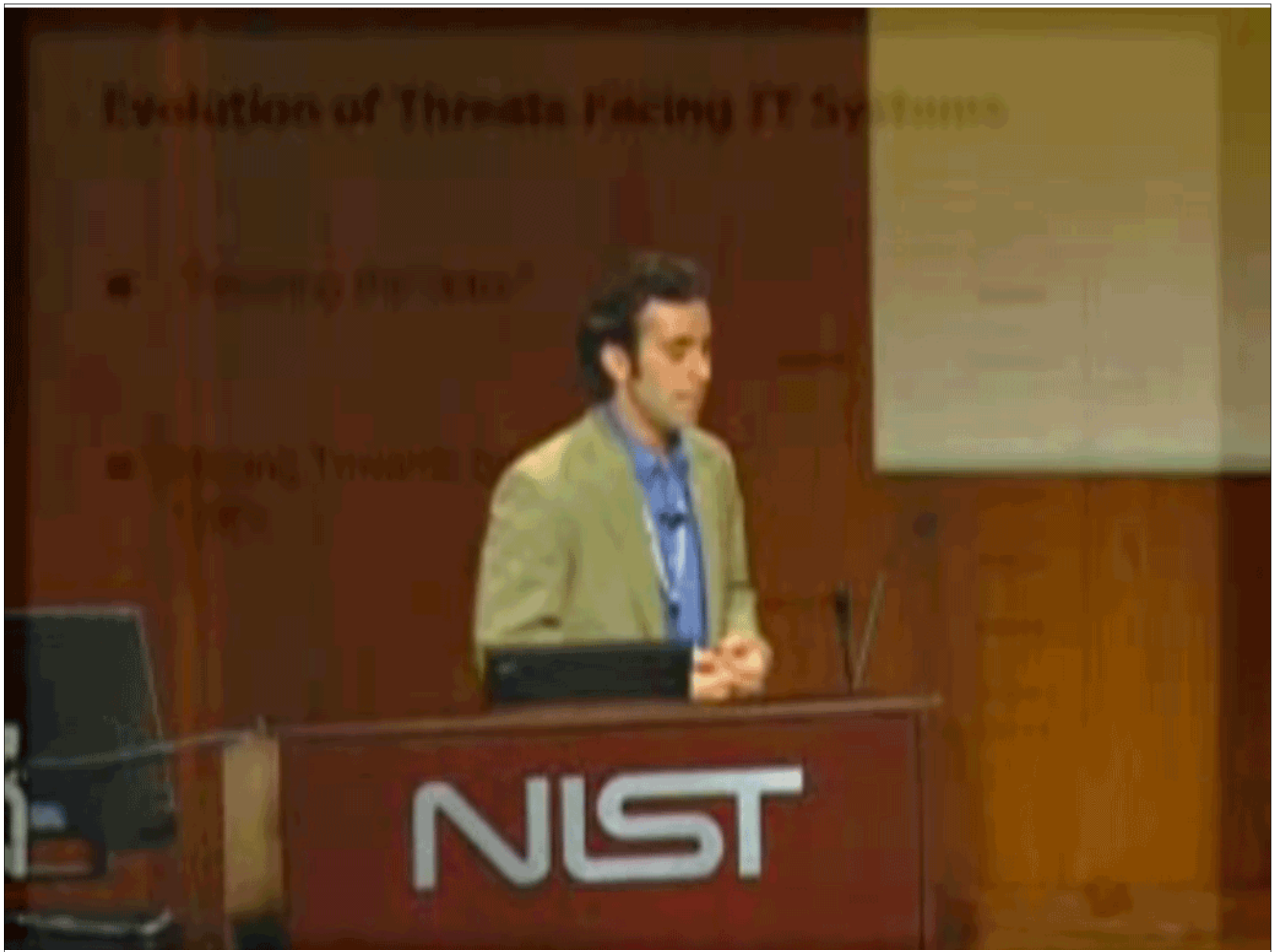


Application Security and User Experience

Alex Smolen
OWASP AppSec USA 2011





Lost iPod Touch

\$50 Reward

Call Caroline
MacLure

443-629-~~3000~~

Lost ipod touch

\$51 ~~the~~ reward

Call

410-859-~~3000~~

SOCIAL

MIND THE GAP

TECHNICAL



SECURITY

They'll Never Figure Out Your Combination

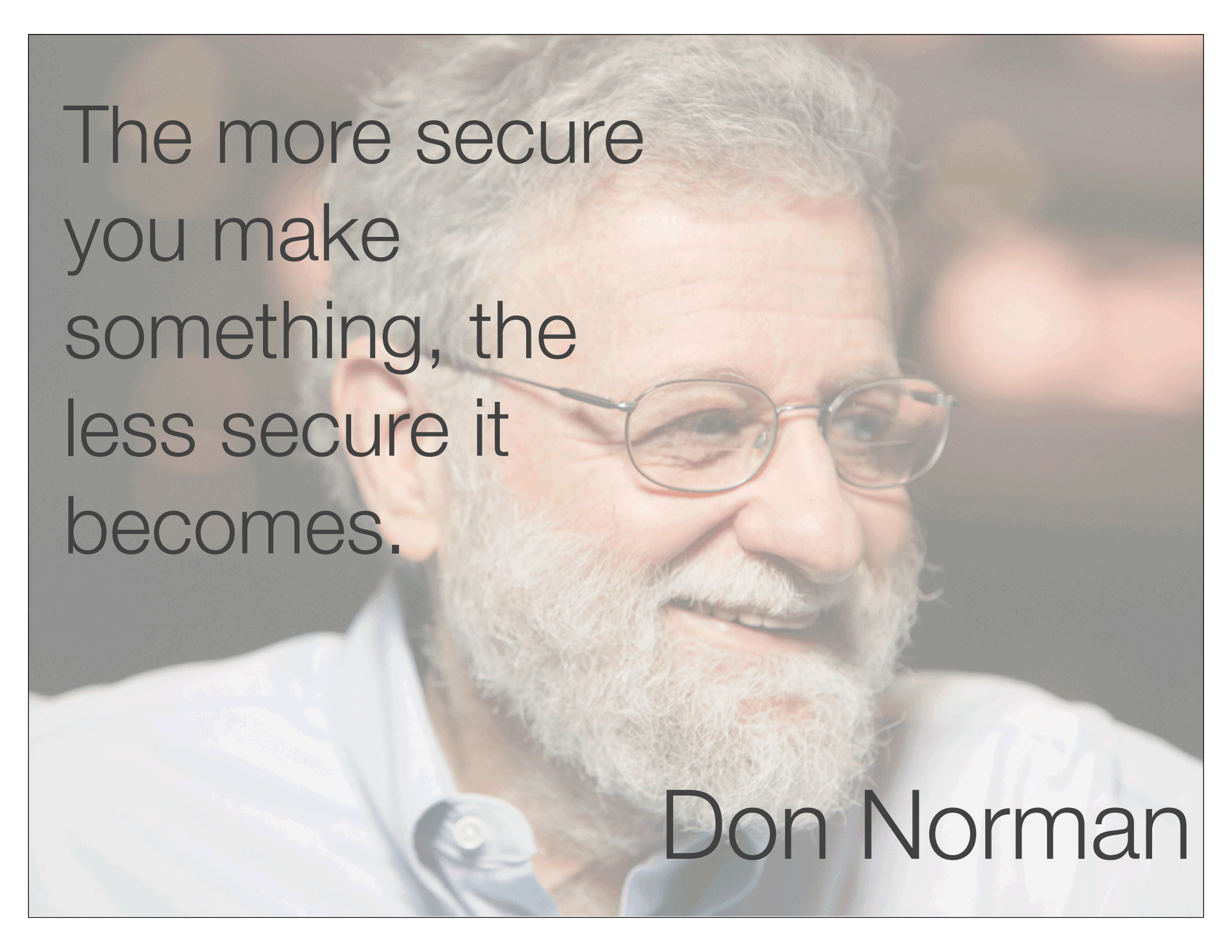
MY TOP-SECRET PASSWORDS

TITLE:		<input type="checkbox"/> WEBSITE <input type="checkbox"/> SERVICE <input type="checkbox"/> EMAIL <input type="checkbox"/> OS	
URL:		<input type="checkbox"/> SOFTWARE <input type="checkbox"/> HARDWARE <input type="checkbox"/> FORUM <input type="checkbox"/> FTP	
START DATE:	EXP. DATE:	STATUS: <input type="checkbox"/> MEMBERSHIP <input type="checkbox"/> PAID	
NAME USED:	EMAIL USED:	<input type="checkbox"/> SHARED <input type="checkbox"/> FREE	
USER NAME:		PASSWORD:	
SECRET QUESTION:		SECRET ANSWER:	
TITLE:			
<input type="checkbox"/> WEBSITE <input type="checkbox"/> SERVICE <input type="checkbox"/> EMAIL <input type="checkbox"/> OS			
<input type="checkbox"/> SOFTWARE <input type="checkbox"/> HARDWARE <input type="checkbox"/> FORUM <input type="checkbox"/> FTP			
START DATE:	EXP. DATE:	STATUS: <input type="checkbox"/> MEMBERSHIP <input type="checkbox"/> PAID	
NAME USED:	EMAIL USED:	<input type="checkbox"/> SHARED <input type="checkbox"/> FREE	
USER NAME:		PASSWORD:	
SECRET QUESTION:		SECRET ANSWER:	
TITLE:			
<input type="checkbox"/> WEBSITE <input type="checkbox"/> SERVICE <input type="checkbox"/> EMAIL <input type="checkbox"/> OS			
<input type="checkbox"/> SOFTWARE <input type="checkbox"/> HARDWARE <input type="checkbox"/> FORUM <input type="checkbox"/> FTP			
START DATE:	EXP. DATE:	STATUS: <input type="checkbox"/> MEMBERSHIP <input type="checkbox"/> PAID	
NAME USED:	EMAIL USED:	<input type="checkbox"/> SHARED <input type="checkbox"/> FREE	
USER NAME:		PASSWORD:	
SECRET QUESTION:		SECRET ANSWER:	
TITLE:			
<input type="checkbox"/> WEBSITE <input type="checkbox"/> SERVICE <input type="checkbox"/> EMAIL <input type="checkbox"/> OS			
<input type="checkbox"/> SOFTWARE <input type="checkbox"/> HARDWARE <input type="checkbox"/> FORUM <input type="checkbox"/> FTP			
START DATE:	EXP. DATE:	STATUS: <input type="checkbox"/> MEMBERSHIP <input type="checkbox"/> PAID	
NAME USED:	EMAIL USED:	<input type="checkbox"/> SHARED <input type="checkbox"/> FREE	
USER NAME:		PASSWORD:	
SECRET QUESTION:		SECRET ANSWER:	

"WHY TRY TO REMEMBER WHAT YOU COULD JUST WRITE DOWN?"

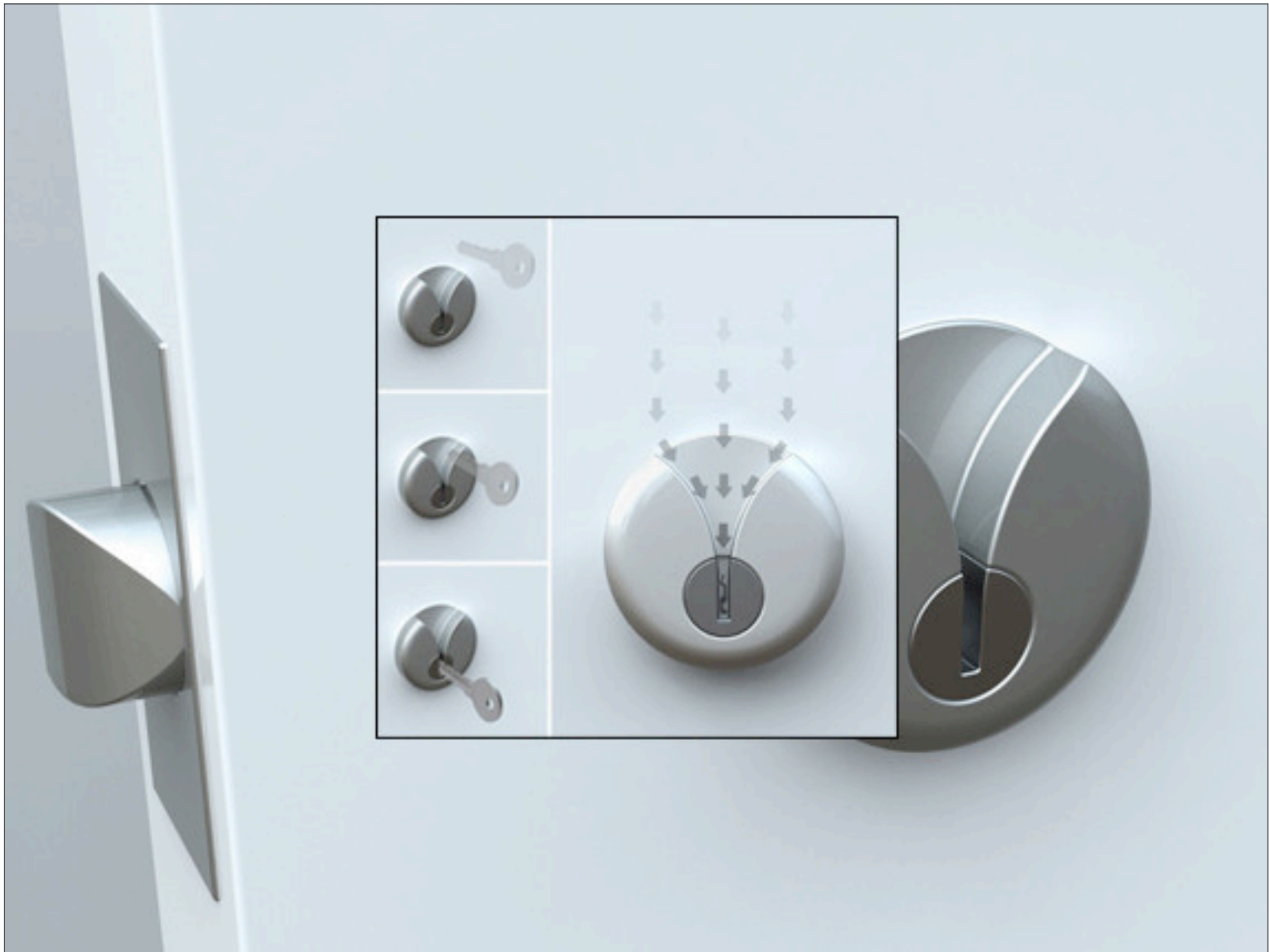
© 2004 BRYAN'S STORE, INC.



A close-up portrait of Don Norman, an older man with a full white beard and glasses, smiling slightly. He is wearing a light blue button-down shirt. The background is blurred, showing warm, out-of-focus lights.

The more secure
you make
something, the
less secure it
becomes.

Don Norman





Dylan [redacted] wow! you can type your facebook password into a comment and it comes up as stars!! ***** hahaha thats so cool!
4 hours ago



Übermensch [redacted] ***** Holy shit, you're right.
3 hours ago



Edizzle [redacted] *****
2 hours ago



Edizzle [redacted] Too cool
2 hours ago

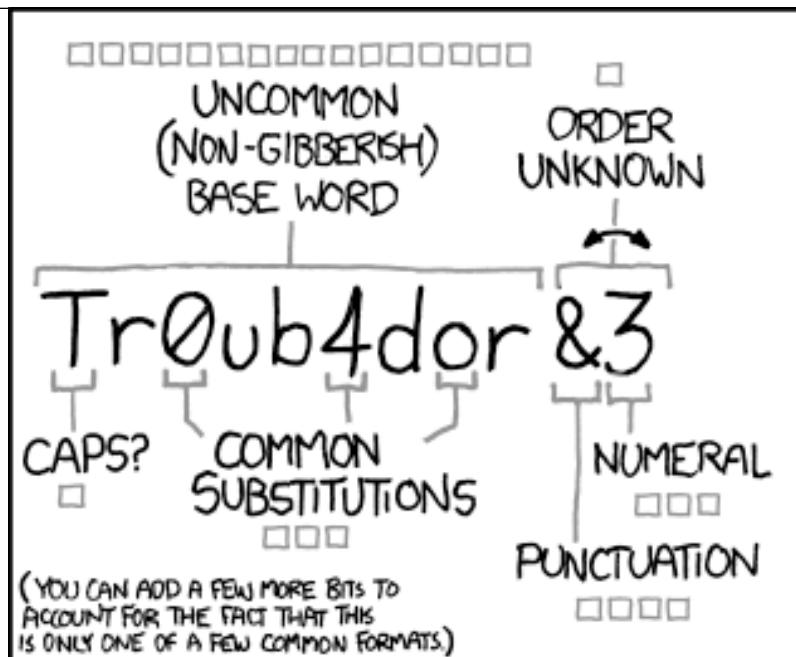


Luke [redacted] isecretlylove50cent
about an hour ago



Luke [redacted] FUCK I FUCKING HATE YOU
about an hour ago





~28 BITS OF ENTROPY

□□□□□□□□
□□□□□□□□
□□□
□□□□


$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

(PLAUSIBLE ATTACK ON A WEAK REMOTE
WEB SERVICE. YES, CRACKING A STOLEN
HASH IS FASTER, BUT IT'S NOT WHAT THE
AVERAGE USER SHOULD WORRY ABOUT.)

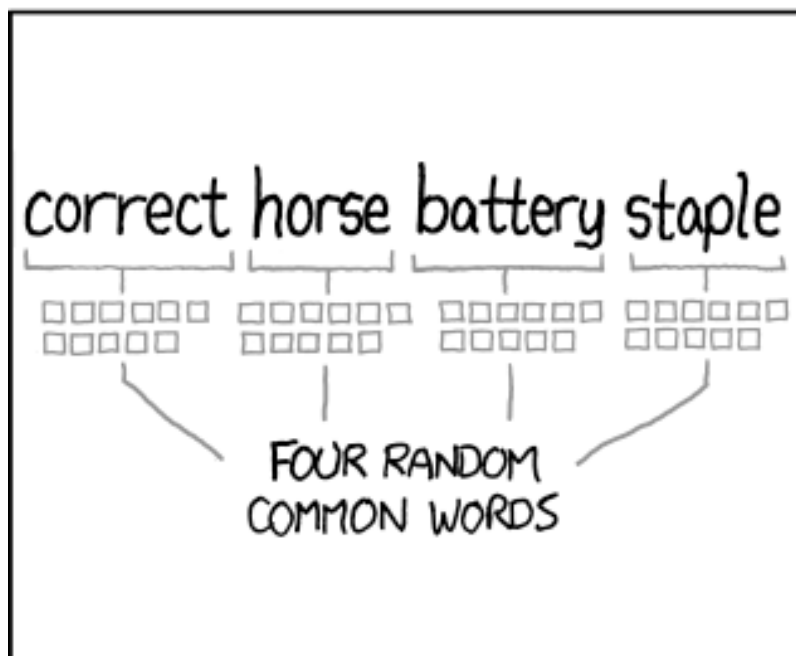
DIFFICULTY TO GUESS:
EASY

WAS IT TROMBONE? NO,
TROUBADOR. AND ONE OF
THE 0s WAS A ZERO?

AND THERE WAS
SOME SYMBOL...



DIFFICULTY TO REMEMBER:
HARD



~44 BITS OF ENTROPY

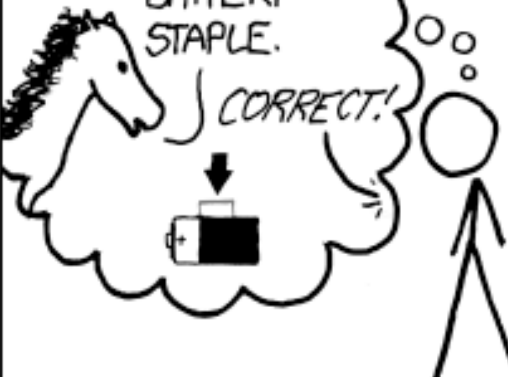
□□□□□□□□□□
□□□□□□□□□□
□□□□□□□□□□
□□□□□□□□□□

$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

DIFFICULTY TO GUESS:
HARD

THAT'S A
BATTERY
STAPLE.

CORRECT!



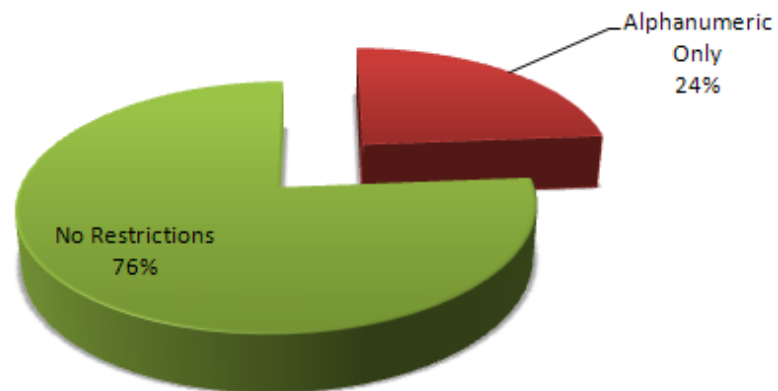
DIFFICULTY TO REMEMBER:
YOU'VE ALREADY
MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED
EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS
TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

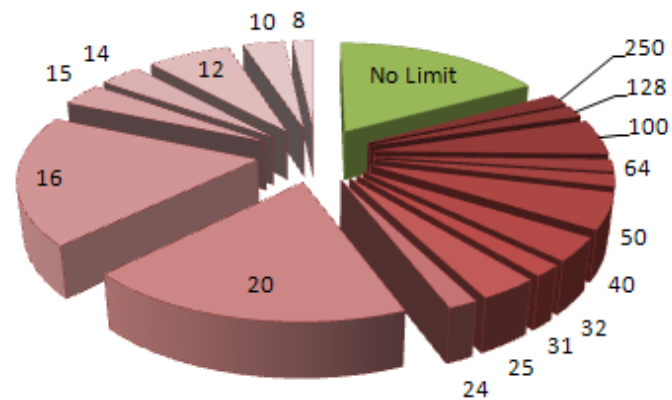
$$H = L \frac{\log N}{\log 2}$$

where N is the number of possible symbols and L is the number of symbols in the password

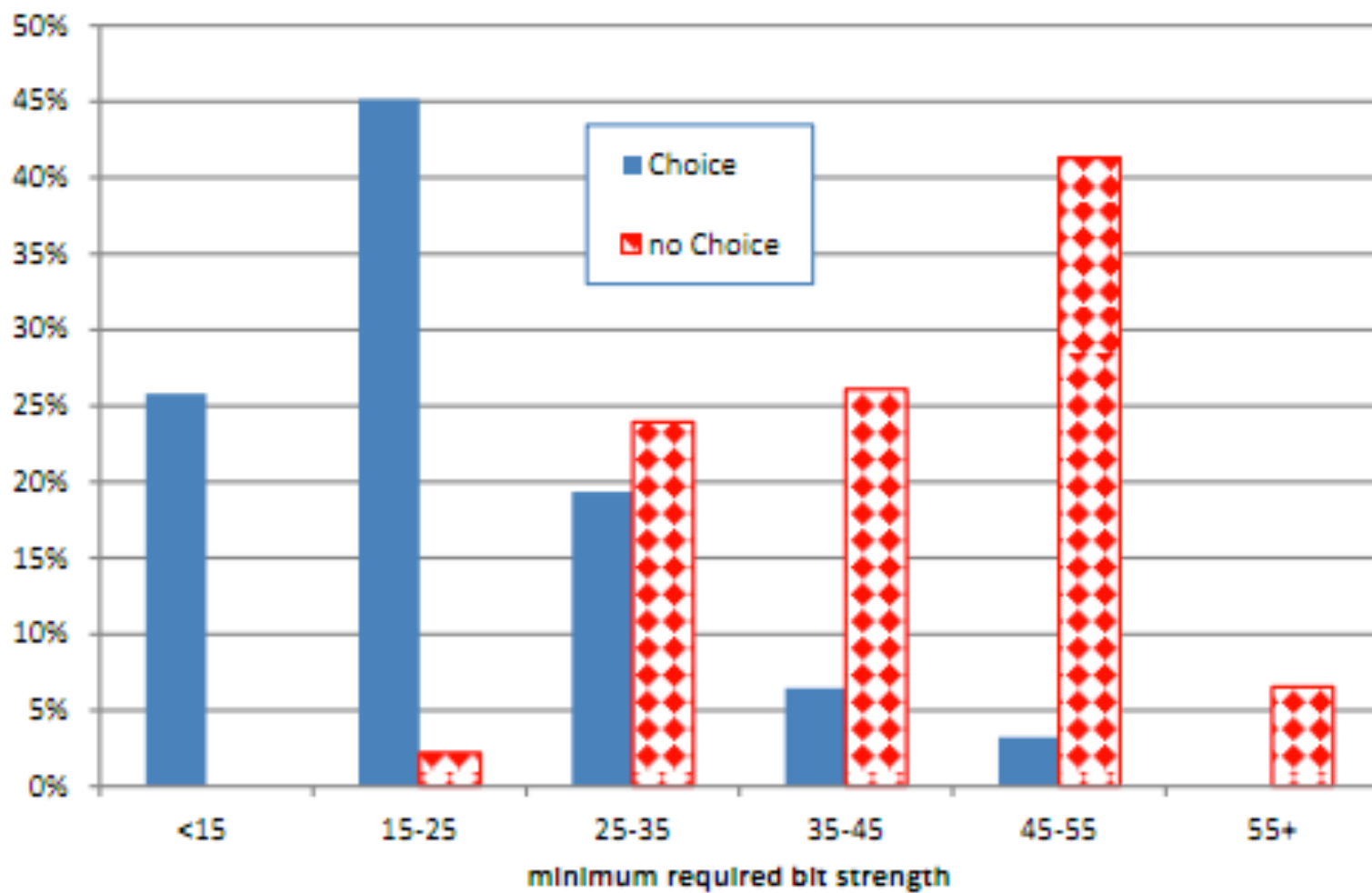
Password Character Restrictions - Alexa Top 100



Password Length Limits - Alexa Top 100



Source : <https://defuse.ca/password-policy-hall-of-shame.htm>





Source: <http://research.microsoft.com/pubs/132623/wheredosecuritypoliciescomefrom.pdf>

We conclude that forcing users to choose strong passwords appears misguided: this offers no defense against the common password stealing attacks and there are better means to address bulk guessing attacks.

D. Florencio, C. Herley, B. Coskun. *Do Strong Passwords Accomplish Anything?* HotSec '07

Password	uxmovement
Retype Password	<input checked="" type="checkbox"/> Check password

Source: <http://uxdesign.smashingmagazine.com/?p=95518>





Hi

Someone requested that your Last.fm password be reset.

If this wasn't you, there's nothing to worry about - simply ignore this email and nothing will change.

If you DID ask to reset the password on your Last.fm account, just click here to make it happen:

<http://www.last.fm/settings/resetpassword/?id=5811756&key=>

Thanks,
The Last.fm Team

Change your Last.fm email settings here:

<http://www.last.fm/settings/notifications>

Or to directly unsubscribe from all emails without any nonsense:

<http://www.last.fm/settings/unsubscribe/?auth=8234945811756>

Last.fm Ltd, Karen House, 1-11 Baches Street, London, UK, N1 6DL

Password:* -this will serve as your Login Password

Challenge Question:

Challenge Answer*:

Biography** (Limit 150 words.)

Challenge Word
City of Birth
Mother's Maiden Name
Eye Color
Pet's Name
Month of Birth

*Challenge Question ✓

*Challenge Answer

Continue Cancel

What is the name of your hometown?
What is your mother's maiden name?
What is your pet's name?
What is your preferred internet password?
Who was your childhood hero?

!?!?



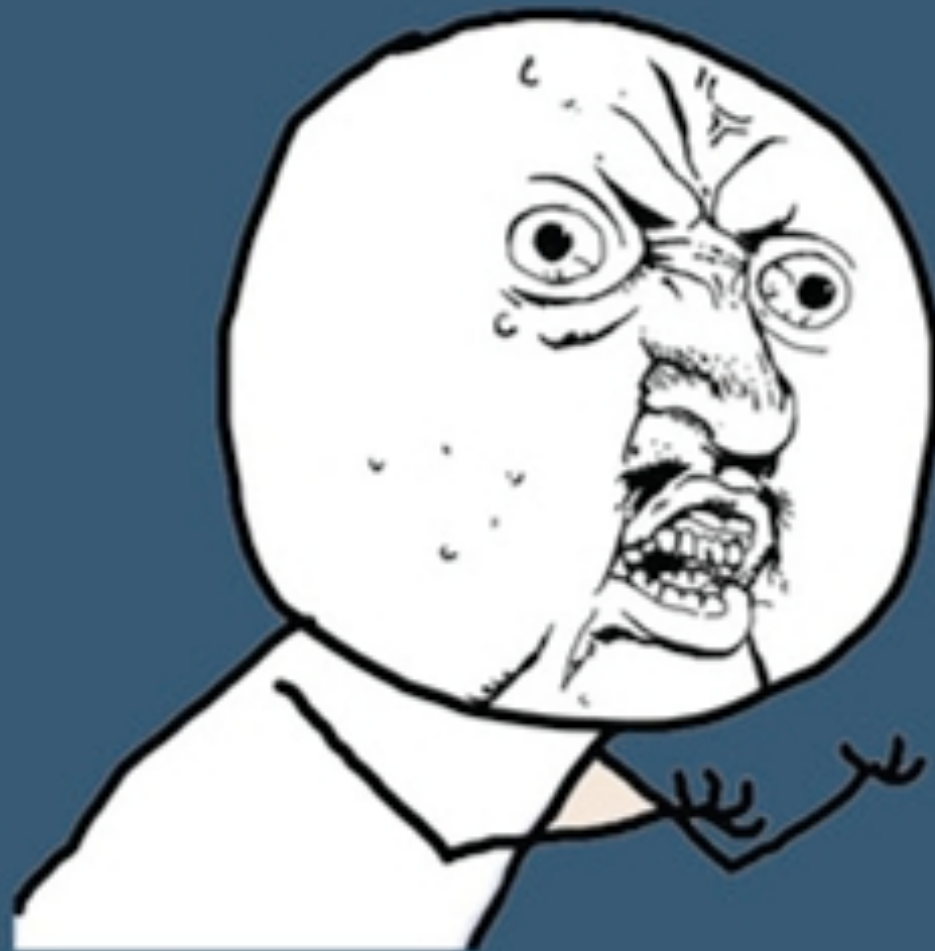
Windows Internet Explorer



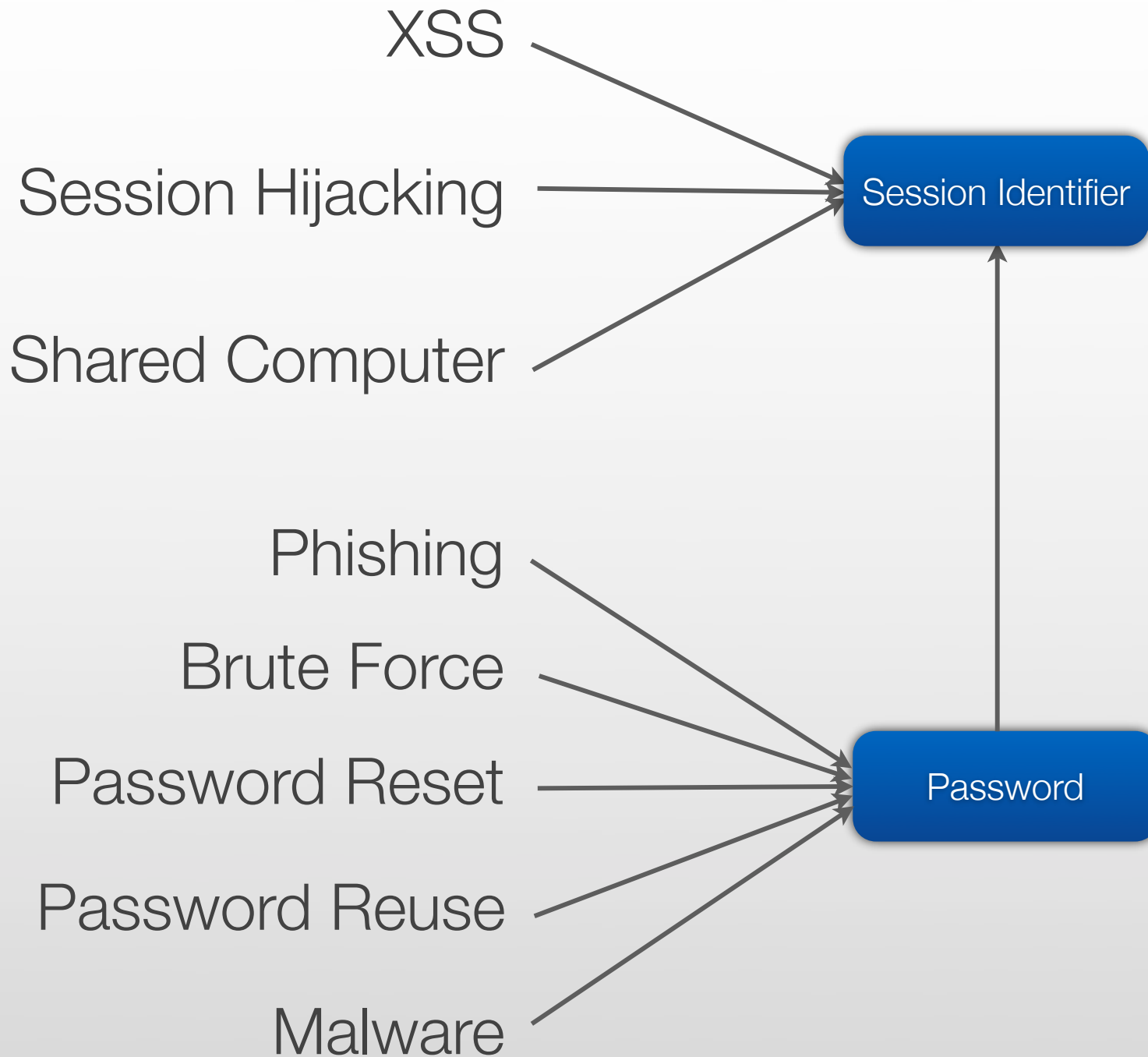
Because of inactivity, your session has timed out and is no longer active. Click OK to reload the page.

OK

KEEP ME LOGGED IN CHECK



Y U NO KEEP ME LOGGED IN

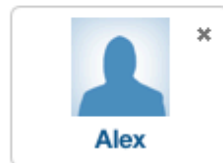




A continually improving collection of questions and answers created, edited, and organized by everyone who uses it.

You are now logged out of your account in this browser, but you are still logged in from **1 other browser**.

Login to Quora or [Create an Account](#)

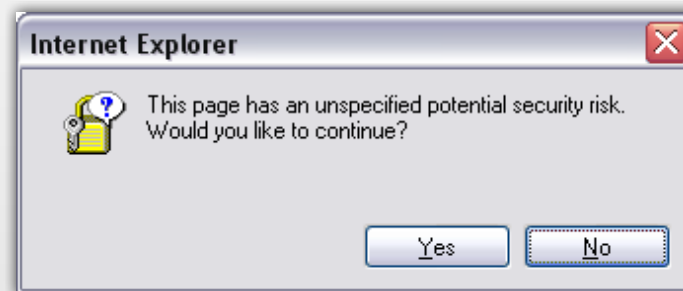
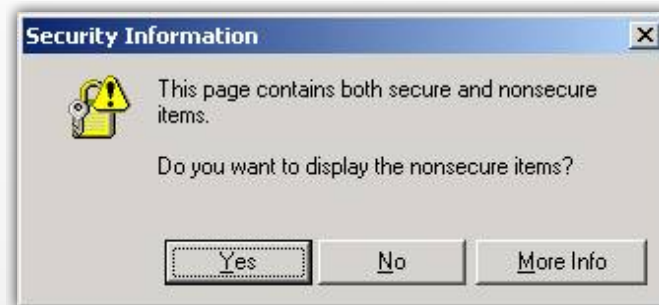


[Login As Another User](#)

I Can Relate:

"Username or Password is
Incorrect."...why don't you just
tell me which one?!

www.icanrelate.info








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](#)

Emperor's New Security Indicators

- 57 subjects
- How many withheld password?
 - 0 after HTTPS removed
 - 2 after site authentication image removed
 - 25 after warning page
 - 30 always typed in their password

Johnny can't encrypt

- 12 subjects using PGP
- How many sent secure email?
 - 3 emailed the private key
 - 1 forgot the passphrase
 - 7 used their public key to encrypt
- Only 2 of 5 encrypted messages were decrypted

Security Check

Enter **both words** below, **separated by a space**.

Can't read the words below? Try different words or an audio captcha.



Text in the box:

HOW SECURE IS MY PASSWORD?

...



Common Password: In The Top 40 Most Used Passwords

Your password is very commonly used. It would be hacked almost instantly.



Possibly A Word

Your password looks like it could be a dictionary word or a name. If it's a name with personal significance it might be easy to guess. If it's a dictionary word it could be hacked very quickly.



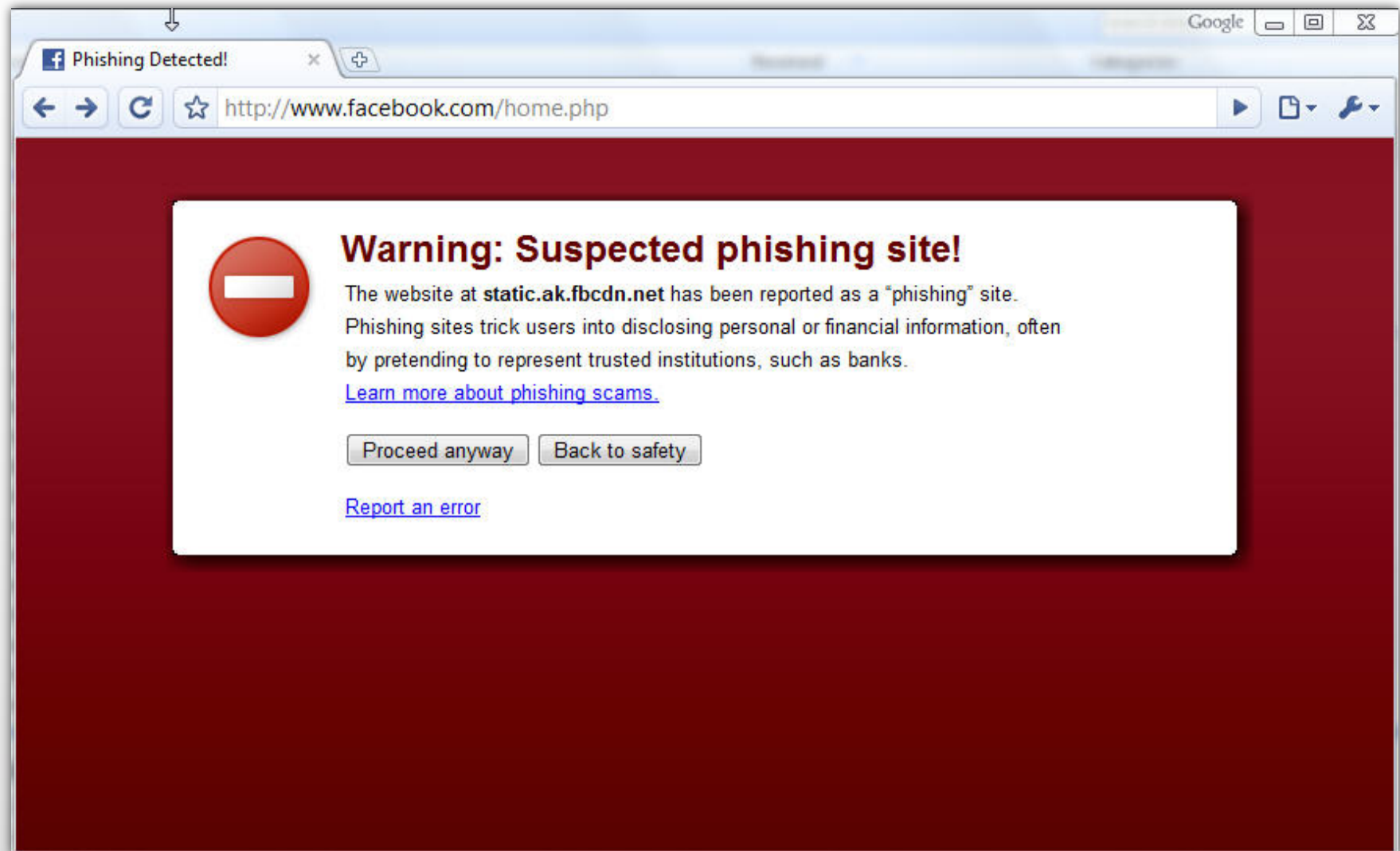
Length: Very Short

Your password is very short. The longer a password is the more secure it will be.



Character Variety: Just Letters

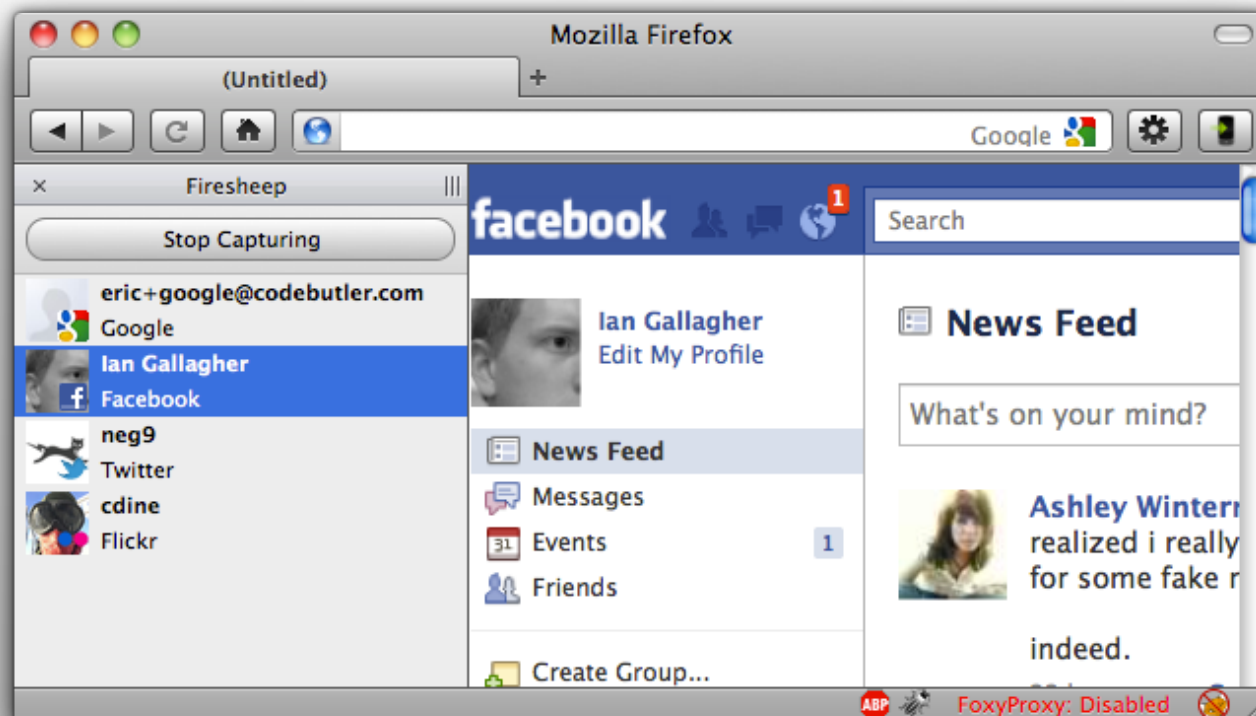
Your password only contains letters. Adding numbers and symbols can make your password more secure.





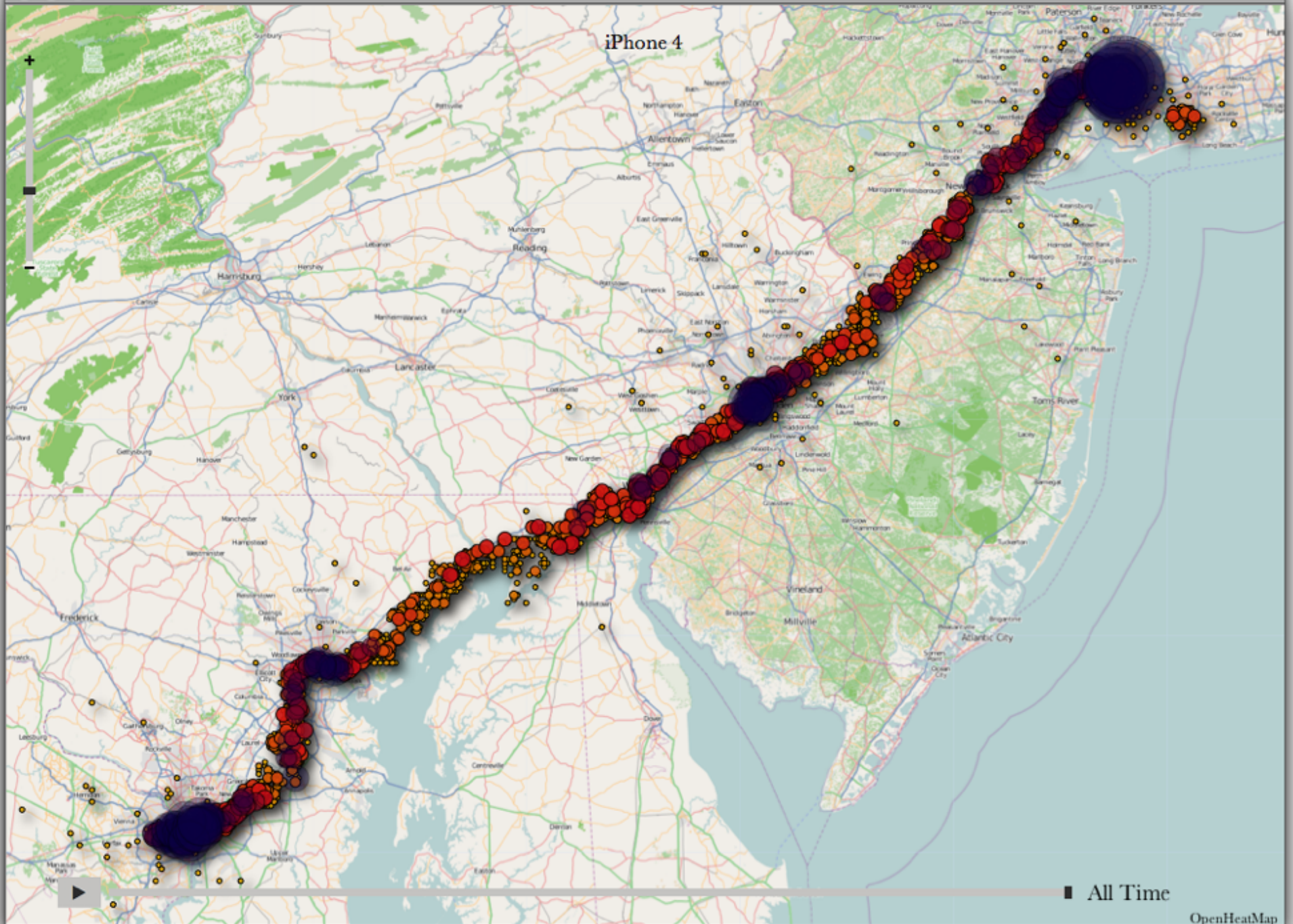
Warning: We believe your account was recently accessed from: Poland

Your filters are forwarding some of your email to 2 other email addresses



iPhoneTracker

iPhone 4



■ All Time

OpenHeatMap

Continue to Books?

You are allowing Books access to both you and your friends information below:



Others Have Allowed

- ☒ * Name: Andrew Besmer
- ☒ * Networks: UNC Charlotte
- ☒ Movies: WALL-E 16%
- ☐ Books: ~~The Cat In The~~ 92%

Also give Books the following information about your friends:

Name: Heather Richter Lipford, etc...

Networks: UNC Charlotte

Movies: Ratatouille

Books: ~~Green Eggs and Ham~~

[Continue to...](#) or Cancel

Request for Permission

Cool Social App is requesting permission to do the following:



Access my basic information

Includes name, profile picture, gender, networks, user ID, list of friends, and any other information I've shared with everyone.



Send me email

Cool Social App may email me directly at brent@example.com · [Change](#)



Access my profile information

Birthday

[Report Application](#)



Cool Social App

Logged in as  (Not You?)

Allow

Don't Allow

<u>Browser</u>	<u>Standard SSL</u>	<u>EVSSL</u>
-----------------------	----------------------------	---------------------

Internet Explorer 9	Gray padlock in address bar	Gray padlock plus full green address bar with company name or CA
---------------------	-----------------------------	------------------------------------------------------------------

Internet Explorer 8	Yellow padlock in address bar	Yellow padlock plus full green address bar with company name or CA
---------------------	-------------------------------	--------------------------------------------------------------------

Firefox 4	Blue security emblem in address bar	Green security emblem in address bar with company name
-----------	-------------------------------------	--------------------------------------------------------

Firefox 3	Padlock at bottom plus blue security emblem in address bar	Padlock at bottom plus green emblem in address bar with company name
-----------	------------------------------------------------------------	----------------------------------------------------------------------

Chrome 11	Green padlock in address bar	Green padlock plus green emblem in address bar with company name
-----------	------------------------------	------------------------------------------------------------------

Opera 11	Dark padlock plus yellow emblem in address bar written as "Secure"	Dark padlock plus green emblem in address bar written as "Trusted"
----------	--------------------------------------------------------------------	--------------------------------------------------------------------

Konqueror 4	Green shield with white check mark in address bar	Green shield with white check mark in address bar
-------------	---------------------------------------------------	---------------------------------------------------

Safari 5	Gray padlock in address bar	Gray padlock plus green company name in address bar
----------	-----------------------------	-----------------------------------------------------

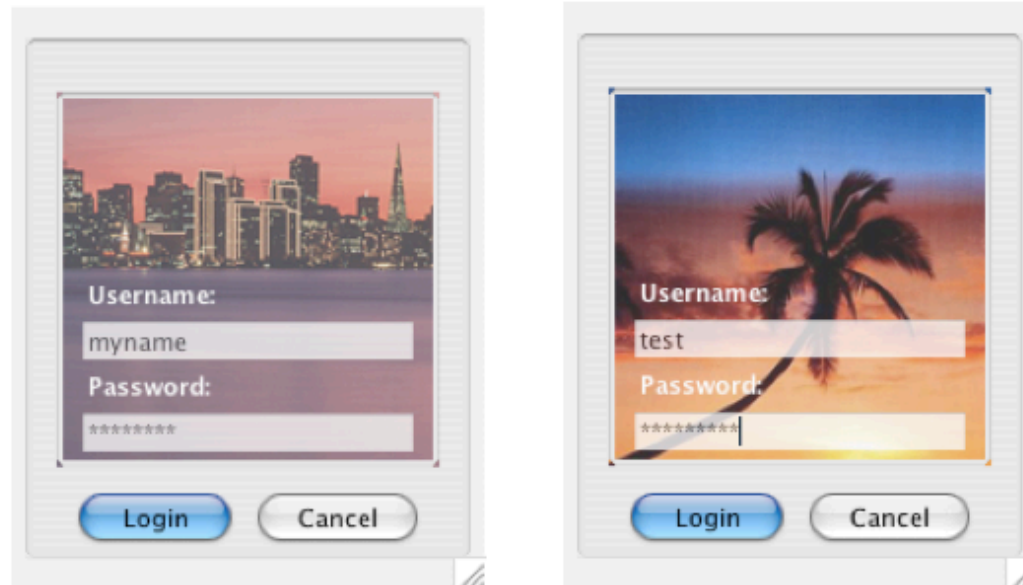
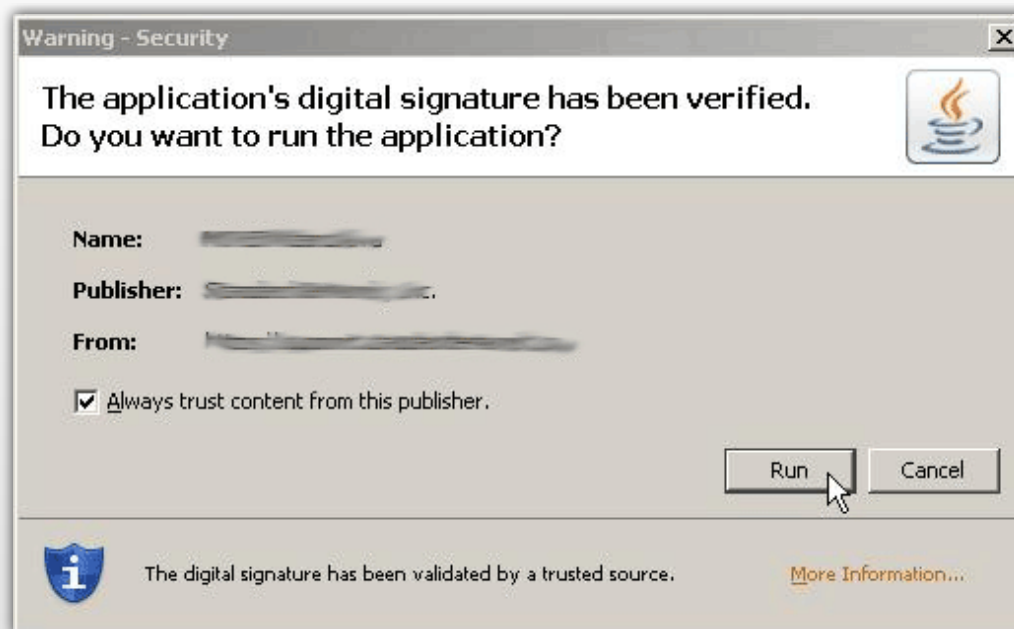


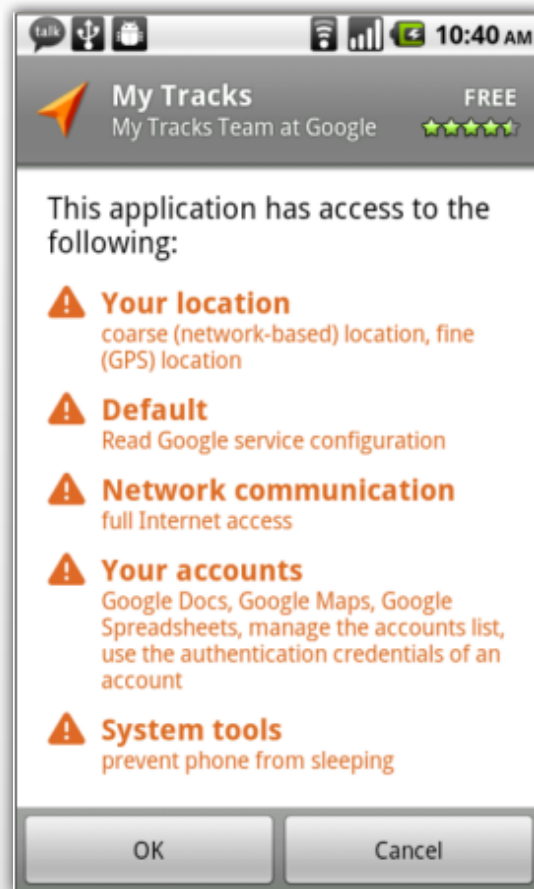
Figure 1: The trusted password window uses a background image to prevent spoofing of the window and textboxes.

The Acme Policy

types of information	how we use your information					who we share your information with	
	provide service & maintain site	research & development	marketing	telemarketing	profiling	other companies	public forums
contact information	!	!	OUT	OUT	—	IN	—
cookies	!	!	OUT	OUT	—	IN	—
demographic information	—	—	—	—	—	—	—
financial information	—	—	—	—	—	—	—
health information	—	—	—	—	—	—	—
preferences	!	!	OUT	OUT	—	IN	!
purchasing information	!	!	OUT	OUT	—	IN	—

Source: <http://cups.cs.cmu.edu/privacylabel/>







Balance

An aerial photograph of a road intersection. A road from the top left turns right, crossing over a road that runs horizontally across the middle. A security barrier is positioned at the intersection. Several cars are parked in a lot to the right, and a few cars are on the road. The area is surrounded by grass and trees. The text "Too much security can be counter-productive" is overlaid in white.

Too much security can
be counter-productive



The image shows a white, rectangular keyboard device with a minimalist design. At the top, there are two sets of seven vertical ventilation slots on either side of the brand name 'SUPERCODER 2000' and the tagline 'Air cooled coding keyboard for professional use.'. Below this, a single 'Done' key is centered. Further down, the keys '0' and '1' are visible. The device is connected to a cable at the top. The text 'Usability for us' is overlaid in the center of the image.

Usability for us

