

# The password thicket: technical and market failures in human authentication on the web

**Joseph Bonneau    Sören Preibusch**

{jcb82,sdp36}@cl.cam.ac.uk



**UNIVERSITY OF  
CAMBRIDGE**

**Computer Laboratory**

WEIS 2010

The Ninth Workshop on the Economics of Information Security

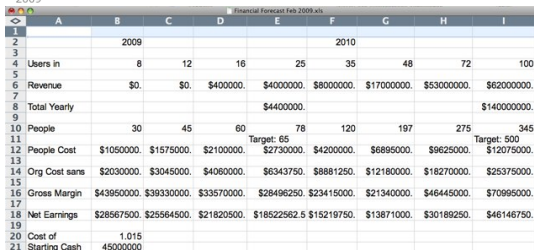
Boston, MA, USA

June 7, 2010

# Password authentication is losing viability

## In Our Inbox: Hundreds Of Confidential Twitter Documents

by Michael Arrington on Jul 14, 2009 **481 Comments** [Like](#) 11 [Buzz](#) **82** 1408 [retweet](#)



The screenshot shows a spreadsheet titled "Financial Forecast Feb 2009.xls" with columns A through I. The data is organized into two main sections for the years 2009 and 2010. The 2009 data is in columns B through D, and the 2010 data is in columns E through G. The 2010 data is further divided into two sub-sections: "Target" and "Actual".

	A	B	C	D	E	F	G	H	I
1									
2		2009				2010			
3									
4	Users in	8	12	16	25	35	48	72	100
5	Revenue	\$0.	\$0.	\$400000.	\$4000000.	\$8000000.	\$17000000.	\$53000000.	\$62000000.
6									
7	Total Yearly				\$4400000.				\$140000000.
8									
9	People	30	45	60	78	120	197	275	345
10					Target: 65				Target: 500
11	People Cost	\$1050000.	\$1575000.	\$2100000.	\$2730000.	\$4200000.	\$6895000.	\$9625000.	\$12075000.
12									
13	Org Cost sans	\$2030000.	\$3045000.	\$4060000.	\$6343750.	\$8881250.	\$12180000.	\$18270000.	\$25375000.
14									
15	Gross Margin	\$43950000.	\$39330000.	\$33570000.	\$28496250.	\$23415000.	\$21340000.	\$46445000.	\$70995000.
16									
17	Net Earnings	\$28567500.	\$25564500.	\$21820500.	\$18522562.5	\$15219750.	\$13871000.	\$30189250.	\$46146750.
18									
19									
20	Cost of	1.015							
21	Starting Cash	45000000							

Twitter hack  
July 2009

# Password authentication is losing viability

guardian.co.uk Search

News [Sport](#) [Comment](#) [Culture](#) [Business](#) [Money](#) [Life & style](#) [Travel](#) [Environment](#)

News [Technology](#) [Technology blog](#)

## TECHNOLOGY BLOG



[Previous](#) [Blog home](#) [Next](#)

### 32.6m passwords may have been compromised in RockYou hack

RockYou, which provides widgets popular with MySpace and Facebook users, has been hacked and 32.6m users are being urged to change their passwords



Part of the RockYou website

Posted by  Jack Schofield Tuesday 15 December 2009 17:33 GMT [guardian.co.uk](#)

[Print](#) [Email](#) [Facebook](#) [Twitter](#) [LinkedIn](#) [Google+](#) [RSS](#)

[larger](#) [smaller](#)

**Technology**  
Hacking · Data and computer security · Cloud computing

**Media**  
Social networking

**More from Technology**  
[blog on](#)

## RockYou SQL injection hack January 2010

# Password authentication is losing viability

## Facebook founder Mark Zuckerberg 'hacked into emails of rivals and journalists'

By MAIL FOREIGN SERVICE

Last updated at 2:09 AM on 6th March 2010

[Comments \(5\)](#) [Add to My Stories](#)

Facebook founder Mark Zuckerberg has been accused of hacking into the email accounts of rivals and journalists.

The CEO of the world's most successful social networking website was accused of at least two breaches of privacy in a series of articles run by BusinessInsider.com.

As part of a two-year investigation detailing the founding of Facebook, the magazine uncovered what it claimed was evidence of the hackings in 2004.

In the first instance, it said that, when Zuckerberg discovered that Harvard's student newspaper The Crimson was planning on running an article on him in 2004, he used reporters' Facebook logins to hack into their accounts.

In the second instance, the magazine claimed Zuckerberg hacked into the accounts of rivals at Harvard who accused him of stealing their idea for a social network. He then allegedly tried to sabotage the rival network they had set up.

Business Insider claimed that Zuckerberg learned The Crimson was planning to write an article on him when he was called in for an interview in 2004.

The newspaper was investigating allegations by other Harvard students that Zuckerberg had stolen their social networking idea - allegations that are now well-documented and became the subject of a \$65million legal suit.



© Reuters

**Allegations: Facebook founder Mark Zuckerberg**

## Zuckerberg e-mail hacking 2005



# Password authentication is losing viability

TechCrunch [About](#) | [More Headlines](#)

## Twitter Asks Users To Reset Passwords After Possible Phishing Attack

Robin Wauers  
TechCrunch.com  
Tuesday, February 2, 2010; 1:20 AM

[Twitter](#) is locking many users out of the system this morning, and sending them notices that they need to change their passwords in order to regain access to the service, due to concerns over a [possible phishing attack](#).

While some people are worried that the e-mails might have actually been a phishing attack, there's a [flood of tweets](#) from users having received the same message after effectively getting denied access to their accounts, so this seems 100% legit.

The message, copied here by a [blogger](#), reads:

Due to concern that your account may have been compromised in a phishing attack that took place off-Twitter, your password was reset. Please create a new password by opening this link in your browser: [PASSWORD RESET LINK].

The message adds:

As a reminder, you should be extraordinarily suspicious of any third party that offers to artificially inflate your follower count. We do not endorse any of these sites.



## Twitter mass reset February 2010

# A thicket 30 years in the making



*We've conducted experiments to try to determine typical users' habits in the choice of passwords . . . The results were disappointing, except to the bad guy.*

—Morris and Thompson, 1979

# Conventional wisdom is gloomy

## 1 Users can't manage

- re-use
- weak passwords
- post-it notes
- sharing

## 2 Free alternatives hard

- graphical
- cognitive

## 3 2-factor too expensive

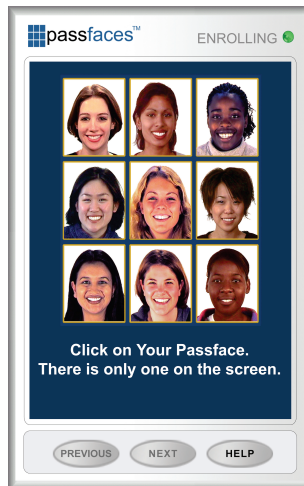
- hardware tokens
- client certs
- smartphone

## 4 Single sign-on limited



# Conventional wisdom is gloomy

- 1 **Users can't manage**
  - re-use
  - weak passwords
  - post-it notes
  - sharing
- 2 **Free alternatives hard**
  - graphical
  - cognitive
- 3 2-factor too expensive
  - hardware tokens
  - client certs
  - smartphone
- 4 Single sign-on limited



Passfaces

# Conventional wisdom is gloomy

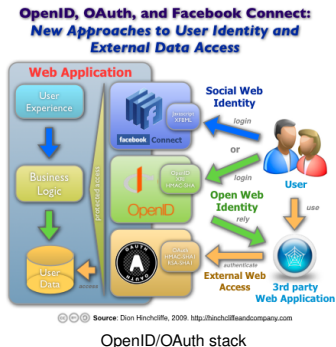
- 1 **Users can't manage**
  - re-use
  - weak passwords
  - post-it notes
  - sharing
- 2 **Free alternatives hard**
  - graphical
  - cognitive
- 3 **2-factor too expensive**
  - hardware tokens
  - client certs
  - smartphone
- 4 **Single sign-on limited**



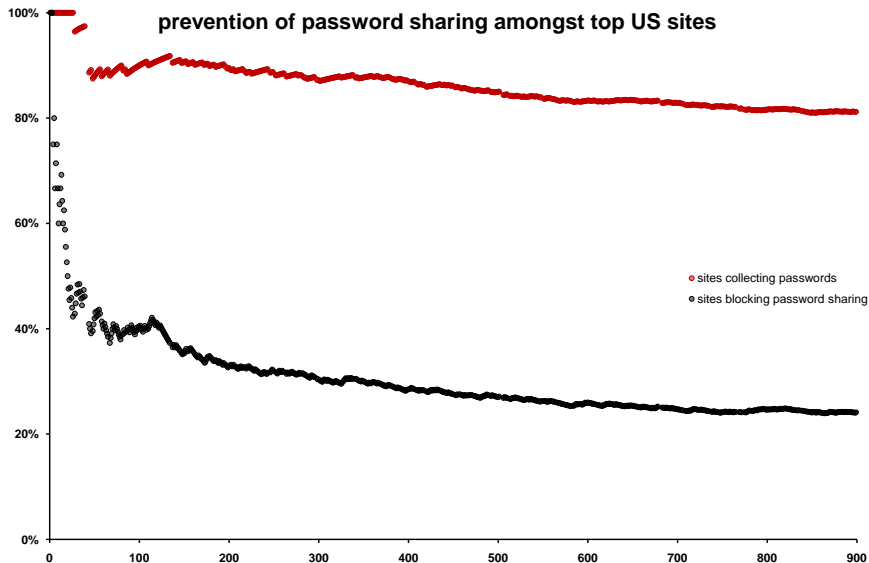
Cronto

# Conventional wisdom is gloomy

- 1 **Users can't manage**
  - re-use
  - weak passwords
  - post-it notes
  - sharing
- 2 **Free alternatives hard**
  - graphical
  - cognitive
- 3 **2-factor too expensive**
  - hardware tokens
  - client certs
  - smartphone
- 4 **Single sign-on limited**



# Password collection remains ubiquitous




# Supply side of the market remains poorly understood

- 1 How does the user experience vary from site to site?
- 2 What implementation weaknesses exist?
- 3 Which circumstantial factors affect sites' implementation choices?
- 4 How do sites' security requirements affect their choices?
- 5 Why do websites choose to collect passwords?



# Coarse classification of password deployment cases



View Photos of Me (533)

View Videos of Me (2)

Edit My Profile

Write something about yourself.

**Information**


Networks:  
Cambridge Grad Student '11  
Stanford Alum '06

Birthday:  
July 17, 1984

Current City:  
San Francisco, CA

**Friends**


664 friends See All




Brett Talbot




Ryan Sil




Tyler Jank



Chris Ching



Bob Borek






Katie Stenson

**Joseph Bonneau**

Wall Info Photos Boxes +


What's on your mind?

Attach:     

Options

**Molly Fox**

In these photos: Joseph Bonneau



**Hail the MiniCleggs of Bratislava**

Easter, part the first.

May 23 at 7:07pm · View album

**Stella Nordhagen**

In these photos: Joseph Bonneau




**Hail Hail Hail**

9 new photos


A (belated) celebration of colour!

May 18 at 4:53pm · View album

**RECENT ACTIVITY**

 Joseph is now friends with Michelle Russo Vinroe and Katie Haberman.

 Joseph attended Gates Distinguished Lecture. · Comment · Like

 Joseph and Noah Isserman are now friends. · Comment · Like

## Identity

# Coarse classification of password deployment cases

Quantity:

 **Add to Cart**

or

 **Buy now with 1-Click<sup>®</sup>**

**Ship to:**

☐ Add gift-wrap/note

or

 **Add to Cart with  
FREE Two-Day Shipping**


**Amazon Prime Free Trial  
required. Sign up when you  
check out. [Learn More](#)**

**Add to Wish List** ▼

**E-commerce**

# Coarse classification of password deployment cases


---

 **CURRENT E-MAILS**

---

You have no subscriptions for Email newsletters.


---

 **MY ALERTS** [+ Create News Alert](#)

---

You have no alerts, use the "Create News Alert" link above to create one.


---

 **MY STOCK ALERTS** [+ Create Stock Alert](#)

---

You have no alerts, use the "Create Stock Alert" link above to create one.

---

 **COMMENT NOTIFICATIONS**

---

Receive a notification when your comment is posted or replied to by an NYTimes reporter.

[SUBSCRIBE](#)

---

**TODAY'S HEADLINES**

---

**TODAY'S HEADLINES** [SUBSCRIBE](#)

DAILY

Get general top headlines or create a customized e-mail by selecting from the categories below.

[See Sample](#)

<input type="checkbox"/> U.S.	<input type="checkbox"/> Daily Featured Section	<input type="checkbox"/> Editorial
<input type="checkbox"/> Sports	<input type="checkbox"/> Business	<input type="checkbox"/> Technology
<input type="checkbox"/> Politics	<input type="checkbox"/> World	<input type="checkbox"/> NY Region
<input type="checkbox"/> Op-Ed	<input type="checkbox"/> Arts	

**Content**

# Random study sample designed for depth, breadth



# Site classification allows for feature overlap

Feature	I	E	C	Tot.
News displayed	15	0	49	64
Products for sale	4	50	1	55
Payment details stored	7	30	2	39
Social networking	28	1	2	31
Premium accounts available	17	3	8	28
Email accounts provided	17	0	2	19
Discussion forums	16	1	2	19

# Complete evaluation of visible password security

## 1 enrolment

- p. advice
- data collected

## 2 login

- data transmission

## 3 update

- re-authentication
- p. requirements

## 4 recovery

- backup auth.
- replacement

## 5 attacks

- user probing
- p. guessing

Create your profile

Welcome!

Creating a personal profile has many advantages:

- Your online orders will be easy to place. You don't have to add your personal information every time.
- You can save your personal preferences and designs on the IKEA Server and quickly access them when you are in the store.

Fields marked with \* are mandatory

1 Where do you live?  
Your preferred store

2 Your personal information  
Month  Birthday  Year   
    
\*First name   
\*Address   
\*City   
\*Postcode (ex. 12345)   
\*Mobile number

3 Your phone numbers  
\*Home phone number (Ex. 000-000-0000)  Tel.   
\*Mobile phone number (Ex. 000-000-0000)

4 Enter your username  
\*Email address  \*\*No other email address

5 Choose your password  
Password rules:  
Password must contain at least 7 characters  
Password must contain at least 1 digit  
Password must contain at least 1 letter  
Password must not be the same as username  
Password can not have 3 of the same consecutive characters, nor 4 of the same characters throughout.  
\*Password  \*\*No other password

6 Validation Image  
  
Are you still having problems with the image? Don't worry, we can help you. [Click here](#)  
Enter the characters you see in the image into the field below.  
If you can't see all the letters, just change the image by [clicking here](#)

7 Confirmation and agreement  
☐ I agree that IKEA saves my personal information and agree to the IKEA privacy policy  
[Privacy Policy](#)

8 Save your information  
  
☐ Remember me? What's this?

IKEA

# Complete evaluation of visible password security

## 1 enrolment

- p. advice
- data collected

## 2 login

- data transmission

## 3 update

- re-authentication
- p. requirements

## 4 recovery

- backup auth.
- replacement

## 5 attacks

- user probing
- p. guessing

Login

Login to access your profile. For more information regarding your order call: 1-800-434-IKEA

1 Login in here

Enter your username: (email address)

Enter your password:

[Forgot your password? Click here.](#)

Login

☐ Remember me [What's this?](#)

IKEA

# Complete evaluation of visible password security

- 1 **enrolment**
  - p. advice
  - data collected
- 2 **login**
  - data transmission
- 3 **update**
  - re-authentication
  - p. requirements
- 4 **recovery**
  - backup auth.
  - replacement
- 5 **attacks**
  - user probing
  - p. guessing

## Change my password

Change your password. Follow the instructions below.

Fields marked with \* are mandatory

### 1 Enter password

Password rules:

Password must contain at least 7 characters

Password must contain at least 1 digit

Password must contain at least 1 letter

Password must not be the same as username

Password can not have 3 of the same consecutive characters, nor 4 of the same characters throughout.

\*Old password

Please enter old Password.

\*Password

\*Re-enter password

### 2 Save my new password

Save and continue

IKEA



# Complete evaluation of visible password security

- 1 **enrolment**
  - p. advice
  - data collected
- 2 **login**
  - data transmission
- 3 **update**
  - re-authentication
  - p. requirements
- 4 **recovery**
  - backup auth.
  - replacement
- 5 **attacks**
  - user probing
  - p. guessing

Request a new password

If you have forgotten your password you can order a new one here.

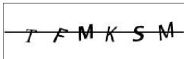
Fields marked with \* are mandatory.

\*Username (e-mail address)

Please enter Username or Password.

1 How do you want to receive your new password?  
• \*Send out new password via email

2 Validation image



Are you still having problems with the letters?  
Don't worry, we can help you. [Click here](#)

Enter the characters you see in the image into the field below.  
If you can't see all the letters, just change the image by [clicking here](#)

3 Get new password

---

IKEA

# Complete evaluation of visible password security

## 1 enrolment

- p. advice
- data collected

## 2 login

- data transmission

## 3 update

- re-authentication
- p. requirements

## 4 recovery

- backup auth.
- replacement

## 5 attacks

- user probing
- p. guessing

### Login

Login to access your profile. For more information regarding your order call:  
1-800-434-IKEA

Please enter your username and password.

Login error - Invalid username/password!

### 1 Login in here

Enter your username: (email address)

Enter your password:

[Forgot your password? Click here.](#)

Login

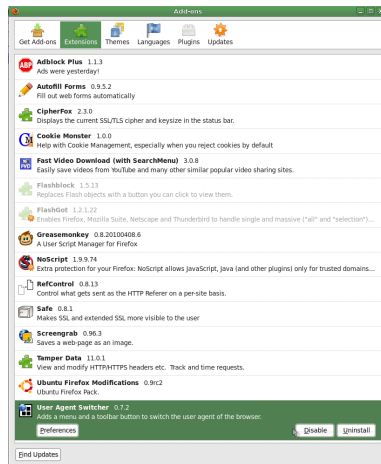
☐ Remember me [What's this?](#)

IKEA

# Semi-automated human-in-the-loop evaluation

Mozilla Firefox v 3.5.8 with:

- **Autofill Forms 0.9.5.2**
- **CipherFox 2.3.0**
- **Cookie Monster 0.98.0**
- **DOM Inspector 2.0.4**
- **Greasemonkey 0.8.20100211.5**
- **Screengrab 0.96.2**
- **Tamper Data 11.0.1**



# Findings

- 1 How does the user experience vary from site to site?
- 2 What implementation weaknesses exist?
- 3 Which circumstantial factors affect sites' implementation choices?
- 4 How do sites' security requirements affect their choices?
- 5 Why do websites choose to collect passwords?

# User experience varies considerably

Choose a Password, which you'll also enter each time you use this service. Your password should be 5-15 characters in length and shouldn't include punctuation, symbol characters or spaces.

**Important:** We'll record your User Name and Password EXACTLY as you type them, so make a note if you enter in upper and lower case.

WSJ 1996

Please register to gain free access to WSJ tools.

First Name	Last Name
<input type="text"/>	<input type="text"/>
Email (your email address will be your login)	
<input type="text"/>	
Confirm Email	
<input type="text"/>	
Create a Password	Confirm Password
<input type="text"/>	<input type="text"/>

From time to time, we will send you e-mail announcements on new features and special offers from The Wall Street Journal Online.

[REGISTER NOW ▶](#)

[Why Register? ▼](#)

[Privacy Policy](#) | [Terms & Conditions](#)

WSJ 2010

- Bare-bones password entry is universal
- Advice rare and inconsistent

# User experience varies considerably

Advice	I	E	C	Tot.
Use digits	9	6	3	18
Use symbols	9	2	3	14
Graphical strength indicator	9	0	2	11
Difficult to guess	5	2	2	9
Not a dictionary word	6	0	2	8
Change regularly	4	0	1	5
<b>Any</b>	<b>18</b>	<b>8</b>	<b>7</b>	<b>33</b>

- Bare-bones password entry is universal
- Advice rare and inconsistent

# Findings

- 1 How does the user experience vary from site to site?
- 2 What implementation weaknesses exist?**
- 3 Which circumstantial factors affect sites' implementation choices?
- 4 How do sites' security requirements affect their choices?
- 5 Why do websites choose to collect passwords?

# TLS deployment sparse and inconsistent

Please enter a new password

Email: facebook@ucam.preibusch.net

New Password:

(required)

Confirm Password:

(required)

Change Password

☐ Keep me logged in

[Forgot your password?](#)

Email

Password

Login

## Password

- Do not use the same password that you use for other online accounts.
- Your new password must be at least 6 characters in length.
- Use a combination of letters, numbers, and punctuation.
- Passwords are case-sensitive. Remember to check your CAPS lock key.

Old Password:

New Password:

(required)

Confirm Password:

(required)

Change Password

## Sign Up

It's free and anyone can join

First Name:

Last Name:

Your Email:

New Password:

I am: **Select Sex:**

Birthday: **Month:** **Day:** **Year:**

Why do I need to provide this?

Sign Up

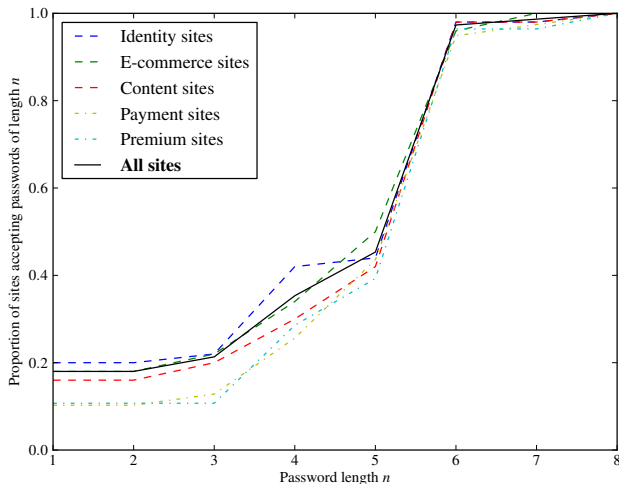
Facebook



# TLS deployment sparse and inconsistent

TLS Deployment	I	E	C	Tot.
Full	10	39	10	<b>59</b>
Full/POST	3	1	1	<b>5</b>
Inconsistent	14	6	5	<b>25</b>
None	23	4	34	<b>61</b>

# No standard for password length



# No standard for password recovery

Dear Joseph Bonneau,

You requested us to send you your EasyChair login information. Please use the following data to log in to EasyChair:

User name: jbonneau

Password: -----

Best regards,  
EasyChair Messenger.

EasyChair (not surveyed)

# No standard for password recovery

Hello, jbonneau:

Thanks for using your Ticketmaster account.

This is a temporary password: ---

Use this temporary password to login and reset your password again.

We hope you enjoy using your account!

Thanks,  
The Ticketmaster Team

Ticketmaster

# No standard for password recovery

Hi jbonneau,

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/?id=<userid>&key=<authentication-token>>

Best Regards,  
The Last.fm Team

Last.fm

# No standard for password recovery

Recovery Mechanism	I	E	C	Tot.
Email only	32	42	46	<b>120</b>
Email plus personal knowledge	11	4	3	<b>18</b>
Personal knowledge only	5	2	1	<b>8</b>
None available	2	2	0	<b>4</b>
<b>Email contents</b>				
Original password (cleartext)	5	14	17	<b>36</b>
Temporary password	11	15	12	<b>38</b>
Reset link	29	18	20	<b>67</b>

# Password guessing rarely prevented

## The following errors were encountered

- You are only permitted to make four login attempts every 1 minute(s)

[Return to Previous Page](#)

Truthdig

- Timeout
- Lockout/forced reset
- CAPTCHA

## Sign In

---

**Too many tries!**

If you forgot your password, you can [get help finding it](#), or you can [open a new account](#).

Cafe Press

- Timeout
- Lockout/forced reset
- CAPTCHA



# Password guessing rarely prevented

## Log in

---

Don't have an account? [Create one](#).

To help protect against automated password cracking, please enter the words that appear below in the box ([more info](#)):

signsowned

Username:

Password:

☐ Remember me (up to 30 days)

Wikipedia

- Timeout
- Lockout/forced reset
- CAPTCHA

# Password guessing rarely prevented

countermeasure	I	E	C	Tot.
CAPTCHA	11	2	1	14
timeout	2	1	2	5
reset	1	3	1	5
none	37	43	46	126

# Password guessing rarely prevented

limit	I	E	C	Tot.
3	3	0	0	3
4	1	1	0	2
5	3	2	4	9
6	2	2	0	4
7	1	0	0	1
10	2	0	0	2
15	1	0	0	1
20	0	1	0	1
25	1	0	0	1
> 100	37	43	46	126

## Create an Account

### Required information for Google account

Your current email address:

There's already a Google Account associated with this email address. Please sign in; or, if you forgot your password, [reset it](#) now. [\[?\]](#)

Google

- Enrolment
- Login
- Recovery

# User probing prevention rarely complete

Sign In

E-mail:

Password:

☒ Remember me on this computer

! Oops, unknown user email. Have you signed up yet?

Sign In

Forgot your password?

Ask

- Enrolment
- Login
- Recovery

# User probing prevention rarely complete

## Request to Reset Your Password

Please fix the following errors:



- **We're sorry, but that email address is not in our records. Please confirm your information is correct and try again.**

Don't worry about forgetting your password, resetting it is quick and easy.

**Just enter your email address:**

Continue

Zappos!

- Enrolment
- Login
- Recovery

# User probing prevention rarely complete

interface	I	E	C	Tot.
enrolment	4	1	1	6
login	43	41	38	132
reset	11	7	2	20
all	1	1	0	2

# 10-dimensional password security policies

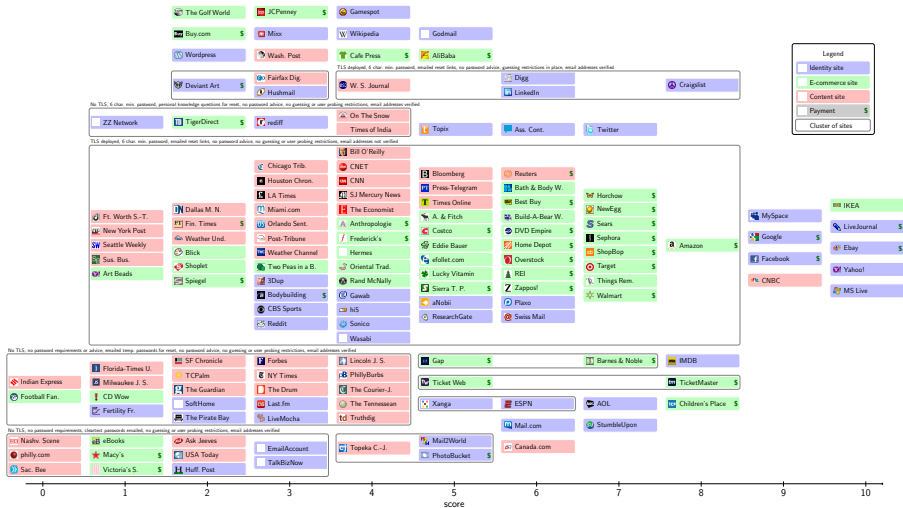
feature	cardinality
Enrolment email contents	8
Password advice	16
Minimum password length	8
Password requirements	16
Federated login support	8
Password update	8
Password recovery mechanism	8
Brute force restrictions	4
User probing restricted	12
TLS deployment	4



# Most sites re-inventing the wheel

Uniqueness radius	% of sites
0	100.0
1	90.6
2	56.0
3	24.0
4	7.3
5	1.3
6	0.0

# Security-conscious sites are pioneers



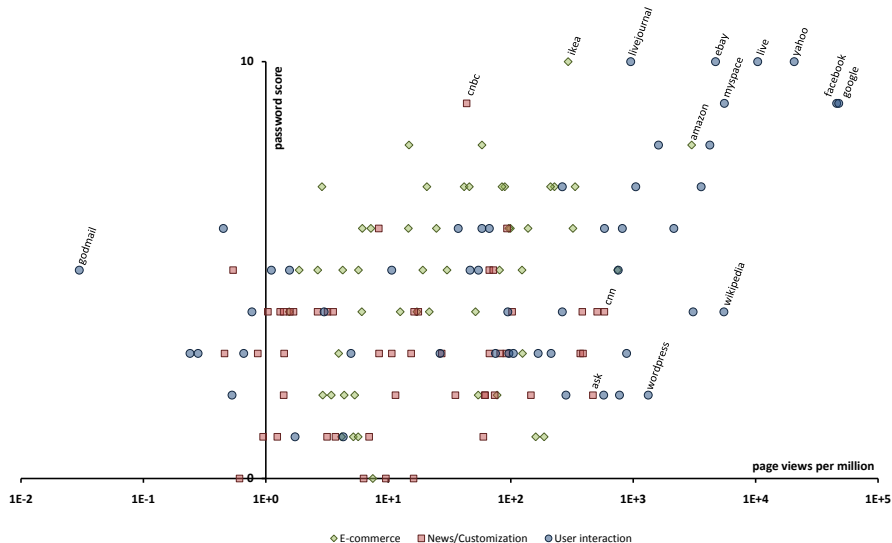
# Findings

- 1 How does the user experience vary from site to site?
- 2 What implementation weaknesses exist?
- 3 Which circumstantial factors affect sites' implementation choices?**
- 4 How do sites' security requirements affect their choices?
- 5 Why do websites choose to collect passwords?

# 10-point aggregate password score used for analysis

feature	scoring
<b>enrolment</b>	
Password selection advice given	+1 pt
Minimum password length required	+1 pt
Dictionary words prohibited	+1 pt
Numbers or symbols required	+1 pt
User list protected from probing	+1 pt
Cleartext password sent in email after enrolment	-1 pt
<b>login</b>	
Password hashed in-browser before POST	+1 pt
Limits placed on password guessing	+1 pt
User list protected from probing	+1 pt
Federated identity login accepted	+1 pt
<b>password update</b>	
Password re-entry required to authorise update	+1 pt
Notification email sent after password reset	+1 pt
<b>password recovery</b>	
Password update required after recovery	+1 pt
Cleartext password sent in email upon request	-1 pt
User list protected from probing	+1 pt
<b>encryption</b>	
Full TLS for all password submission	+2 pts
POST only TLS for password submission	+1 pt

## More popular sites do better



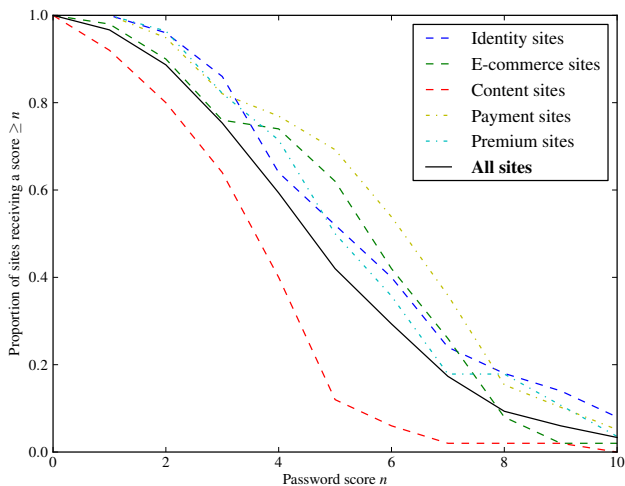
# Popular, growing, competent sites are more secure

	Password score > median	TLS deployed correctly	Guessing attacks restricted	Minimum password length enforced	Dictionary words prohibited	Cleartext passwords mailed	Notification of password reset	Email verified on enrolment	CAPTCHA required on enrolment
Positive 3-mo. traffic change	↑↑	+	↑↑↑		↑	+	+		
Years online > 10		↑↑	↓↓	+				↓	↓
Load time < med.	↑	↑	↑		↑	—	↑	↓↓↓	
Traffic Rank > 25 <sup>th</sup> %ile	↑↑↑	↑	+	+			↑↑	+	
Traffic Rank > med.	↑↑↑		↑↑	+	↑↑↑	↓	↑	+	+
Traffic Rank > 75 <sup>th</sup> %ile	↑↑↑		↑↑↑	↑	↑↑↑	↓	+	↑↑↑	↑↑
Industry Traffic Rank > 25 <sup>th</sup> %ile	↑↑↑	+	+	↑			↑	+	
Industry Traffic Rank > med.	↑↑↑	+	↑↑↑	↑↑↑	↑↑↑		↑↑		
Industry Traffic Rank > 75 <sup>th</sup> %ile	↑↑↑	↑	↑↑	↑	↑↑	—	↑↑	+	
Page Views > 25 <sup>th</sup> %ile	↑↑↑	↑↑					↑↑		
Page Views > med.	↑↑↑		↑↑	+	↑↑↑	↓	↑	+	+
Page Views > 75 <sup>th</sup> %ile	↑↑↑		↑↑↑	+	↑↑↑	↓↓	↑	↑↑	↑↑↑

# Findings

- 1 How does the user experience vary from site to site?
- 2 What implementation weaknesses exist?
- 3 Which circumstantial factors affect sites' implementation choices?
- 4 How do sites' security requirements affect their choices?**
- 5 Why do websites choose to collect passwords?

# Content sites provide the least security

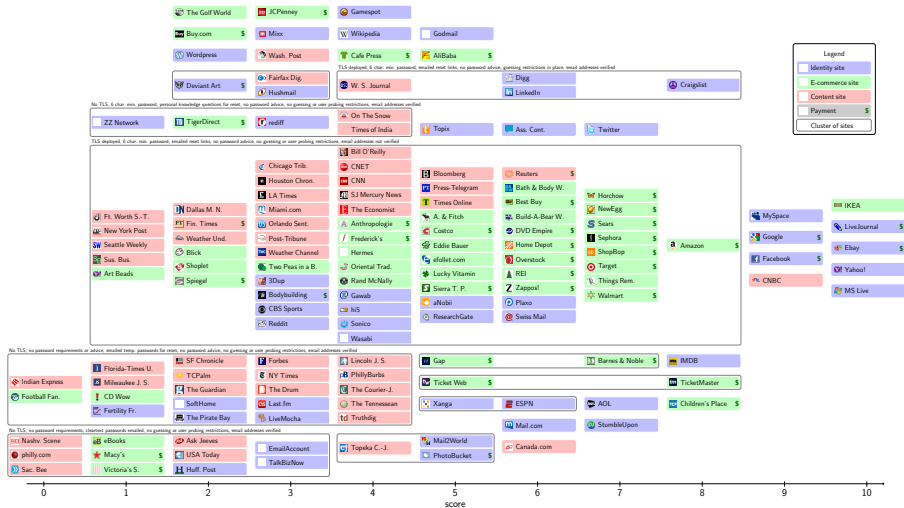




# Payment-storing sites do it best

	Password score > median	TLS deployed correctly	Guessing attacks restricted	Minimum password length enforced	Dictionary words prohibited	Digits	Symbols	Cleartext passwords mailed	Notification of password reset	Email verified on enrolment	CAPTCHA required on enrolment
Identity segment	+	↓↓	↑		↑↑↑	+	↑	↓↓		↑	↑↑↑
E-commerce segment	↑	↑↑↑			—		—		↑	↓↓↓	↓↓↓
Content segment	↓↓↓	↓↓↓	↓		↓	—		↑	↓↓	↑↑↑	—
Premium accounts offered					+			—			↑↑
Payment details stored	↑↑↑	↑↑↑	+	+		↑			↑↑↑	↓↓↓	—
E-mail provided	+					+	↑↑	—		—	↑↑↑
Social networking features		↓↓↓	↑↑	—	↑			↓		↑↑↑	↑↑

# Security policies vary far more than requirements



# Findings

- 1 How does the user experience vary from site to site?
- 2 What implementation weaknesses exist?
- 3 Which circumstantial factors affect sites' implementation choices?
- 4 How do sites' security requirements affect their choices?
- 5 Why do websites choose to collect passwords?

# Content sites want email, marketing data

## Tell Us About Yourself (Required)

Gender: ☒ Male ☐ Female

Year of Birth:  ([Click here](#) if you are under 13)

ZIP Code:

Country of Residence:

Household Income:

Job Title:

Industry:

Company Size:

New York Times

# Content sites want email, marketing data

<b>Data</b>	<b>I</b>	<b>E</b>	<b>C</b>	<b>Tot.</b>
Email address	38	50	49	<b>137</b>
Email verified	29	1	35	<b>65</b>
Email updates offered	21	42	47	<b>110</b>
Postcode	15	30	34	<b>79</b>
Mailing address	5	19	8	<b>32</b>
Phone number	5	20	7	<b>32</b>
Marketing data	4	6	13	<b>23</b>
Username	35	5	29	<b>69</b>
CAPTCHA	29	3	11	<b>43</b>

- Password over-collection is a tragedy of the commons
- Password insecurity is a negative externality

# Economic models



- Password over-collection is a tragedy of the commons
- Password insecurity is a negative externality

# Economic models



- Password over-collection is a tragedy of the commons
- Password insecurity is a negative externality



# Regulatory fixes

- Tax
- Licensing
- Liability
- Standards

# Regulatory fixes

**1040** Department of the Treasury—Internal Revenue Service **2007** OMB No. 1545-0047

**U.S. Individual Income Tax Return**

For the year Jan. 1, 2007, or other tax year beginning 2007 ending 20

**Label** See instructions on page 102. **Use the IRS label.** Otherwise, please print or type.

Your first name and initial Last name

If a joint return, spouse's first name and initial Last name

Home address (number and street). If you have a P.O. box, see page 10. Apt. no.

City, town or post office, state, and ZIP code. If you have a foreign address, see page 12.

**Your social security number**

**Spouse's social security number**

**Check here if you, or your spouse if filing jointly, want \$3 to go to this fund (see page 11).** ☐ Year ☐ Spouse

**Filing Status**

☐ Single ☐ Head of household (with qualifying person). (See page 13). If the qualifying person is a child but not your dependent, enter the child's name here. ☐ **Married filing jointly (even if only one had income)** ☐ **Married filing separately.** Enter spouse's SSN above and full name here. ☐ **Qualifying widow(er) with dependent child (see page 14).**

**Exemptions**

**a** ☐ Yourself. If someone can claim you as a dependent, do not check box 6a. **b** ☐ Spouse **c** **Dependents.** (i) First name Last name (ii) Dependent's social security number (iii) Relationship to you (or if still to be added, see page 15) **d** Total number of exemptions claimed

More than four dependents, see page 15.

**Income**

7 Wages, salaries, tips, etc. Attach Form(s) W-2 **8a** Taxable interest. Attach Schedule B if required **8b** Tax-exempt interest. Do not include on line 8a **9a** Ordinary dividends. Attach Schedule D if required **9b** Qualified dividends (see page 10). **10** Taxable refunds, credits, or offsets of state and local income taxes (see page 10). **11** Alimony received **12** Business income or (loss). Attach Schedule C or C-EZ **13** Capital gain or (loss). Attach Schedule D if required. If not required, check here **14** Other gains or (losses). Attach Form 4797 **15a** IRA distributions **15b** Taxable amount (see page 21) **16a** Pensions and annuities **16b** Taxable amount (see page 22) **17** Rental real estate, royalties, partnerships, S corporations, trusts, etc. Attach Schedule E **18** Farm income or (loss). Attach Schedule F **19** Unemployment compensation **20a** Social security benefits **20b** Taxable amount (see page 24) **21** Other income. List type and amount (see page 34). **22** Add the amounts in lines 7 through 21. This is your total income **23** Deductible expenses (see page 30) **24** Subtract the amount on line 23 from line 22. This is your adjusted gross income

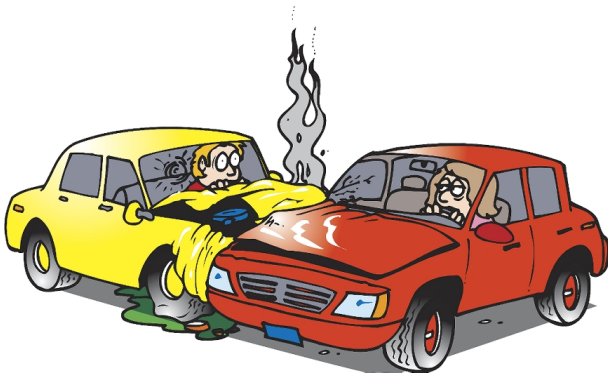
Attach to income statement of separately owned estate, trust, etc.

- Tax
- Licensing
- Liability
- Standards



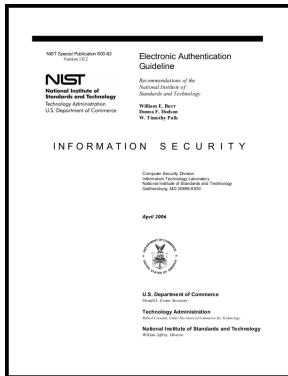
- Tax
- Licensing
- Liability
- Standards

# Regulatory fixes



- Tax
- Licensing
- Liability
- Standards

# Regulatory fixes



- Tax
- Licensing
- Liability
- Standards

## Change Your Password (optional)

A Password must be at least 6 characters or longer, and may not include blank spaces, or the characters: `<> " (A good example of a password: RUGT_7).`

New Password:

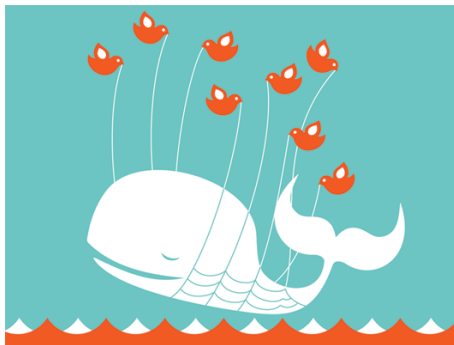
Please note passwords are case sensitive.

Confirm Password:

Costco

- It's a thicket out there
- The market is failing
- Psychological barriers may exist

# Perspectives



- It's a thicket out there
- The market is failing
- Psychological barriers may exist



- It's a thicket out there
- The market is failing
- Psychological barriers may exist



# OpenID to the rescue?

**Registering for Mixx is fast, fun, and easy!** Here at Mixx, we don't think you should have to create yet another username and password. We work with several sites that you may already use. Simply select the account you'd like your new Mixx account to work with and we'll handle the rest!



Register using your OpenID URL

Register



Mixx

# OpenID to the rescue?

## Feeling geeky?

When you log in to a website that supports OpenID login we'll send your OpenID identifier to the website so it can identify you.

To make things easy, we have generated this identifier for you:

<https://me.yahoo.com/a/OU2iCjRytdHt3TZVle>

You don't need to save this identifier. While logging in to websites, you can simply look for a Yahoo! button or type **yahoo.com** in the OpenID text field. You can also choose additional custom identifiers for your Yahoo! account below.

Yahoo!

# Questions?

jcb82@cl.cam.ac.uk  
sdp36@cl.cam.ac.uk

Data available online:

<http://preibusch.de/publ/password-market>