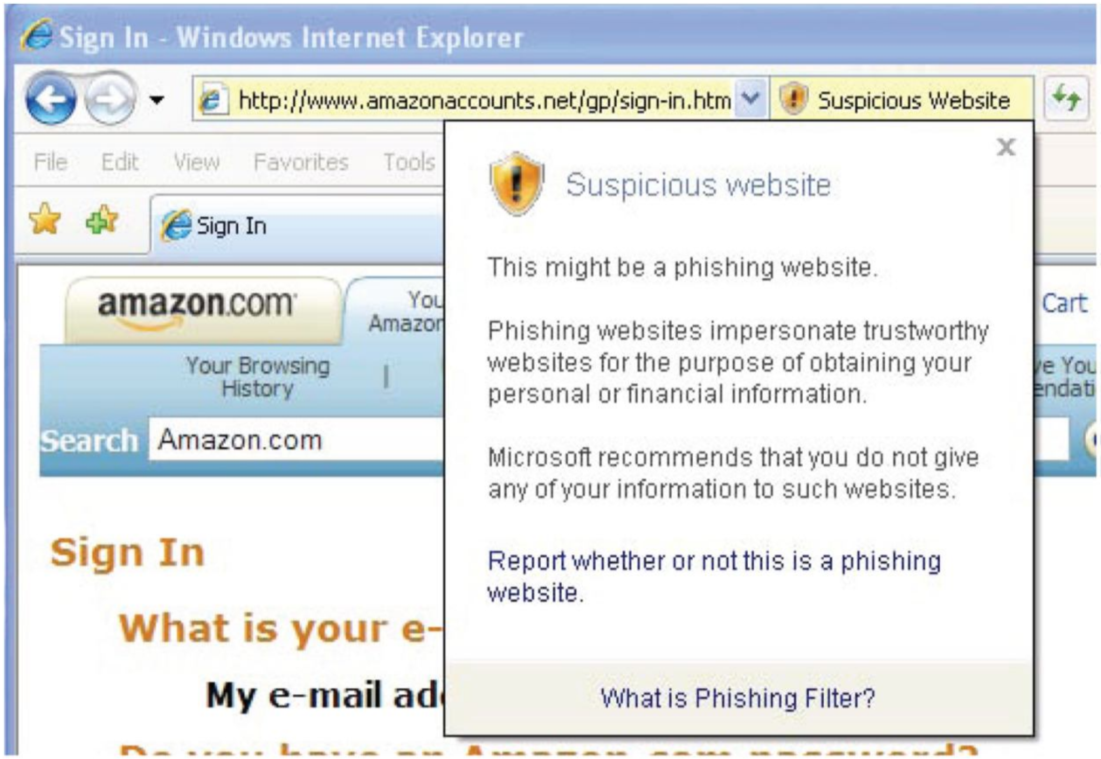
Click here to close this webpage.

Continue to this website (not recommended).

More information

Report that this is not a phishing website.

IE Passive Phishing Warning



Suspicious website

This might be a phishing website.

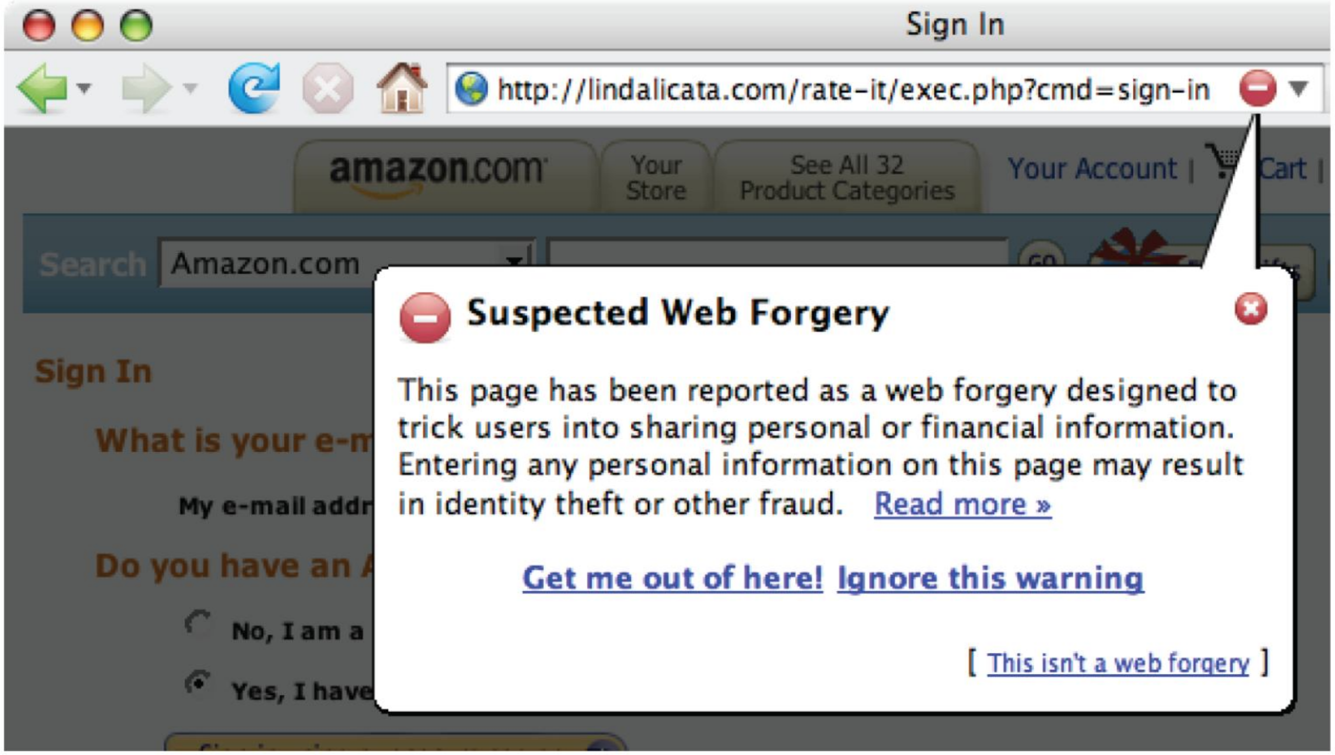
Phishing websites impersonate trustworthy websites for the purpose of obtaining your personal or financial information.

Microsoft recommends that you do not give any of your information to such websites.

Report whether or not this is a phishing website.

What is Phishing Filter?

FF2 Active Phishing Warning



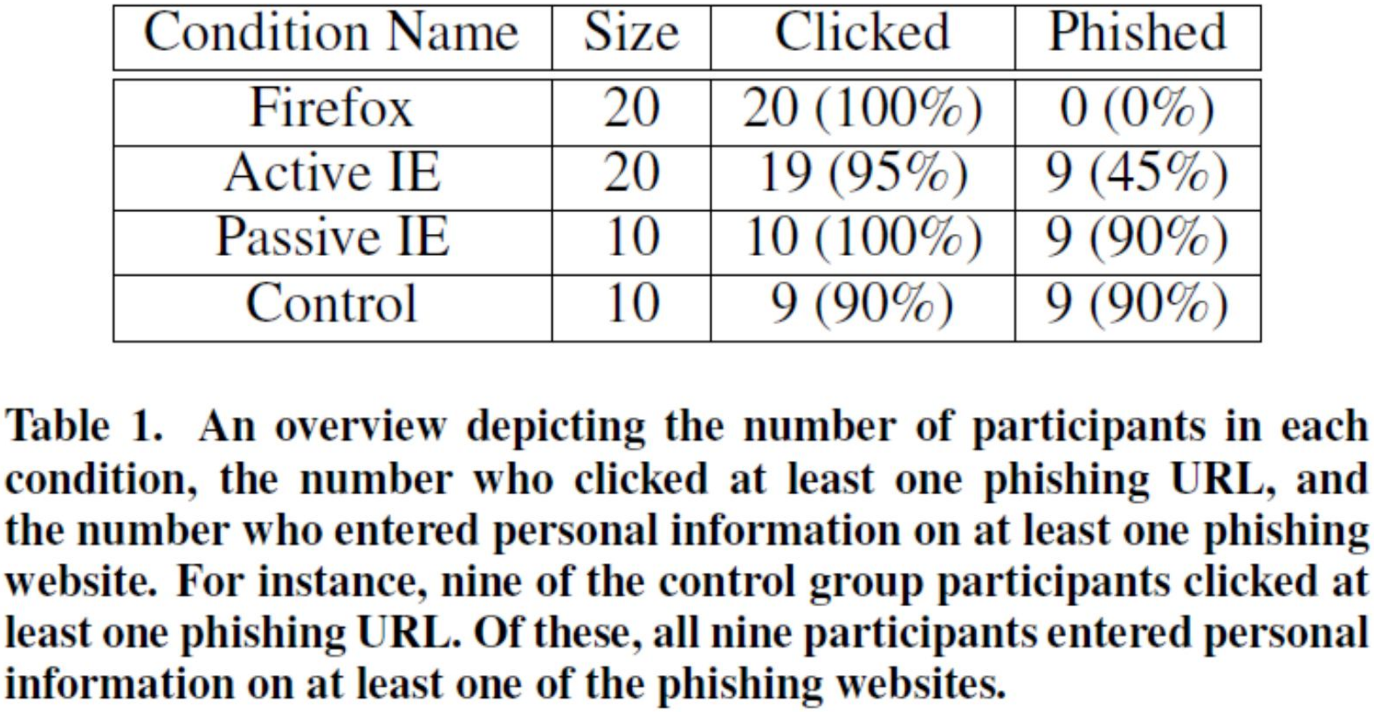
Suspected Web Forgery

This page has been reported as a web forgery designed to trick users into sharing personal or financial information. Entering any personal information on this page may result in identity theft or other fraud. Read more »

Get me out of here! Ignore this warning

[This isn't a web forgery]

and the results …

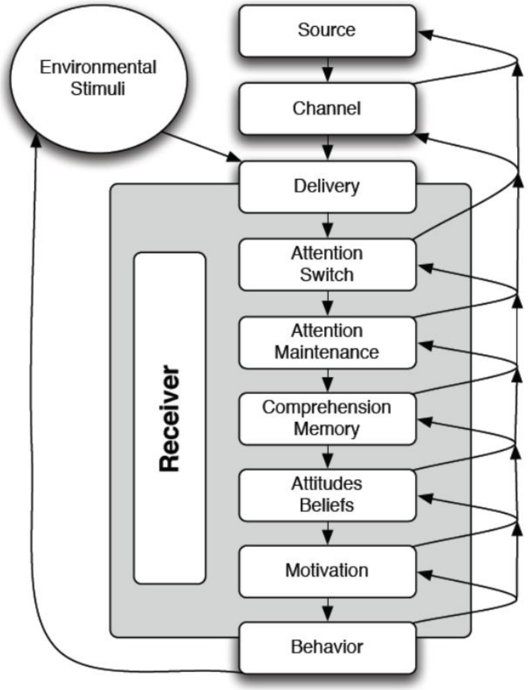


Condition Name	Size	Clicked	Phished
Firefox	20	20 (100%)	0 (0%)
Active IE	20	19 (95%)	9 (45%)
Passive IE	10	10 (100%)	9 (90%)
Control	10	9 (90%)	9 (90%)

Table 1. An overview depicting the number of participants in each condition, the number who clicked at least one phishing URL, and the number who entered personal information on at least one phishing website. For instance, nine of the control group participants clicked at least one phishing URL. Of these, all nine participants entered personal information on at least one of the phishing websites.

Mental Models: C-HIP (Communication-Human Information Processing)

- attention switch & maintenance – do users notice the indicators?
- comprehension/memory – do users know what the indicators mean?
- comprehension/memory – do users know what they are supposed to do when they see the indicators?
- attitudes/beliefs – do they believe the indicators?
- motivation – are they motivated to take the recommended action?
- behavior – will they actually perform those actions?
- environmental stimuli – how do the indicators interact with other indicators & other stimuli?



Conclusions

- the interface can have measurable impacts on the usability of security features
- better interfaces = more secure behavior
- mental models
    - active warnings capture & hold more attention than passive ones, and yield better results

Usable Security Guidelines

Two Main Strategies for Building Usable Secure Systems

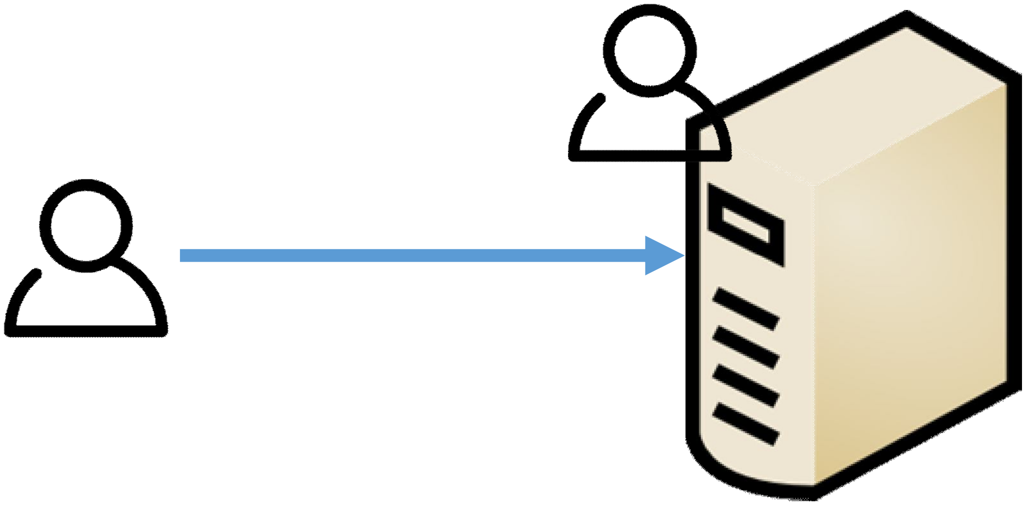
- security designation
- user-assigned identifiers

Some Background

- secure interaction design
  - deals with how to design a system which is both secure & usable
- mental models
- sources of conflict between usability & security

Permission vs. Authority

- permission
  - settings within a system that say who can access a file
- authority
  - who has the power to access something regardless of the permissions



Security & Authority

Authority Granting Guidelines

1- Match the Easiest Way to Do a Task with the Least Granting of Authority

- What are typical user tasks?
- What is the easiest way for the user to accomplish each task?
- What authority is granted to software & other people when the user takes the easiest route to complete the task?
- How can the safest ways of accomplishing the task be made easier & vice verse?

2- Grant Authority to Others in Accordance with User Actions Indicating Consent.

- When does the system give access to the user's resources?
- What user action grants that access?
- Does the user understand that action grants access?

3- Offer the User Ways to Reduce Others' Authority to Access the User's Resources

- What kinds of access does the user grant to software and other users?
- Which types of access can be revoked?
- How can the interface help the user find & revoke access?

Summary

- follow the principle of least privilege
- make the easiest way to complete a task the most secure
- make sure the user consents to the access they allow
- make it easy to reduce others' access

Authorization & Communication Guidelines

1- Users Should Know What Authority Others' Have

- What kinds of authority can software & other users hold?
- What kinds of authority impact user decisions with security consequences?
- How can the interface provide timely access to information about these authorities?

2- Users Should Know What Authority They Themselves Have

- What kinds of authority does the user hold?
- How does the user know they have that authority?
- What might the user decide based on their expectation of authority?

3- Make Sure Users Trust the Software Acting on Their Behalf

- What agents manipulate authority on the user's behalf?
- How can users be sure they are communicating with the intended agent?
- How might the agent be impersonated?
- How might the user's communication with the agent be corrupted/intercepted?

Conclusions

- Make sure that users know what authority they have granted & what that means for security decisions
- Make sure users know what authority they hold
- Create interfaces that make it clear what agent (software) the user is interacting with & providing information to

Interface Guidelines for Usable Security

1- Enable the User to Express Safe Security Policies that Fit the User's Task

- What are some examples of security policies that users might want enforced for typical tasks?
- How can the user express these policies?
- How can the expression of policy be brought closer to the task?

2- Draw Distinctions among Objects & Actions along Boundaries Relevant to the Task

- At what level of detail does the interface allow objects & actions to be separately manipulated?
- What distinctions between affected objects & unaffected objects does the user care about?

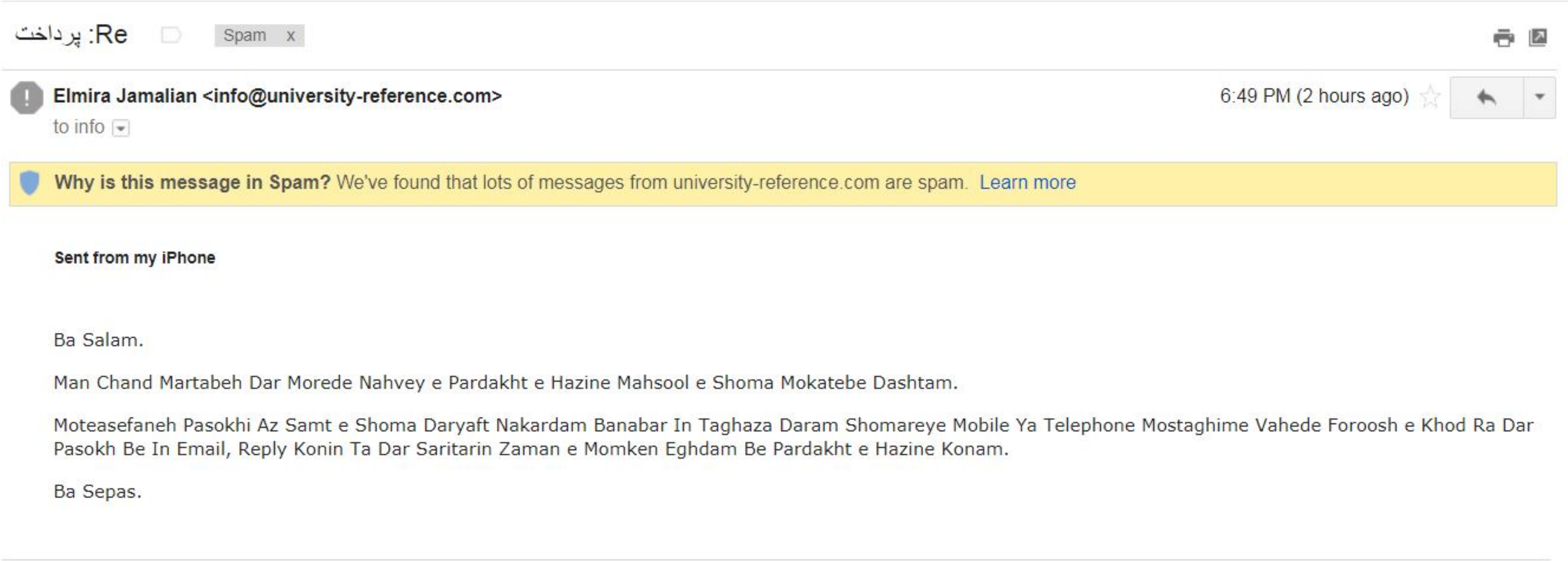
3- Present Objects & Actions using Distinguishable, Truthful Appearances

- How does the user identify & distinguish different objects & actions?
- In what ways can the means of identification be controlled by other parties?
- What aspects of an object's appearance are under system control?
- How can those aspects be chosen to best prevent deception?

Conclusions

- Make it easy for users to control access to their resources
- Show a level of detail that's informative & useful to the user, and no more than that
- Make it easy to see the differences between objects & actions that could be confused

Case Study: Phishing Warnings



Re: پرداخت

Elmira Jamalian <info@university-reference.com>

to info

6:49 PM (2 hours ago)

Why is this message in Spam? We've found that lots of messages from university-reference.com are spam. Learn more

Sent from my iPhone

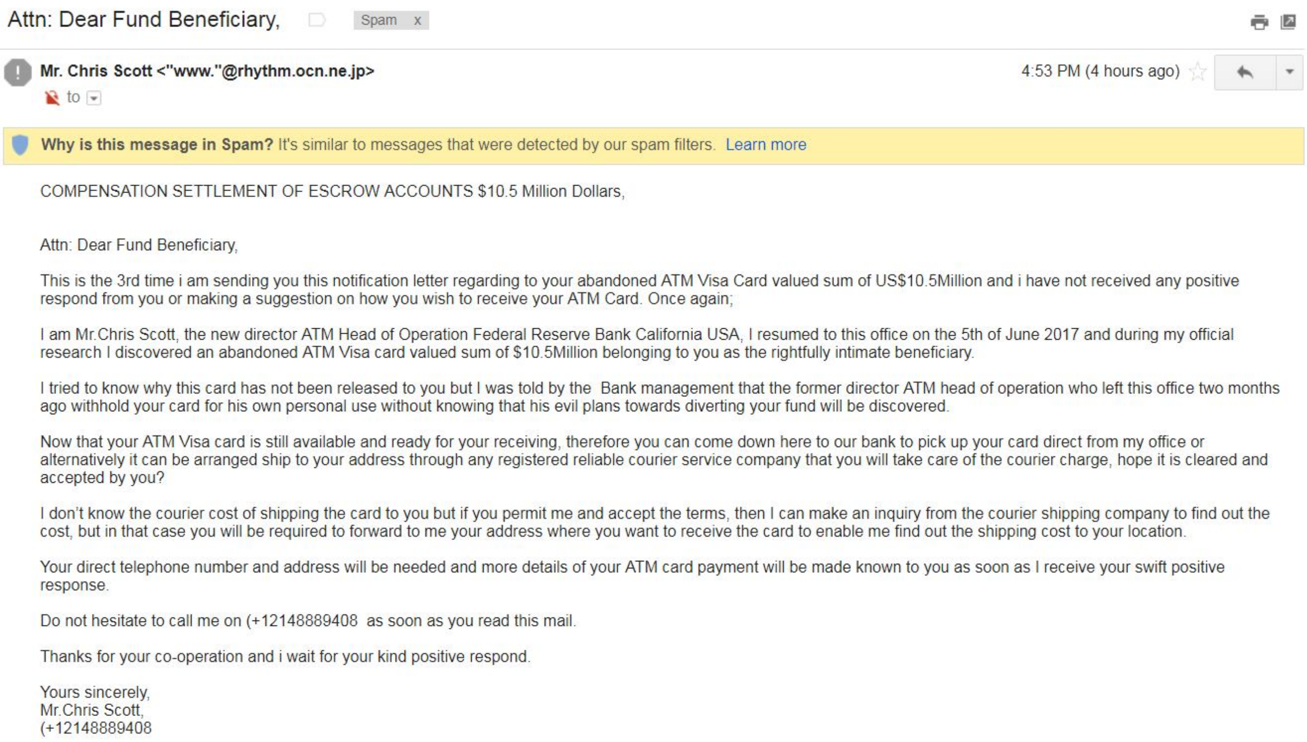
Ba Salam.

Man Chand Martabeh Dar Morede Nahvey e Pardakht e Hazine Mahsool e Shoma Mokatebe Dashtam.

Moteasefaneh Pasokhi Az Samt e Shoma Daryaft Nakardam Banabar In Taghaza Daram Shomareye Mobile Ya Telephone Mostaghime Vahede Foroosh e Khod Ra Dar Pasokh Be In Email, Reply Konin Ta Dar Saritarin Zaman e Momken Eghdam Be Pardakht e Hazine Konam.

Ba Sepas.

Case Study: Phishing Warnings



Attn: Dear Fund Beneficiary,

Mr. Chris Scott <"www."@rhythm.ocn.ne.jp>
to

4:53 PM (4 hours ago)

Why is this message in Spam? It's similar to messages that were detected by our spam filters. Learn more

COMPENSATION SETTLEMENT OF ESCROW ACCOUNTS $10.5 Million Dollars,

Attn: Dear Fund Beneficiary,

This is the 3rd time i am sending you this notification letter regarding to your abandoned ATM Visa Card valued sum of US$10.5Million and i have not received any positive respond from you or making a suggestion on how you wish to receive your ATM Card. Once again;

I am Mr.Chris Scott, the new director ATM Head of Operation Federal Reserve Bank California USA, I resumed to this office on the 5th of June 2017 and during my official research I discovered an abandoned ATM Visa card valued sum of $10.5Million belonging to you as the rightfully intimate beneficiary.

I tried to know why this card has not been released to you but I was told by the Bank management that the former director ATM head of operation who left this office two months ago withhold your card for his own personal use without knowing that his evil plans towards diverting your fund will be discovered.

Now that your ATM Visa card is still available and ready for your receiving, therefore you can come down here to our bank to pick up your card direct from my office or alternatively it can be arranged ship to your address through any registered reliable courier service company that you will take care of the courier charge, hope it is cleared and accepted by you?

I don't know the courier cost of shipping the card to you but if you permit me and accept the terms, then I can make an inquiry from the courier shipping company to find out the cost, but in that case you will be required to forward to me your address where you want to receive the card to enable me find out the shipping cost to your location.

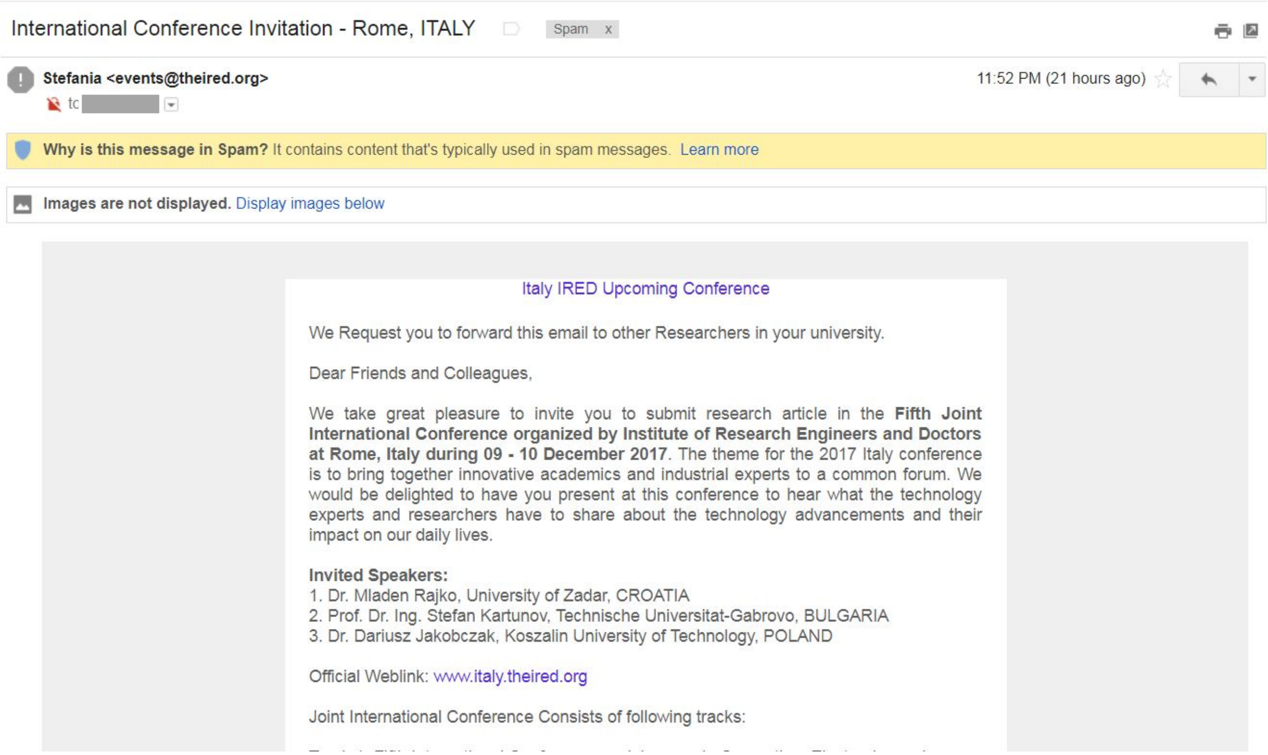
Your direct telephone number and address will be needed and more details of your ATM card payment will be made known to you as soon as I receive your swift positive response.

Do not hesitate to call me on (+12148889408 as soon as you read this mail.

Thanks for your co-operation and i wait for your kind positive respond.

Yours sincerely,
Mr.Chris Scott,
(+12148889408

Case Study: Phishing Warnings



International Conference Invitation - Rome, ITALY

Stefania <events@theired.org>

tc [redacted]

11:52 PM (21 hours ago)

Why is this message in Spam? It contains content that's typically used in spam messages. Learn more

Images are not displayed. Display images below

Italy IRED Upcoming Conference

We Request you to forward this email to other Researchers in your university.

Dear Friends and Colleagues,

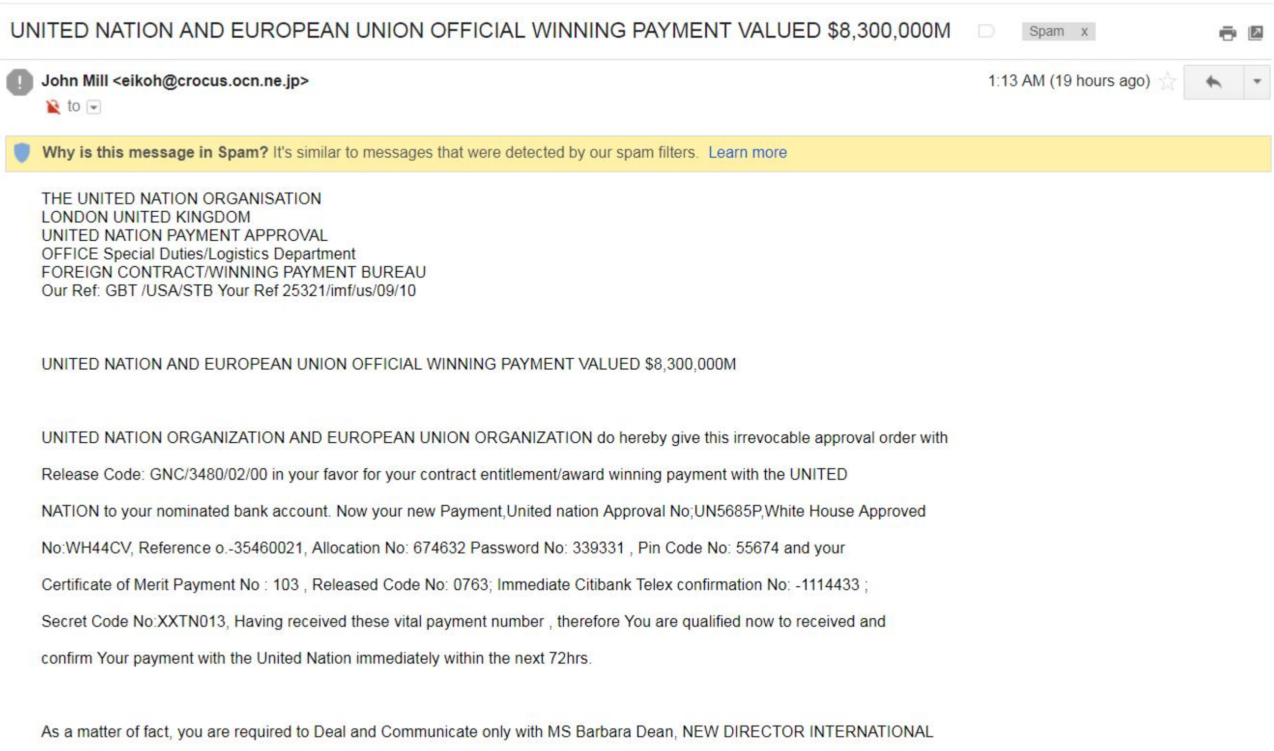
We take great pleasure to invite you to submit research article in the **Fifth Joint International Conference organized by Institute of Research Engineers and Doctors at Rome, Italy during 09 - 10 December 2017**. The theme for the 2017 Italy conference is to bring together innovative academics and industrial experts to a common forum. We would be delighted to have you present at this conference to hear what the technology experts and researchers have to share about the technology advancements and their impact on our daily lives.

Invited Speakers:
1. Dr. Mladen Rajko, University of Zadar, CROATIA
2. Prof. Dr. Ing. Stefan Kartunov, Technische Universitat-Gabrovo, BULGARIA
3. Dr. Dariusz Jakobczak, Koszalin University of Technology, POLAND

Official Weblink: www.italy.theired.org

Joint International Conference Consists of following tracks:

Case Study: Phishing Warnings



UNITED NATION AND EUROPEAN UNION OFFICIAL WINNING PAYMENT VALUED $8,300,000M

John Mill <eikoh@crocus.ocn.ne.jp>

1:13 AM (19 hours ago)

Why is this message in Spam? It's similar to messages that were detected by our spam filters. Learn more

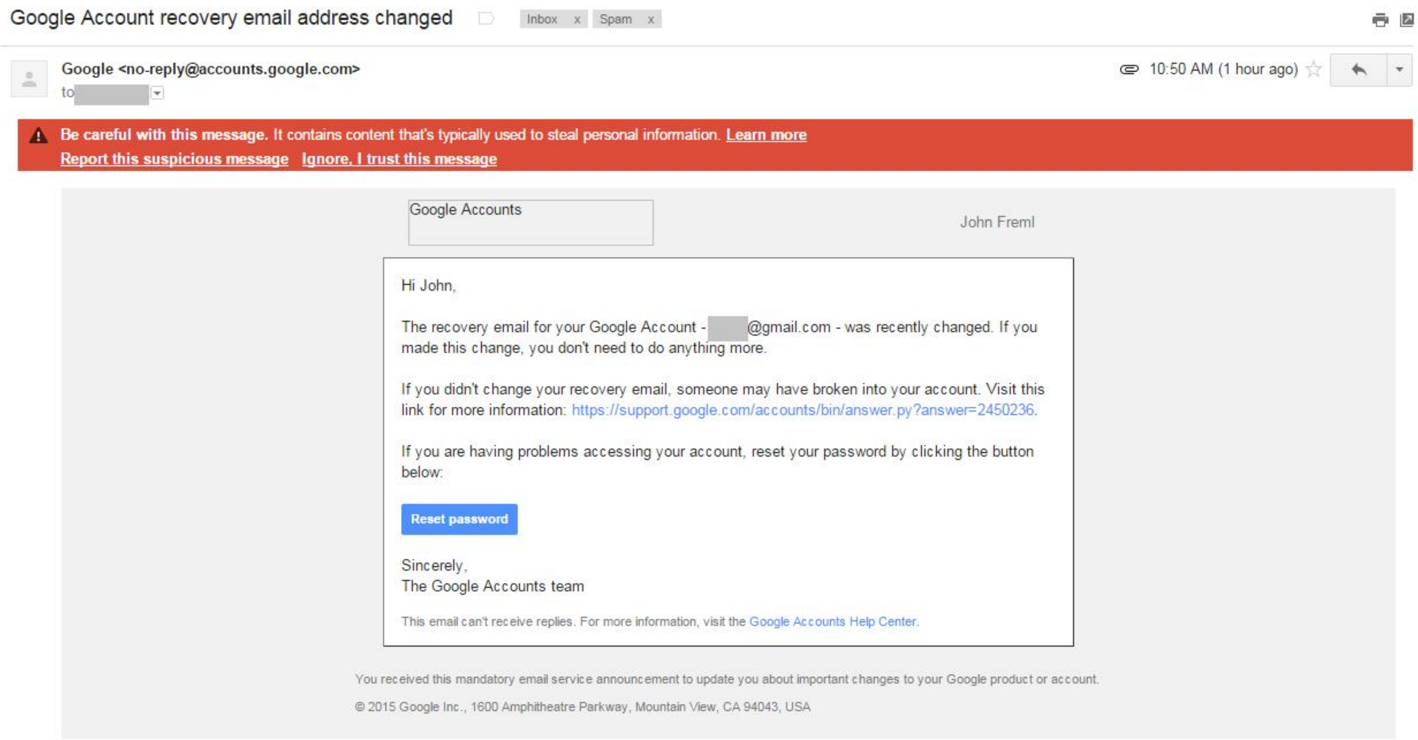
THE UNITED NATION ORGANISATION
LONDON UNITED KINGDOM
UNITED NATION PAYMENT APPROVAL
OFFICE Special Duties/Logistics Department
FOREIGN CONTRACT/WINNING PAYMENT BUREAU
Our Ref: GBT /USA/STB Your Ref 25321/imf/us/09/10

UNITED NATION AND EUROPEAN UNION OFFICIAL WINNING PAYMENT VALUED $8,300,000M

UNITED NATION ORGANIZATION AND EUROPEAN UNION ORGANIZATION do hereby give this irrevocable approval order with Release Code: GNC/3480/02/00 in your favor for your contract entitlement/award winning payment with the UNITED NATION to your nominated bank account. Now your new Payment,United nation Approval No;UN5685P,White House Approved No:WH44CV, Reference o.-35460021, Allocation No: 674632 Password No: 339331 , Pin Code No: 55674 and your Certificate of Merit Payment No : 103 , Released Code No: 0763; Immediate Citibank Telex confirmation No: -1114433 ; Secret Code No:XXTN013, Having received these vital payment number , therefore You are qualified now to received and confirm Your payment with the United Nation immediately within the next 72hrs.

As a matter of fact, you are required to Deal and Communicate only with MS Barbara Dean, NEW DIRECTOR INTERNATIONAL

Case Study: Phishing Warnings



Google Account recovery email address changed

Google <no-reply@accounts.google.com>
to [redacted]

10:50 AM (1 hour ago)

Be careful with this message. It contains content that's typically used to steal personal information. Learn more

Google Accounts

John Freml

Hi John,

The recovery email for your Google Account - [redacted]@gmail.com - was recently changed. If you made this change, you don't need to do anything more.

If you didn't change your recovery email, someone may have broken into your account. Visit this link for more information: https://support.google.com/accounts/bin/answer.py?answer=2450236.

If you are having problems accessing your account, reset your password by clicking the button below:

Sincerely,
The Google Accounts team

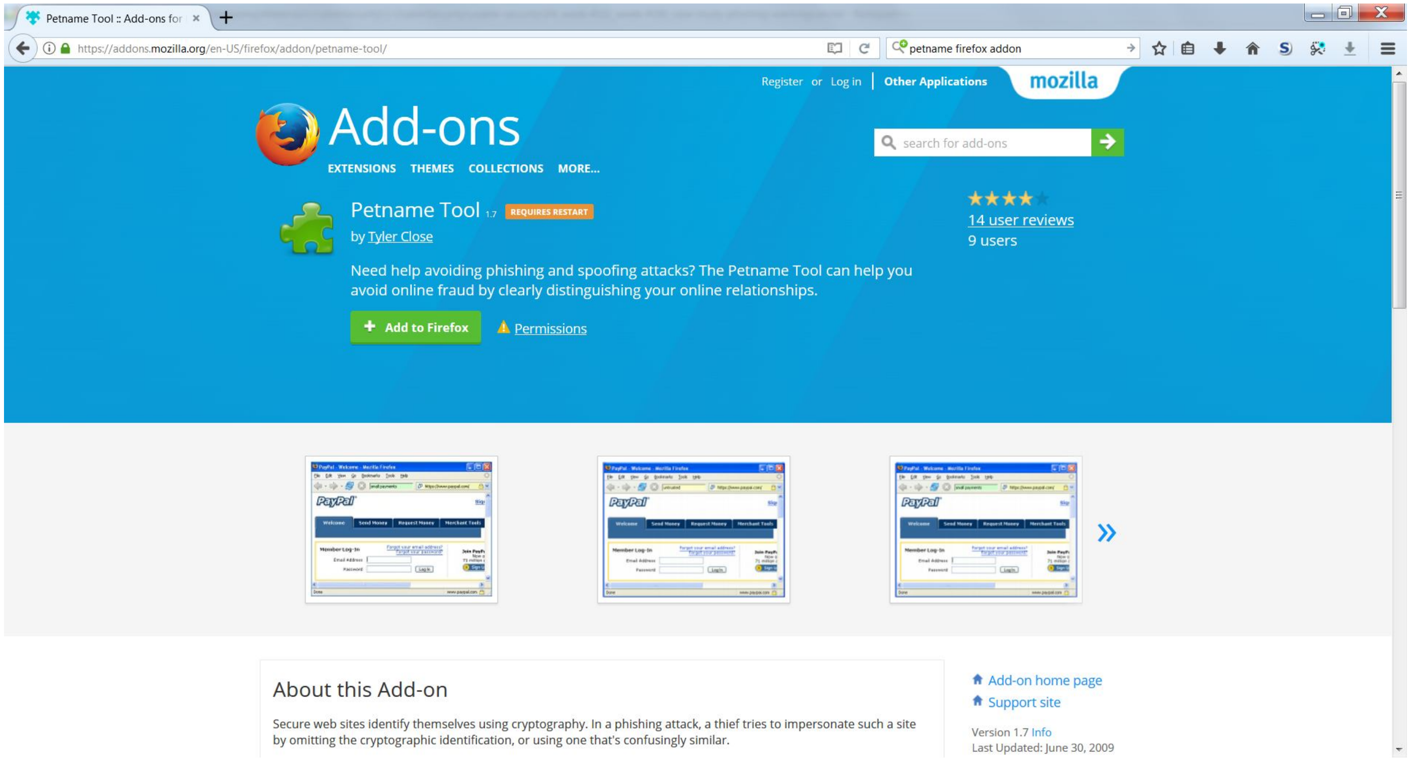
This email can't receive replies. For more information, visit the Google Accounts Help Center.

You received this mandatory email service announcement to update you about important changes to your Google product or account.

© 2015 Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

Enable the user to express safe security policies that fit the user's task

Petname Tool Add-on for Firefox



Petname Tool :: Add-ons for
https://addons.mozilla.org/en-US/firefox/addon/petname-tool/

Register or Log in | Other Applications

EXTENSIONS THEMES COLLECTIONS MORE...

Petname Tool 1.7 REQUIRES RESTART

by Tyler Close

★★★★ 14 user reviews 9 users

Need help avoiding phishing and spoofing attacks? The Petname Tool can help you avoid online fraud by clearly distinguishing your online relationships.

About this Add-on

Secure web sites identify themselves using cryptography. In a phishing attack, a thief tries to impersonate such a site by omitting the cryptographic identification, or using one that's confusingly similar.

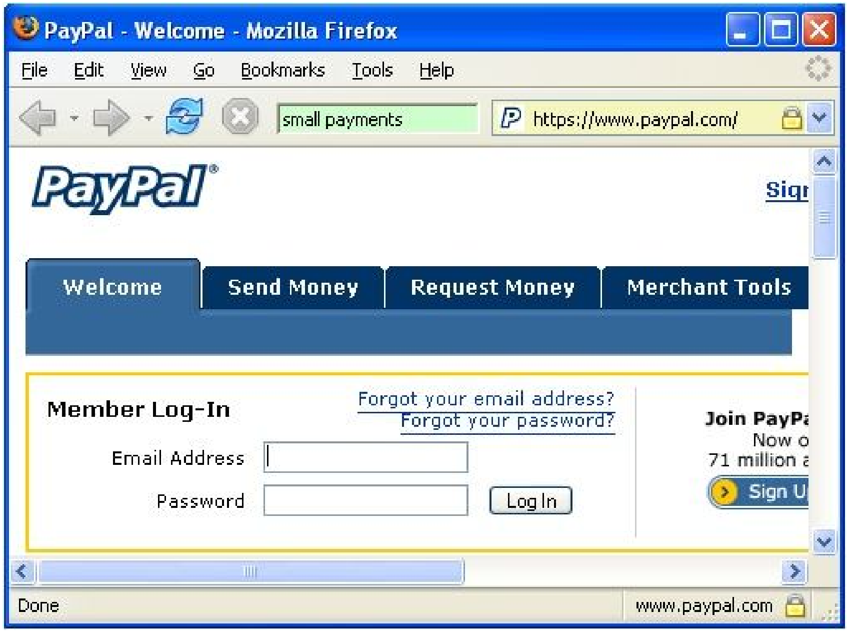
Version 1.7 Info

Last Updated: June 30, 2009

Petname Tool Add-on for Firefox (cont’d)

It is capital I …

https://paypal.com



PayPal - Welcome - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

small payments

https://www.paypal.com/

PayPal®

Sign

Welcome | Send Money | Request Money | Merchant Tools

Member Log-In

Forgot your email address?
Forgot your password?

Email Address

Password

Log In

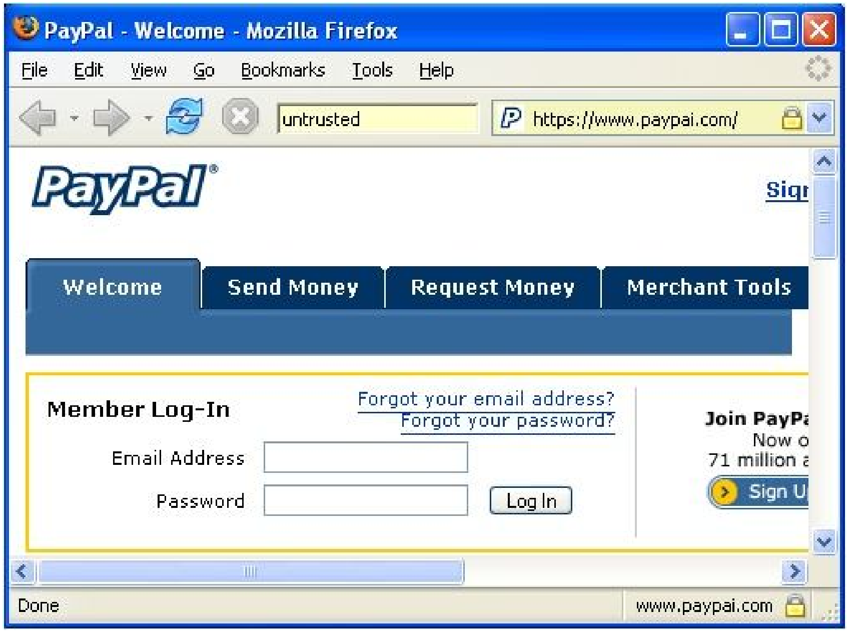
Join PayPa
Now o
71 million a

Sign U

Done

www.paypal.com

https://paypal.com



PayPal - Welcome - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

untrusted

https://www.paypai.com/

PayPal®

Sign

Welcome | Send Money | Request Money | Merchant Tools

Member Log-In

Forgot your email address?
Forgot your password?

Email Address

Password

Log In

Join PayPa
Now o
71 million a

Sign U

Done

www.paypai.com

Enable the user to express safe security policies that fit the user's task

Conclusion

- Automated security controls are good, but not the only solution
- Giving users control can be more secure
- Assist them in the process

Usable Authentication & Passwords