CompSec Seminar

-Psychology and Usability

Presented by:

Amir Shachar

Overview

How are psychology and computer systems related?

- Most of nowadays attacks target people rather than machines

- These attacks are called psychological attacks

- Understanding how people choose their passwords is very important

Psychology

- What are the reasons for psychological attacks? With time people get better at technology, yet our minds stay relatively easy to fool

- Communication over the web is not asymmetric- meaning that good use is not easier than misuse

Why psychology?

Since long ago, armies would get the info from one of the enemy soldiers directly.

How does one convince a soldier (or a person in general) to hand over valuable information?

Understanding the way the mind works helped experts convert people to their side.

Pretexting

Definition – Impersonating as someone with an authority to claim information

i.e. Calling someone asking them to report for jury duty, and ask for their SSN and DOB

Pretexting- potential harms

Pretexting is a very real threat!
2007- Scammers called customers pretending to be from the visa company, and asked for the card details in order to “cancel it”

2007- 62 out of 102 IRS employees who were told to change their password to a given value, did so

Pretexting - Protection

How to deal with it–

Train your staff:

e.g. No discussing information with friends

Let them know how important it is to be discrete :

If they know, they will understand the rules

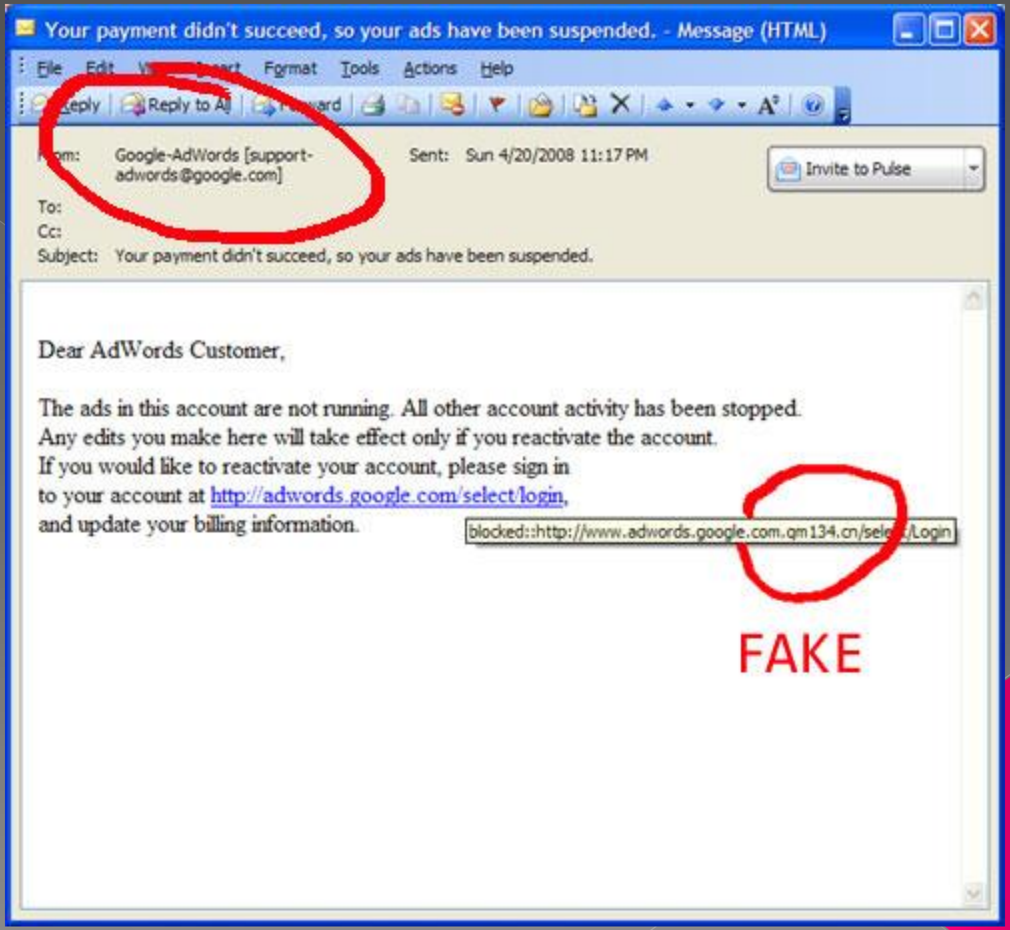
Enforce strict protocols:

No talking about sensitive material outside a secure location

Phishing

Definition: **Phishing** is the act of attempting to get sensitive information, by pretending as a trustworthy entity

Phishing is in many ways worse than pretexting, since the targets are clients/customers


Your payment didn't succeed, so your ads have been suspended. - Message (HTML)
File
Edit
Format
Tools
Actions
Help
Reply
Reply to All
Forward
Invite to Pulse

From: Google-AdWords [support-adwords@google.com]

Sent: Sun 4/20/2008 11:17 PM

To:

Cc:

Subject: Your payment didn't succeed, so your ads have been suspended.

Dear AdWords Customer,

The ads in this account are not running. All other account activity has been stopped.
Any edits you make here will take effect only if you reactivate the account.
If you would like to reactivate your account, please sign in
to your account at http://adwords.google.com/select/login,
and update your billing information.

blocked::http://www.adwords.google.com.qm134.cn/select/Login

FAKE

Phishing

- Early phishing attacks focused on banks

- Much like any other type of virtual attack, they evolved: starting at poorly built fake websites and going as far as setting a fake physical bank branch !!!

It is a part of the never ending good-guys VS. bad-guys race.

Phishing

Losses attributed to phishing were estimated to be over 200milion $ in 2006 in the US alone.

Common attacks: fake emails sent from seemingly genuine banks, social network phishing

Phishermen prefer targets who are unaware of the danger

Psychology

In the use of **CompSec**

Psychology is the study of the mind. Even though it is studied for centuries, very little is known.

What we do know mainly is how the brain reacts in different situations.

This can be taken advantage of in the hands of the bad guys.

Brain **vs** Computer

People think and store data in context. This fact can be manipulated to **trick them.**

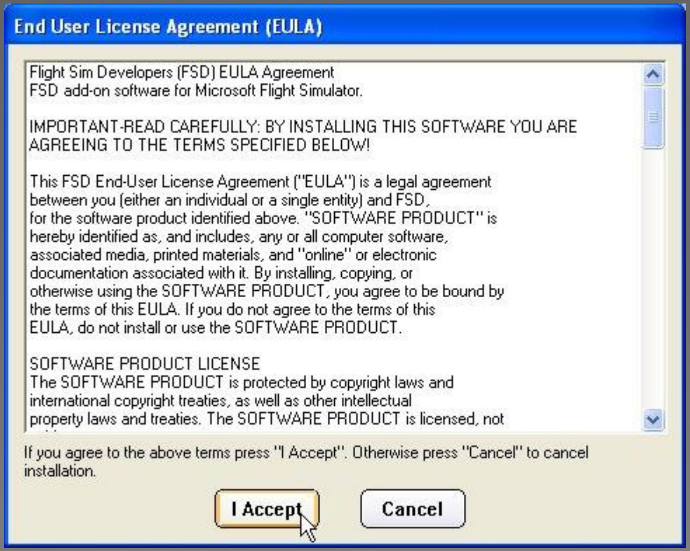
We will address 3 types of psychological errors:

- Lapses at level of skill
- Action taken by following wrong rules
- Cognitive failures – not understanding there is a problem

Brain **vs** Computer

Lapses at level of skill:

we are told that practice makes perfect, but not so in computer security.



End User License Agreement (EULA)

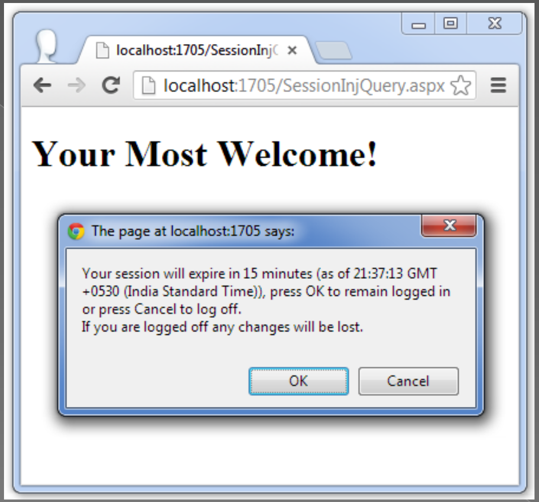
Flight Sim Developers (FSD) EULA Agreement
FSD add-on software for Microsoft Flight Simulator.

IMPORTANT-READ CAREFULLY: BY INSTALLING THIS SOFTWARE YOU ARE AGREEING TO THE TERMS SPECIFIED BELOW!

This FSD End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and FSD, for the software product identified above. "SOFTWARE PRODUCT" is hereby identified as, and includes, any or all computer software, associated media, printed materials, and "online" or electronic documentation associated with it. By installing, copying, or otherwise using the SOFTWARE PRODUCT, you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, do not install or use the SOFTWARE PRODUCT.

SOFTWARE PRODUCT LICENSE
The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The SOFTWARE PRODUCT is licensed, not

If you agree to the above terms press "I Accept". Otherwise press "Cancel" to cancel installation.



localhost:1705/SessionInj
localhost:1705/SessionInjQuery.aspx

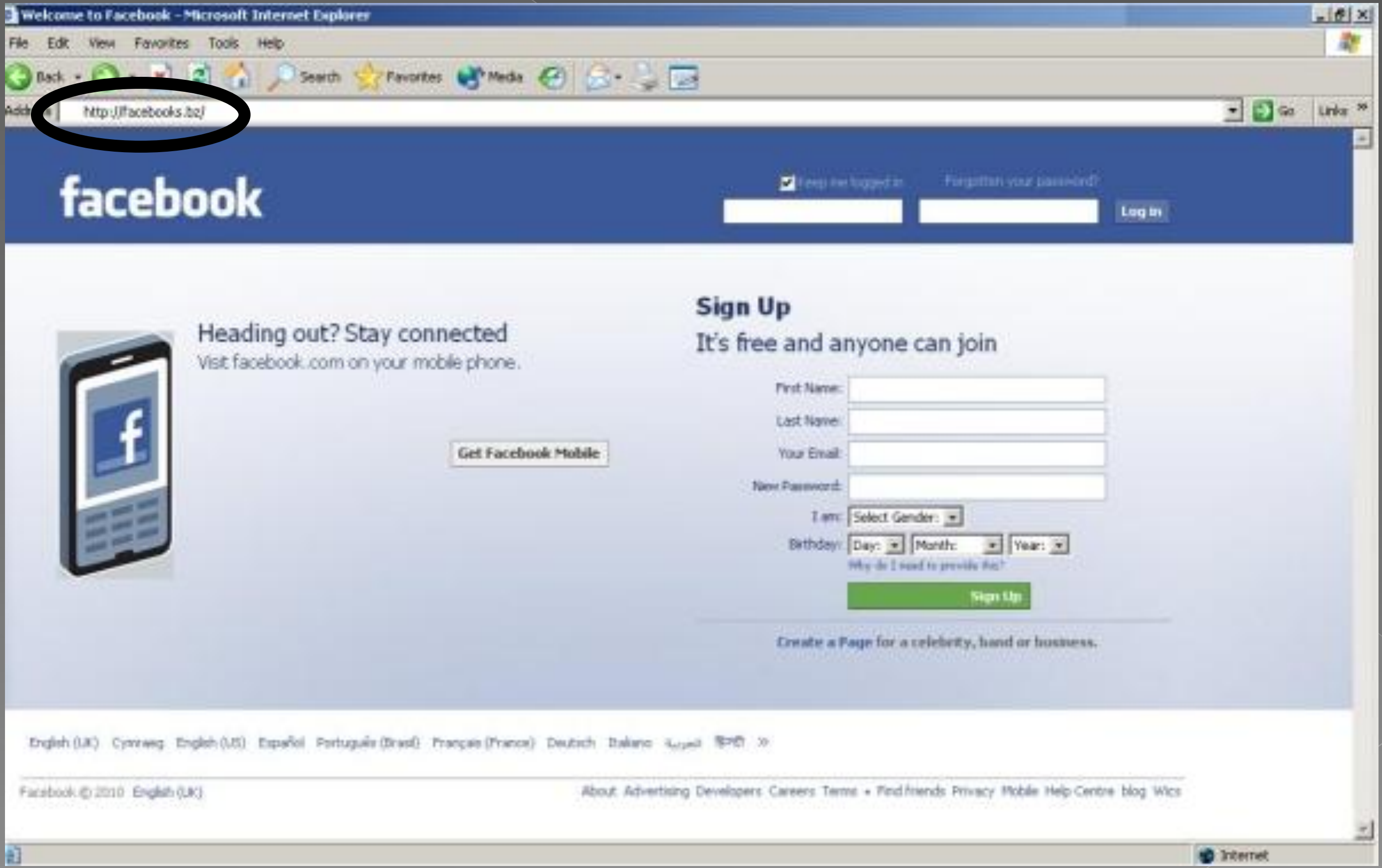
Your Most Welcome!

The page at localhost:1705 says:

Your session will expire in 15 minutes (as of 21:37:13 GMT +0530 (India Standard Time)), press OK to remain logged in or press Cancel to log off.
If you are logged off any changes will be lost.

Brain **vs** Computer

Action taken by following wrong rules:
when overloaded with data, they often forget how to think and resort to their default rule.



Welcome to Facebook - Microsoft Internet Explorer

http://facebooks.bz/

Heading out? Stay connected
Visit facebook.com on your mobile phone.

Sign Up
It's free and anyone can join

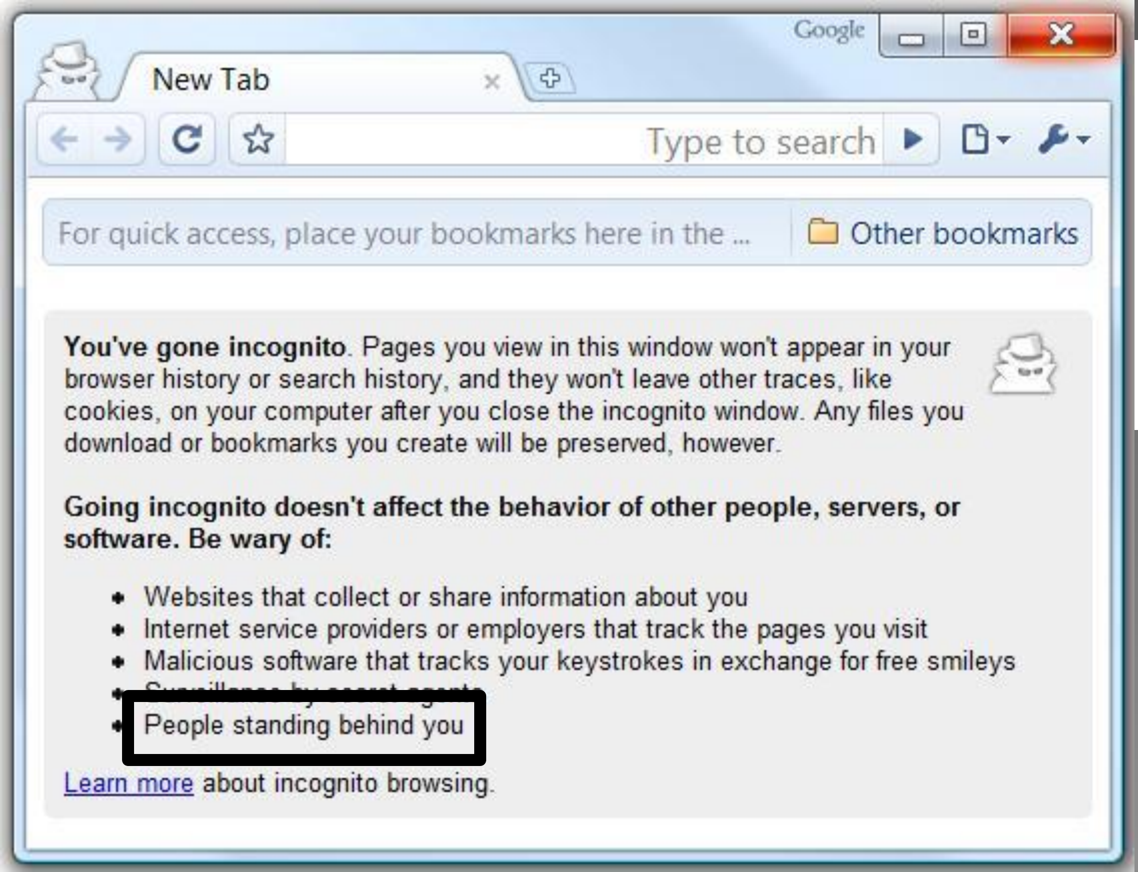
Create a Page for a celebrity, band or business.

Facebook © 2010 English (UK)

File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address
Go
Links
facebook
☑ Keep me logged in
Forgotten your password?
Log in
Get Facebook Mobile
First Name:
Last Name:
Your Email:
New Password:
I am: Select Gender:
Birthday: Day: Month: Year:
Why do I need to provide this?
Sign Up
English (UK) Cymraeg English (US) Español Português (Brasil) Français (France) Deutsch Italiano العربية हिन्दी »
About Advertising Developers Careers Terms • Find friends Privacy Mobile Help Centre blog Widgets
Internet

Brain **vs** Computer

Cognitive failures:
When people do not know they are at risk (shoulder surfing)



You've gone incognito. Pages you view in this window won't appear in your browser history or search history, and they won't leave other traces, like cookies, on your computer after you close the incognito window. Any files you download or bookmarks you create will be preserved, however.

Going incognito doesn't affect the behavior of other people, servers, or software. Be wary of:

- Websites that collect or share information about you
- Internet service providers or employers that track the pages you visit
- Malicious software that tracks your keystrokes in exchange for free smileys
- Surveillance by secret agents
- People standing behind you

Learn more about incognito browsing.

Perceptual Bias

Studies have shown that people tend to over trust in certain situations- a breach used by phishermen.

More conclusions are:

People are bad at evaluating risks

We often try to rely on familiar situations

Perceptual Bias

Heuristics lead us to the <u>misconception of risk:</u>

Safety when in control

The fear of uncertainty

Risk aversion- Settling for a 'good enough' option

Social Psychology

In 1951, a study showed that people were willing to conform no matter how ridiculous the situation was.

In the 70's an experiment showed that the role one plays in society can alter their behavior.

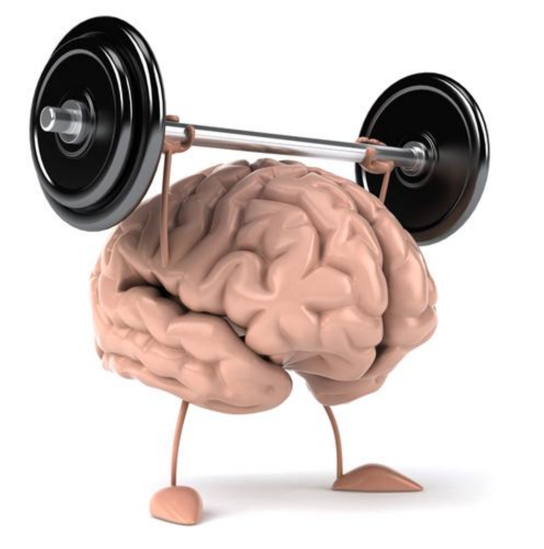
Why does this matter? Peer pressure, authority abuse -> pretexting

Brain vs. Computer

Even though the brain has it's faults, it is still a superior machine to the computer.

Humans recognize faces better, decipher speech with noise, And process images & video better than a computer.

All of the above means that it is possible to create tests to tell humans apart from computers.



Assuring identities over the web

Problem: successfully identifying users.
Solution: A mechanism for authenticating identities .

The three main mechanism types:
Something you know (passwords)

Something you have (keys, credit cards, etc.)

Who you are (fingerprints, voice recognition…)

Passwords

Passwords are absolutely not fit for humans… But they are the cheapest option.

Best use would include a password and a physical or biometric identifier.

Passwords

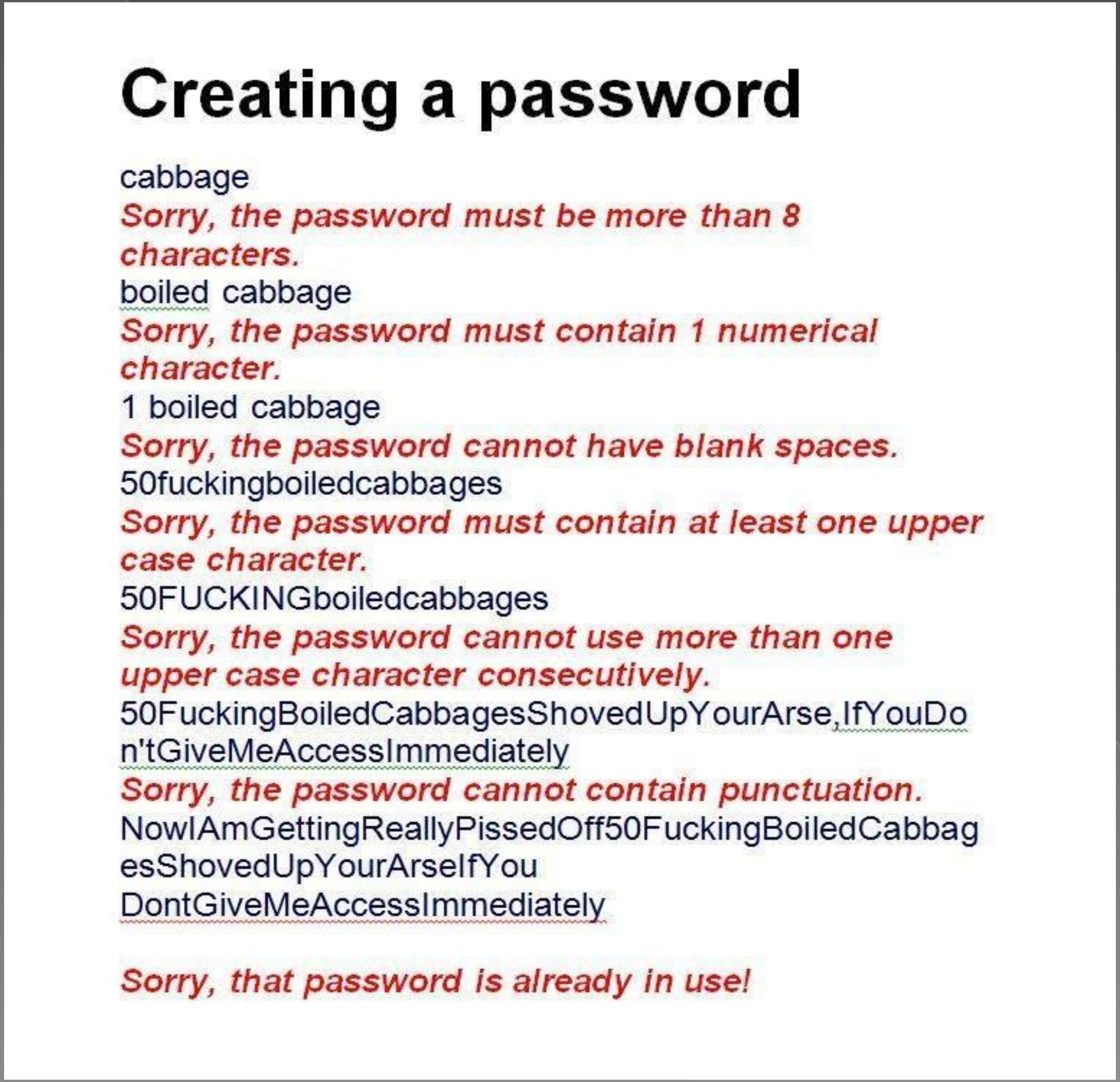
Problems:

1. Will the user get the password right?
   - Insertion errors, entering during stress

2. Will the user remember their password?
   - Issues of length, writing it down

3. Will the user reveal their password in any way?
   - Scams, or just chatter

Password Choosing



Creating a password

cabbage

Sorry, the password must be more than 8 characters.

boiled cabbage

Sorry, the password must contain 1 numerical character.

1 boiled cabbage

Sorry, the password cannot have blank spaces.

50fuckingboiledcabbages

Sorry, the password must contain at least one upper case character.

50FUCKINGboiledcabbages

Sorry, the password cannot use more than one upper case character consecutively.

50FuckingBoiledCabbagesShovedUpYourArse,IfYouDon'tGiveMeAccessImmediately

Sorry, the password cannot contain punctuation.

NowIAmGettingReallyPissedOff50FuckingBoiledCabbagesShovedUpYourArseIfYouDontGiveMeAccessImmediately

Sorry, that password is already in use!

Password Choosing

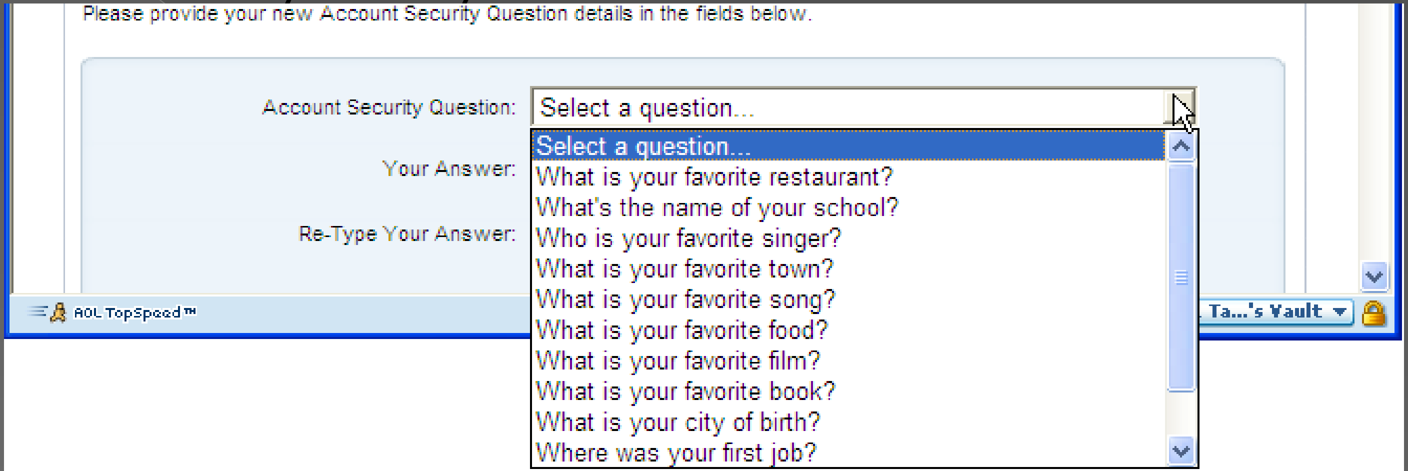
This is more critical than it may seem
An easy password is as good as no password
Bad choices:
*Anything related to your name
*Anything related to a name in general
*Too short of a password
*“password”

People have slightly improved when choosing passwords, but not enough

Password Choosing

A few points to clarify:

Design flaws in your system:



Please provide your new Account Security Question details in the fields below.

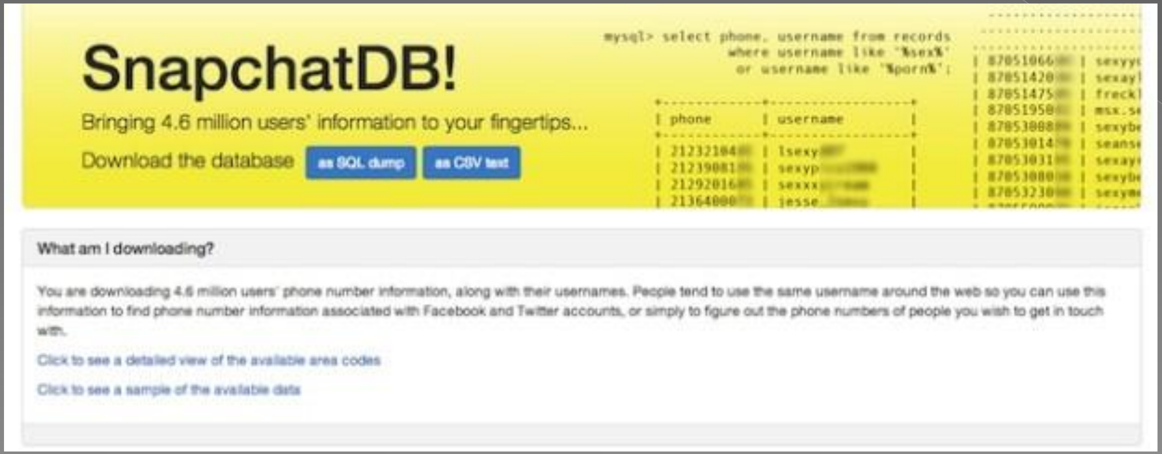
Account Security Question: Select a question...

Your Answer:

Re-Type Your Answer:

Select a question...
What is your favorite restaurant?
What's the name of your school?
Who is your favorite singer?
What is your favorite town?
What is your favorite song?
What is your favorite food?
What is your favorite film?
What is your favorite book?
What is your city of birth?
Where was your first job?
AOL TopSpeed™
Ta...'s Vault

Keeping discretion on your side



SnapchatDB!

Bringing 4.6 million users' information to your fingertips...

Download the database

```
mysql> select phone, username from records
              where username like '%sex%'
              or username like '%porn%';

+-------------+-------------+
| phone       | username    |
+-------------+-------------+
| 21232104[redacted] | lsexy[redacted] |
| 21239081[redacted] | sexyp[redacted] |
| 21292016[redacted] | sexxx[redacted] |
| 21364000[redacted] | jesse[redacted] |

| 87051066[redacted] | sexyy
| 87051420[redacted] | sexay
| 87051475[redacted] | freck
| 87051950[redacted] | msx.s
| 87053008[redacted] | sexyb
| 87053014[redacted] | seans
| 87053031[redacted] | sexay
| 87053080[redacted] | sexyb
| 87053230[redacted] | sexym
```

What am I downloading?

You are downloading 4.6 million users' phone number information, along with their usernames. People tend to use the same username around the web so you can use this information to find phone number information associated with Facebook and Twitter accounts, or simply to figure out the phone numbers of people you wish to get in touch with.

Click to see a detailed view of the available area codes

Click to see a sample of the available data

Password Security

"Trusted path" means that you can be sure you are logging to a genuine terminal.
Known assaults:

Phishing attacks can run a false program on an ATM that would look the same, and gather passwords.

Skimmer: an apparatus that fits on the actual machine, and reads all the input.

Fake terminals

Phishing counter-measures

Password Manglering
Idea: The browser hashes passwords per domain
Flaw: multiple domain sites, logging from new device

Client Certs
Idea: An electronic signature identifies the user
Flaw: Hard to implement securely, vulnerable to phishermen

Phishing counter-measures

Password cache

Idea: The browser inserts passwords only into the right website, stores them on memory

Flaw: multiple domain sites, malware

Educating users

Idea: teaching the users the latest ways of protecting themselves

Flaw: motivates bad guys to improve, does not work with some users

Phishing counter-measures

Two factor authenticating

Idea: Using ‘what you have & what you know’

Flaw: Unaffordable for small institutions, MITM attacks

Two channel authenticating

Idea: Relying on two separate forms of communication to pass info

Flaw: Fails when telephony goes through web, makes phone companies more attack prone

Phishing Evolution

MITM attacks will take on more volume

Banks are getting more and more prepared for attacks , which will cause the focus to shift.

Phishermen get better so telling phish from a genuine email will get harder and harder

Social networks in the hands of phishers act as a strong tool

System design

Questions a designer should attend:

- Strict modulation between users- needed or not?

- Will attacks be general or user-specific?

- Limit password guesses?

- Is the system vulnerable to eavesdropping?

Password storage

One main issue regarding keeping your accounts safe is what to do with passwords?

Naïve approach: keep a file of plaintext passwords. Incredibly dangerous (MIT used this)

Better approach: use hashing.
Very useful when implemented right

Note: password cracking is still a real probability, even if you hash them.

Password guessing

Password space- all possibilities of passwords allowed in a system

If your passwords space can be exhausted- that’s bad news

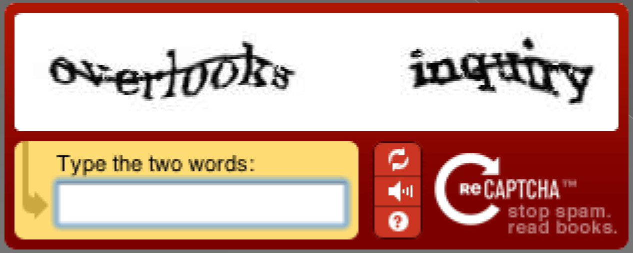
Botnets can be used to exhaust your space more easily- how do we defend against them?

CAPTCHAs

‘Completely Automated Public Turing Test To Tell Computers and Humans Apart’

This is the best method for stopping software from flooding your system.

Using the brains strengths where the computer lacks



Commonly implemented as **textual identification**

CAPTCHAs

Known problem with captcha -
While no program can solve all captchas, attackers gathered captchas and their solutions - which they got from porn sites.

This was countered by german banks that used personal CAPTCHAs

So far this method has proven to be very durable and successful.

Summary

Because of the never ending arms race between attackers and security men, the best option is to make your system hard enough to penetrate so that phishermen prefer to go elsewhere

Summary

The world of IS (info security) needs fresh thinking!

Maybe we should combine CAPTCHAs with passwords and existing methods, to create better protection?

Is there a way to block middleperson attacks?

What more can psychology tell us about IS?