

Unique Security Challenges for Online Social Networks

ICT-Forward 2009
May 4, 2009

Joseph Bonneau, Computer Laboratory

Pessimistic View of Social Networks



The screenshot shows the original Thefacebook website interface. At the top, there is a header with a pixelated profile picture of Mark Zuckerberg on the left, the text "[thefacebook]" in the center, and links for "login", "register", and "about" on the right. Below the header, a left sidebar contains links for "[main]", "[login]", and "[register]". The main content area is titled "[Login]" and features two input fields for "Email:" and "Password:". Below these fields are two buttons labeled "Login" and "Register". A link is provided for users who have forgotten their password: "If you have forgotten your password, click [here](#) to reset it." At the bottom of the page, there are links for "about", "contact", "faq", "advertise", "terms", and "privacy", followed by the text "a Mark Zuckerberg production" and "Thefacebook © 2004".

Just LAMP websites where you list your friends...

The Surprising Depth of Facebook



Mike Barash Location scouting for Photography.Book.Now



3 hours ago · [Comment](#) · [Like](#) · [Share](#)



Holly Kreuter at 10:20pm April 29

You get to do all the fun stuff.



melissa hillard ▶ **Stephanie Bognuda**: even in 1997, we KNEW it was a conspiracy...



Tupac Is Alive!!!!!!!!!!!!!!!!!!!!!! | TMZ.com

Source: www.t TMZ.com

TMZ has obtained photographic evidence that Tupac Shakur is alive and well and drinking Hand Grenades in New Orleans -- unless we're terribly mistaken. ...

7 hours ago · [Comment](#) · [Like](#) · [Share](#) · [See Wall-to-Wall](#)

Highlights



Words to Live By
by Laurie Konigsberg

1 4



Wall Photos
by Becky Neil



Guns 4 Roses
3 friends are fans.
[Become a Fan](#)

Events

[See All](#)



Justin David Carl's birthday Today -

[Send a gift](#)

Cigall Kadoch's birthday Fri - [Send a gift](#)

Brittany Shehi's birthday Fri - [Send a gift](#)

Anna Quider's birthday Sat - [Send a gift](#)

Jessica Pickett's birthday Sat - [Send a gift](#)

Jenny Mackay's birthday Sat - [Send a gift](#)

Facebook Stream

The Surprising Depth of Facebook

Round ends in: **0:39**

E	E	E	T	E
L	E	A	A	W
N	S	N	R	O
P	C	T	E	S
A	A	I	I	I

Click, drag, or type to build words.

 **Rotate Board** (use spacebar as a shortcut)

End this Round

My Score:
153

My Best:
310

LEARS is worth 4

Enter

Words Remaining

3LW	74	6LW	49
4LW	105	7LW	27
5LW	96	8LW	9

Possible Score: 1466 pts

Words you've found:

- LEARS (4)
- LEAR (2)
- TARTS (4)
- TART (2)
- LEANER (6)
- LEAN (2)
- LEAT (2)

My Friends

Nan Gao
416 pts
1st

Adrienne Clark
199 pts
6th

Julie Zhuo
199 pts
7th

CURRENT SCORE
8th 153 pts

Jessica Shang
147 pts
9th

Facebook Applications

The Surprising Depth of Facebook

facebook

Connect [The Run Around](#) with Facebook to interact with your friends on this site and to share on Facebook through your Wall and friends' News Feeds. This site will also be able to automatically post recent activity back to Facebook.

Run Around


Bring your friends and info
Publish content to your Wall

facebook


Email:

Password:

By proceeding, you are allowing The Run Around to access your information and you are agreeing to the [Facebook Terms of Use](#) in your use of The Run Around. By using The Run Around, you also agree to the [The Run Around Terms of Service](#).

[Sign up for Facebook](#)[Connect](#)[Cancel](#)

Facebook Connect

Web 2.0?

Function	Internet version	Facebook version
Page Markup	HTML, JavaScript	FBML
DB Queries	SQL	FBQL
Email	SMTP	FB Mail
Forums	Usenet, etc.	FB Groups
Instant Messages	XMPP	FB Chat
News Streams	RSS	FB Stream
Authentication	OpenID	FB Connect
Photo Sharing	Flickr, etc.	FB Photos
Video Sharing	YouTube, etc.	FB Video
Blogging	Blogger, etc.	FB Notes
Microblogging	Twitter, etc.	FB Status Updates
Micropayment	Peppercoin, etc.	FB Points
Event Planning	E-Vite	FB Events
Classified Ads	craigslist	FB Marketplace

From Al Gore to Mark Zuckerberg

- ♦ Facebook has essentially re-invented the Internet
 - Simpler (mostly)
 - Centralised
 - Proprietary
 - Walled
- ♦ Killer addition is social context



Parallel Trend: The Addition of Social Context

“Given sufficient funding, all web sites expand in functionality until users can add each other as friends”



LIVEJOURNAL

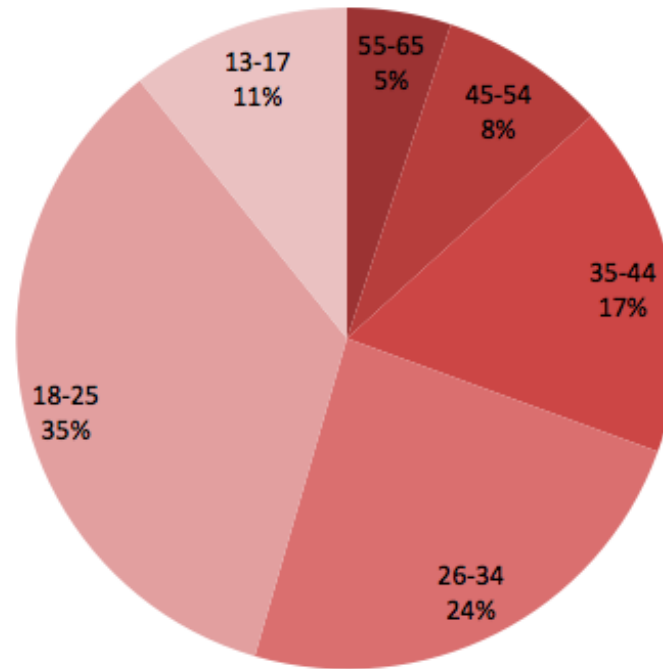


Why I Care About Social Networks

- ♦ Defining Characteristic of Generation Y (Born after 1980)
 - This generation's “Public Space” (boyd, 2007)
- ♦ American teens average 30 minutes per day
 - Also this generation's TV
- ♦ I was a Facebook early adopter in 2004

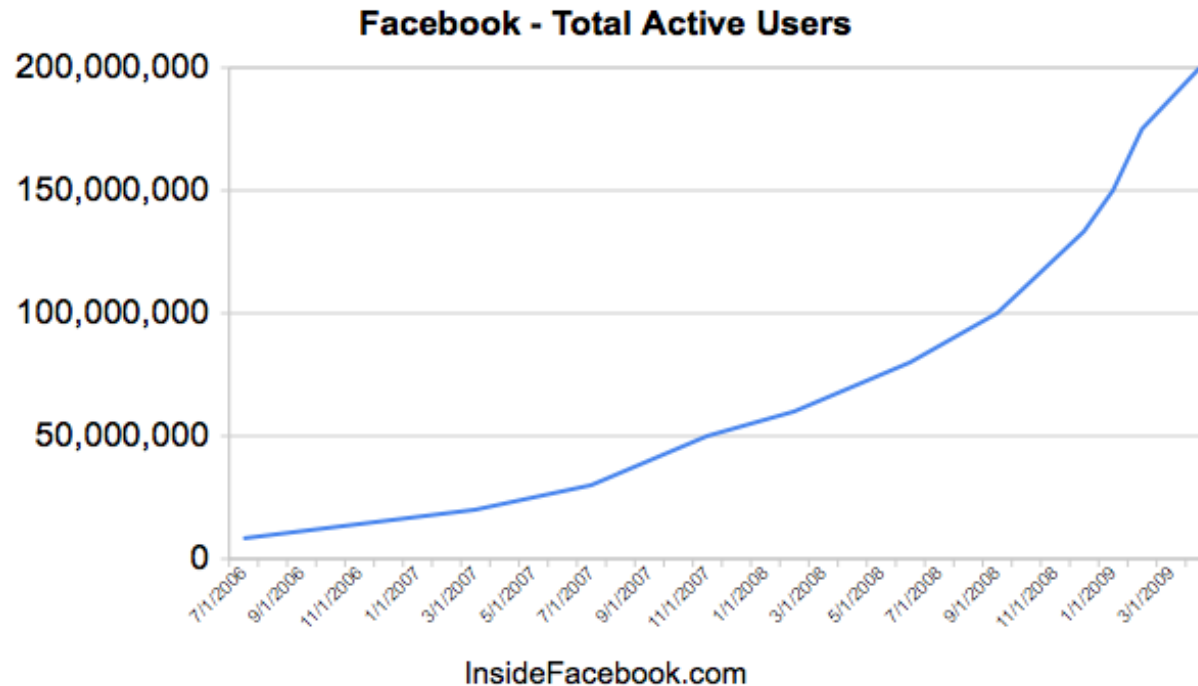
Why I Care About Social Networks

US Facebook Users by Age Group (3/25/09)
(InsideFacebook.com)



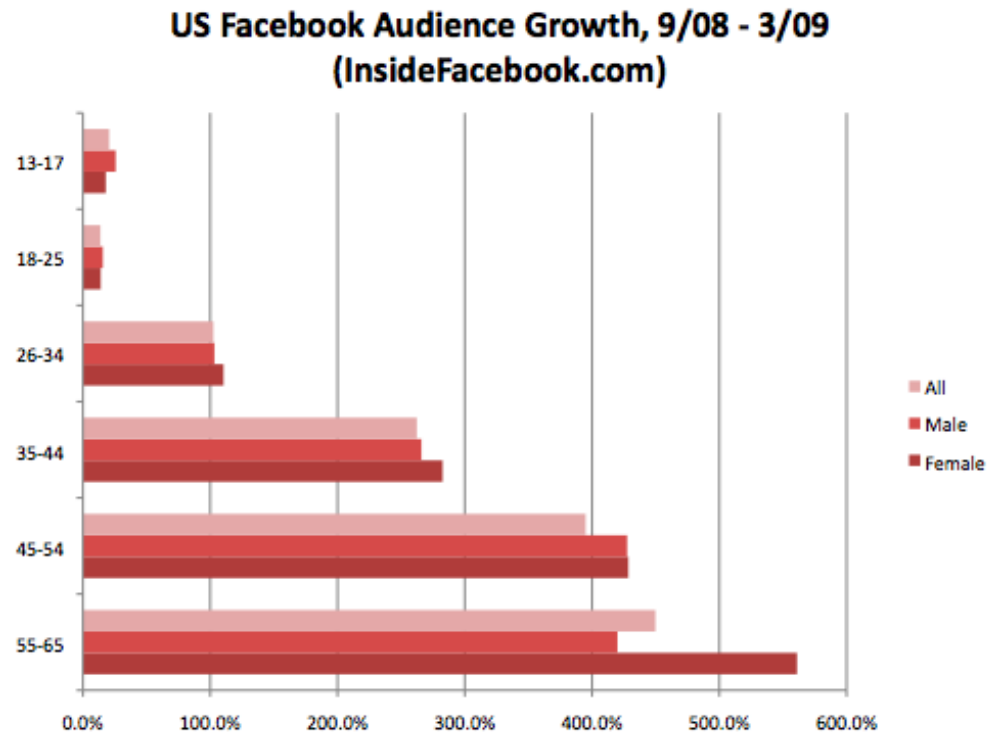
Still fairly dominated by youth

Why Everyone Will Care About Social Networks



Rapid growth

Why Everyone Will Care About Social Networks



Rapid growth in older demographics

Why Everyone Will Care About Social Networks

Country	10/8/08	3Q08 Growth	2008 Growth
United States	32,975,440	16%	94%
United Kingdom	12,410,520	9%	43%
Canada	9,324,600	-2%	7%
Turkey	4,921,980	41%	73%
Chile	3,682,680	50%	3343%
France	3,622,960	48%	183%
Australia	3,559,380	6%	52%
Colombia	3,304,600	23%	325%
Venezuela	1,591,220	48%	1061%
Italy	1,342,600	135%	460%
Sweden	1,324,060	16%	21%
Denmark	1,244,700	58%	204%
Norway	1,227,260	8%	15%
Spain	1,214,200	57%	265%
Mexico	1,168,320	6%	80%
Hong Kong	1,134,860	24%	
Argentina	1,094,780	114%	1033%
South Africa	961,720	-1%	31%
Belgium	925,600	78%	258%
Germany	860,460	24%	79%
India	794,440	3%	47%
Egypt	791,440	-1%	29%
Switzerland	701,420	67%	217%
Finland	680,780	26%	58%
Greece	663,920	28%	260%

Rapid international growth

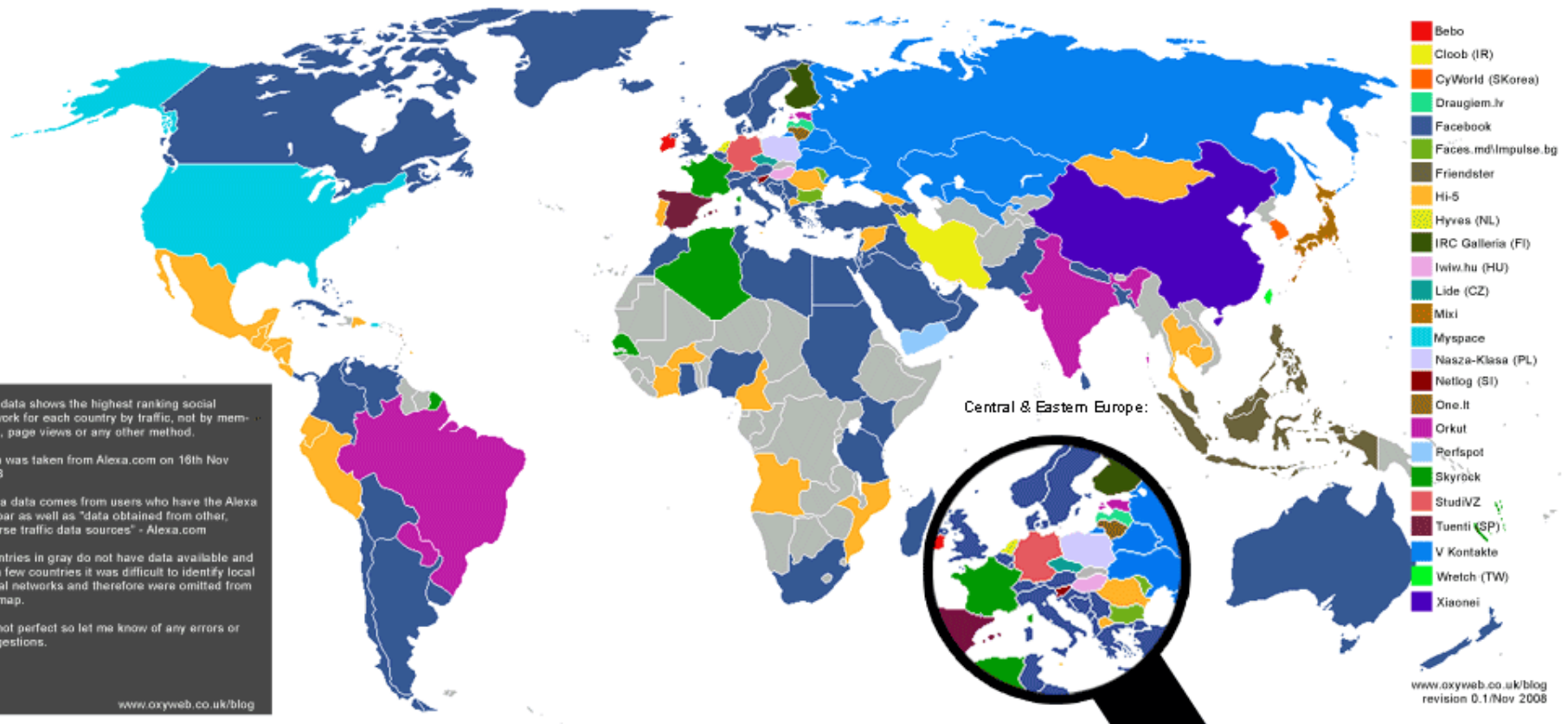
Facebook is Everywhere...



Freetown Christiania (Copenhagen, Denmark)

Facebook is Far From the Only SNS

Most popular services around the world:



Facebook is the SNS that Matters

- ♦ Dominant
 - Largest and fastest-growing
 - Most internationally successful
 - Receives most media attention
- ♦ Advanced
 - Largest feature-set
 - Most complex privacy model
 - Closest representation of real-life social world

Web 2.0?

Function	Internet version	Facebook version
Page Markup	HTML, JavaScript	FBML
DB Queries	SQL	FBQL
Email	SMTP	FB Mail
Forums	Usenet, etc.	FB Groups
Instant Messages	XMPP	FB Chat
News Streams	RSS	FB Stream
Authentication	OpenID	FB Connect
Photo Sharing	Flickr, etc.	FB Photos
Video Sharing	YouTube, etc.	FB Video
Blogging	Blogger, etc.	FB Notes
Microblogging	Twitter, etc.	FB Status Updates
Micropayment	Peppercoin, etc.	FB Points
Event Planning	E-Vite	FB Events
Classified Ads	craigslist	FB Marketplace

The Downside of Re-inventing the Internet

- ♦ SNSs repeating all of the web's security problems
 - Phishing
 - Spam
 - 419 Scams & Fraud
 - Identity Theft/Impersonation
 - Malware
 - Cross-site Scripting
 - Click-Fraud
 - Stalking, Harassment, Bullying, Blackmail
- ♦ The Elephant in the Room
 - Privacy

Differences in the SNS world

- ♦ Each has advantages and disadvantages
 - Centralisation
 - Social Connections
 - Personal Information
 - Economic Uncertainty

Security

Major Security Threats

- ♦ Account compromise
 - Email or SNS (practically the same)
- ♦ Computer compromise
- ♦ Monetary Fraud
- ♦ Service denial
 - Making the site useless

Phishing

☆ from **Facebook** <notification+f_s6a629@facebookmail.com>
reply-to noreply <noreply@facebookmail.com>
to ● Joseph Bonneau <jbonneau@gmail.com>
date Thu, Apr 30, 2009 at 12:36 AM
subject Stella Nordhagen tagged a photo of you on Facebook
mailed-by facebookmail.com
signed-by facebookmail.com

Stella tagged a photo of you in the album "Lent-ilicious!".

To see the photo, follow the link below:

<http://www.facebook.com/n/?photo.php&pid=31548385&op=1&view=all&subj=210132&id=4401279&mid=62e1b6G334d4G1d988a1G5>

Thanks,
The Facebook Team

Genuine Facebook emails

Phishing

☆ from **Facebook** <notification+f_s6a629@facebookmail.com>
reply-to noreply <noreply@facebookmail.com>
to ● Joseph Bonneau <jbonneau@gmail.com>
date Thu, Apr 30, 2009 at 3:44 PM
subject Shoshana Freisinger sent you a message on Facebook...
mailed-by facebookmail.com
signed-by facebookmail.com

Shoshana sent you a message.

Subject: Look at this!

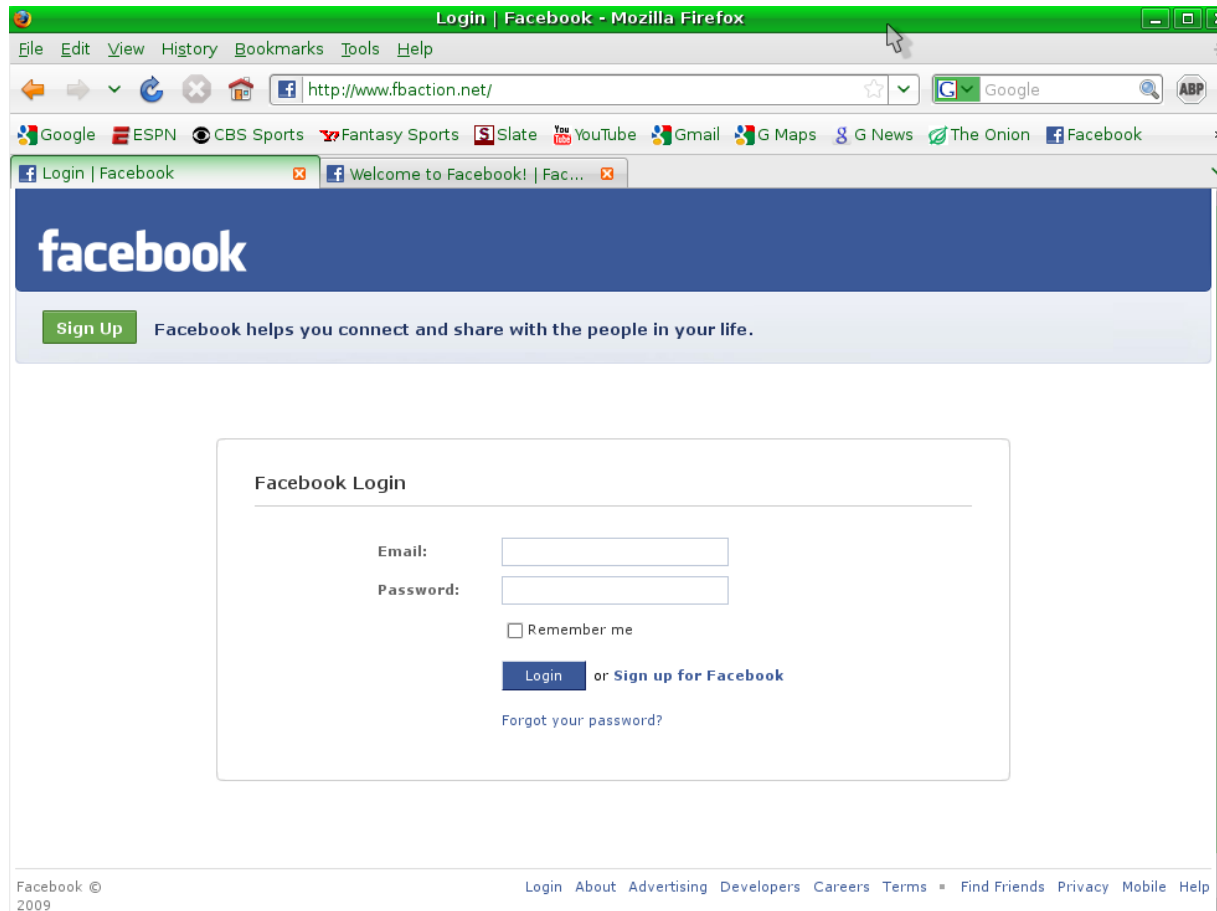
"fbstarter.com"

To reply to this message, follow the link below:

<http://www.facebook.com/n/?inbox/readmessage.php&t=1139989896147&mid=63b67eG334d4G1da651eG0>

Phishing attempt, April 30, 2009

Phishing



Phishing attempt, April 30, 2009

Phishing

- ♦ Major Phishing attempts, April 29-30, 2009
 - Simple “look at this” messages
 - Users directed to *www.fbstarter.com*, *www.fbaction.net*
 - Phished credentials used to automatically log in, send more mail
 - Some users report passwords changed
- ♦ Most “elaborate” scheme seen yet
- ♦ Phishtank reports Facebook 7th most common target
 - Behind only banks, PayPal, eBay

Why SNSs are Vulnerable to Phishing

- ♦ “Social Phishing” is far more effective
 - 72% successful in controlled study (Jagatic et al.)
- ♦ No TLS for login page
- ♦ No anti-phishing measures
- ♦ Frequent genuine emails with login-links
- ♦ Users don't consider SNS password as valuable
- ♦ Web 2.0 sites encourage password sharing...

Password Sharing

facebook

Connect [The Run Around](#) with Facebook to interact with your friends on this site and to share on Facebook through your Wall and friends' News Feeds. This site will also be able to automatically post recent activity back to Facebook.



Email:

Password:

By proceeding, you are allowing The Run Around to access your information and you are agreeing to the [Facebook Terms of Use](#) in your use of The Run Around. By using The Run Around, you also agree to the [The Run Around Terms of Service](#).

[Sign up for Facebook](#)

[Connect](#)

[Cancel](#)

Invite Your Friends



Web Email (Hotmail, Gmail, Yahoo, etc.)

Invite contacts from your email account.

Your
Email:

Password:

[Find Your Friends](#)

We won't store your password or contact anyone without your permission.



Find People You Email

Searching your email account is the fastest and most effective way to find your friends on Facebook.

Your Email:

Password:

[Find Friends](#)

We won't store your password or contact anyone without your permission.

✓ **Valid webmail address**

[Upload Contact File](#)



Find People You IM

Find out which of your AOL Instant Messenger or Windows Live Messenger buddies are on Facebook.

[Import AIM Buddy List »](#)

[Import Windows Live Contacts »](#)

SNS Phishing Defense

- ♦ Many advantages over email phishing prevention
 - Real-time monitoring
 - Can block, revoke messages
 - Block outgoing links
- ♦ Fast response to recent attacks
 - Emails blocked, removed, sites down within 24 hours

Malware

☆ from **Facebook** <notification+f_s6a629@facebookmail.com>
reply-to noreply <noreply@facebookmail.com>
to ● Joseph Bonneau <jbonneau@gmail.com>
date Fri, Dec 5, 2008 at 5:08 PM
subject Katie Gunst sent you a message on Facebook..
mailed-by facebookmail.com

Katie sent you a message.

Subject: Nice ass! But why you put them in the internet?

"YAYYYYYY

[http://www.facebook.com/l.php?u=http://geocities.com%2Frubingallegos09%2F%3Fdchbb850%3D13191be140046e6d498e1ac0d07d218c"](http://www.facebook.com/l.php?u=http://geocities.com%2Frubingallegos09%2F%3Fdchbb850%3D13191be140046e6d498e1ac0d07d218c)

Koobface worm, launched August 2008

Malware



Koobface worm, launched August 2008

Malware

- ♦ Koobface worm, launched August 2008
 - Harvest Facebook accounts
 - Spreads through Facebook messages
- ♦ Similar to Phishing
 - Rapid spread via social context
 - SNS can use social context to detect
 - Also, warn users leaving site

Malware Defense

Be careful


For the safety and privacy of your Facebook account, remember to never enter your password unless you're on the real Facebook web site. Also be sure to only download software from sites you trust

<http://geocities.com/rubingallegos09/?dchbb850=13191be140046e6d498e1ac0d07d218c>

Continue

Cancel

Malware Defense

 External Link Alert


You are about to leave MySpace.com

In an effort to stop phishing, we are warning you:
DO NOT ENTER YOUR MYSPACE PASSWORD on this new website!

This warning does not mean that there is anything dangerous about the website you are about to visit. It is just a warning not to enter your MySpace password there, even if it looks like a MySpace login page.

Follow External Link To: http://www.dizzspace.com/signup/friend_r_andagirl/

[Tom's Blog about Phishing](#) [Tom's Blog about this Warning Page](#)

 [Go Back to MySpace](#)

☐ Don't show me this alert again.



Scams

Attention all Facebook members.

Facebook is recently becoming very overpopulated,
There have been many members complaining that Facebook
is becoming very slow. Record shows that the reason is
that there are too many non-active Facebook members
And on the other side too many new Facebook members.
We will be sending this messages around to see if the
Members are active or not, If you're active please send
to 15 other users using Copy+Paste to show that you are active
Those who do not send this message within 2 weeks,
The user will be deleted without hesitation to create more space,
If Facebook is still overpopulated we kindly ask for donations but
until then send this message to all your friends and make sure you send
this message to show me that your active and not deleted.

Founder of Facebook
Mark Zuckerberg

Scams

Calvin: hey

Evan: holy moly. what's up man?

Calvin: i need your help urgently

Evan: yes sir

Calvin: am stuck here in london

Evan: stuck?

Calvin: yes i came here for a vacation

Calvin: on my process coming back home i was robbed inside the hotel i logged in

Evan: ok so what do you need

Calvin: can you loan me \$900 to get a return ticket back home and pay my hotel bills

Evan: how do you want me to loan it to you?

Calvin: you can have the money send via western union


Scams

- ♦ Effective due to social context
 - Skilled impersonators should be able to do much better
- ♦ Not much can be done to prevent
 - Education
- ♦ Again, build detection system using social context, history
 - Unexpected log-ins
 - References to Western Union, etc.

Spam

- ♦ Major factor in the decline of MySpace, Friendster
- ♦ Attractive target
 - Can message any user in the system
 - “Social Spam” much more effective than random spam
 - Account creation is very cheap

Spam

From:	Psychic - Alex Silver  Alex Silver California Psychic
Date:	Apr 29 11:35 PM
Subject:	Psychic Stimulus Package
Body:	<p style="text-align: center;">Psychic Stimulus Package Alex Silver <u>VISIT MY SITE</u></p> <p>For a limited time I am offering an introductory offer to all new clients. Get a 15 minute live psychic reading online and YOU SET THE PRICE. Pay whatever you can afford or feel is fair.</p> <p>This is a good way to save some money and also get to know me, see what I can do and to get answers to your pressing psychic questions.</p> <p>Use the PayPal BUY NOW button below and enter any amount that feels right to you. Once you have completed the payment process you will be redirected and your psychic reading will take place with me in the chat box on your left.</p>



Spam

- ♦ Many advantages for SNS
 - Global monitoring, blocking
 - Automatically detect spammer profiles
 - Analyse link history
 - Analyse graph structure
 - Analyse profile
- ♦ Aggressively request CAPTCHAs
- ♦ Legal: Facebook won US \$873 M award

Spam

- ♦ Tough question: Spam vs. Viral Promotion?
- ♦ Facebook moving to two-classes of user:
 - User profiles bound to represent “real people”
 - Limits on friend count
 - Limits on usernames
 - Limits on messages
 - “Pages” for celebrities, companies, bands, charities, etc.
 - Most limits removed
 - Subject to stricter control

Common Trends

- ♦ Social channels increase susceptibility
 - Personal information also aids greatly in targeted attacks
- ♦ Fundamental issue: SNS environment leads to carelessness
 - Rapid, erratic browsing
 - Fun, noisy, unpredictable environment
 - People use SNS with their brain turned off

Common Trends

- Centralisation helps in prevention
 - Complete control of messaging platform, blocking, revocation
- Social Context also useful
 - Can develop strong IDS

Privacy



Data of Interest

- ♦ Profile Data
 - Loads of PII (contact info, address, DOB)
 - Tastes, preferences
- ♦ Graph Data
 - Friendship connections
 - Common group membership
 - Communication patterns
- ♦ Activity Data
 - Time, frequency of log-in, typical behavior

Interested Parties

- ♦ Data Aggregation
 - Marketers, Insurers, Credit Ratings Agencies, Intelligence, etc.
 - SNS operator implicitly included
 - Often, graph information is more important than profiles
- ♦ Targeted Data Leaks
 - Employers, Universities, Fraudsters, Local Police, Friends, etc.
 - Usually care about profile data and photos

Major Privacy Problems

- ♦ Complicated privacy model
 - Settings confusing and open by default
- ♦ Implementation errors
 - Frequently unable to enforce model
- ♦ Economic pressure
 - SNS needs data sharing to grow and profit

Complicated Privacy Model

- ♦ Facebook has over 60 settings on 7 pages
 - 90% of users don't edit
- ♦ Open by default
- ♦ Many settings have unexpected interactions

Privacy Settings Confusion

enable photo tagging:

☒ yes

- People can tag my photos with their friends
- My friends can tag me in photos
- People can see a list of photos I am tagged in

Orkut Photo Tagging

Privacy Settings Confusion

Facebook Connect Applications

Facebook Connect is a way to use applications outside of Facebook. You can take your Facebook profile information all over the Internet, and send interesting information back to your Facebook account.

When your friend connects their Facebook account with an application outside of Facebook, they will be able to compare their Facebook Friend List with information from that website in order to invite more friends to connect.

☐ Don't allow friends to view my memberships on other websites through Facebook Connect.

Facebook Connect

Implementation errors

- ♦ Extreme complexity
 - Especially with third-party applications and sites
 - Many moving parts written by different teams
- ♦ Extreme size
 - Content must be stored in third-party CDNs
- ♦ Sites built rapidly with privacy as an after-thought
- ♦ Long history of privacy-related bugs

Implementation errors

Facebook Markup Language

```
<fb:swf swfsrc="http://myserver/flash.swf"  
imgsrc="http://myserver/image.jpg" imgstyle="-moz-  
binding:url(\'http://myserver/xssmoz.xml#xss\');" />
```

Translated into HTML:

```

```

Result: arbitrary JavaScript execution (Felt, 2007)

Implementation errors

User ID

210132

Response Format

XML

Callback

Method (Documentation)

fql.query

query

select uid1, uid2 from friend where uid1 in (1, 2, 3, 4, 5) and uid2 in (1, 2, 3, 4, 5)

Call Method

\$facebook->api_client->fql_query('select uid1, uid2 from friend where uid1 in (1, 2, 3, 4, 5) and uid2 in (1, 2, 3, 4, 5)');

<?xml version="1.0" encoding="UTF-8"?>
<fql_query_response xmlns="http://api.facebook.com/1.0/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
 <friend_info>
 <uid1>4</uid1>
 <uid2>5</uid2>
 </friend_info>
 <friend_info>
 <uid1>5</uid1>
 <uid2>4</uid2>
 </friend_info>
</fql_query_response>

Facebook Query Language Exploits (Bonneau, Anderson, Danezis, 2009)

Implementation errors

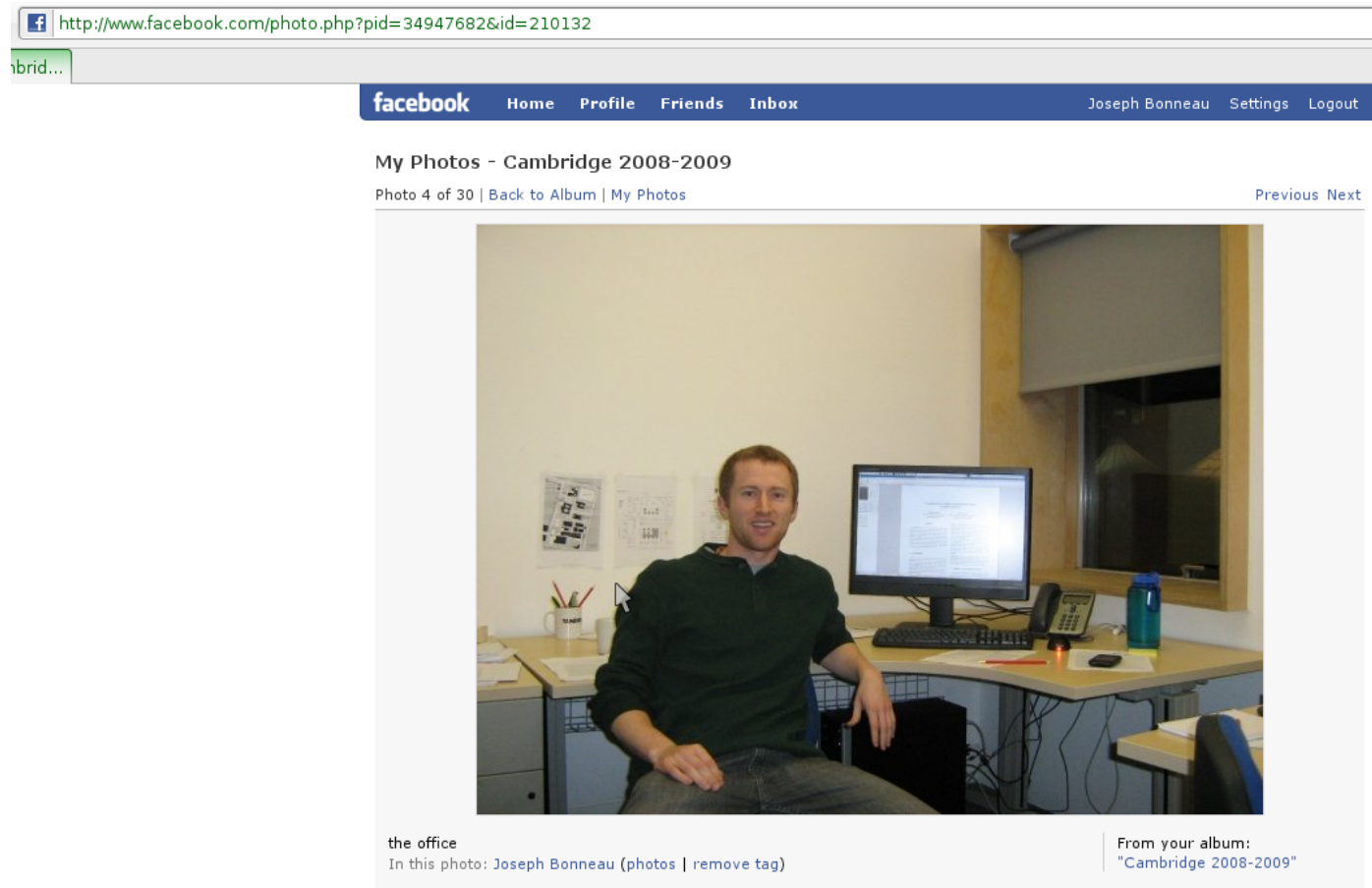


Photo Exploits: PHP parameter fiddling (Ng, 2008)

Implementation errors



Photo Exploits: Content Delivery Network URL fiddling (Bonneau, 2009)

Economic Pressure

- ♦ Most SNSs still lose money
 - Advertising business model yet to prove its viability
- ♦ Grow first, monetize later
 - “Growth is primary, revenue is secondary” - Mark Zuckerberg
- ♦ Privacy is often an impediment to new features
 - Facebook Beacon
 - News feed
 - Site re-designs

Application Security

Allow Access?

Allowing [Scramble](#) access will let it pull your profile information, photos, your friends' info, and other content that it requires to work.

 **Allow** or [cancel](#)

By proceeding, you are allowing Scramble to access your information and you are agreeing to the [Facebook Terms of Use](#) in your use of Scramble.

- Applications given full access to profile data of installed users
- Even less revenue available for application developers...

Public Listings

facebook

☐ Remember Me

Forgotten your password?

E-mail address

Log in

Sign Up

Sign up for Facebook to connect with Joseph Bonneau.



Not the right Joseph Bonneau you were looking for? [Search more](#)

Joseph Bonneau
[Add as Friend](#) | [Send a Message](#) | [View Friends](#)
Here are some of **Joseph Bonneau's** friends:


David Cottingham


Emma Alden


Aisling Byrne


Stella Nordhagen


David J Hornsby


Jillian Sullivan


Pedro Alejandro Ortega


Eirik George Tsarpalis

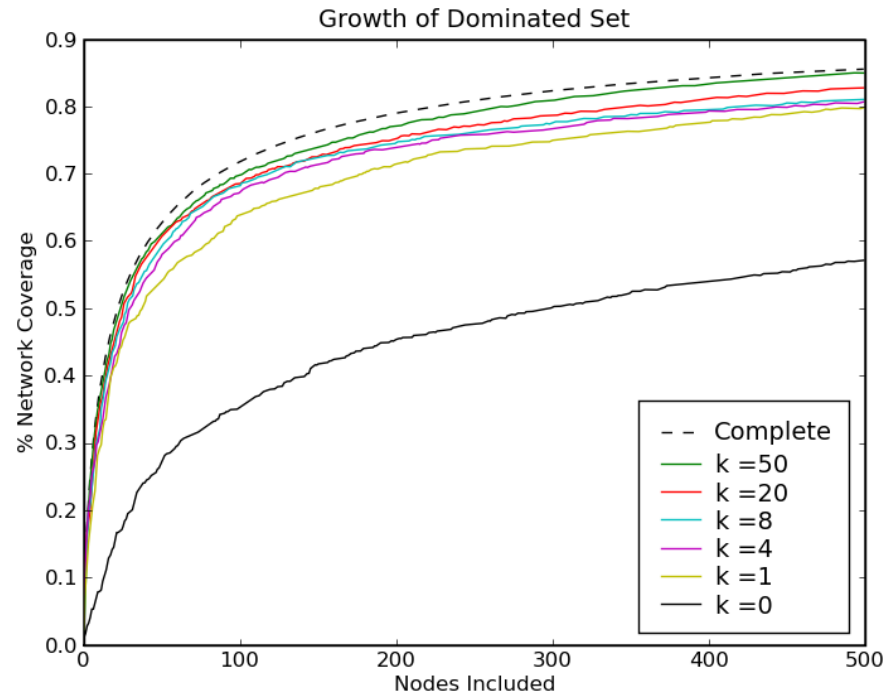
Joseph Bonneau is on Facebook.
[Sign up for Facebook](#) to connect with Joseph Bonneau.

Sign Up

It's free and anyone can join. Already a Member? [Log in](#) [menghubungi Joseph Bonneau](#)

Facebook © 2009 English (UK) [Log in](#) [About](#) [Advertising](#) [Developers](#) [Jobs](#) [Terms](#) [Find Friends](#) [Privacy](#) [Help](#)

Public Listings



Public Listings provide enough graph data to approximate most functions
(Bonneau, Anderson, Stajano, Anderson, 2009)

Terms of Service

Terms of Service, hi5:

We provide your Personal Information to third party service providers who work on behalf of or with hi5 under confidentiality agreements to provide some of the services and features of the hi5 community and to help us communicate with hi5 Members. These service providers may use your personal information to communicate with you about offers and services from hi5 and our marketing partners. However, these service providers do not have any independent right to share this information.

If you decide to use one of the additional services that are offered by our partners, we may forward Personal Information to these partners to enable them to provide the services that you requested.

We also provide information to third-party advertising companies, as described in the next section.

Please be aware that the handling of your Personal Information by our partners or the third-party advertising companies is governed by their privacy policy, not ours.

Most Terms of Service reserve broad rights to user data

Market Dynamics

- ♦ Sites avoid competing on privacy as a selling point
- ♦ Significant lock-in
- ♦ Enormous Network effects
- ♦ Privacy rarely mentioned during sign-up
 - Privacy salience reduces enjoyment of site
- ♦ Users can't determine which sites are better
 - Lemons market

Conclusions

- Social Networking coming to dominate the web
- Makes malicious behaviour more enticing
- Also aids prevention
- Privacy is still a mess

Questions?

Publications

- *Democracy Theatre: Commentary on Facebook's Proposed Governance Scheme*. Joseph Bonneau, Sören Preibusch, Jonathan Anderson, Richard Clayton, Ross Anderson. Public report, 2009.
- Eight Friends are Enough: Social Graph Approximation via Public Listings. Joseph Bonneau, Jonathan Anderson, Frank Stajano, Ross Anderson. *The Second ACM Workshop on Social Network Systems*, 2009
- The Jungle: A Field Study into the Market for Privacy in Social Networks. Joseph Bonneau, Sören Preibusch. *WEIS 2009: The Eighth Workshop on the Economics of Information Security*, 2009.
- Prying the Social Graph out of a Social Network. Joseph Bonneau, Jonathan Anderson, George Danezis. *ASONAM 2009: The 2009 International Conference on Social Network Analysis and Mining*, 2009.
- Privacy Preserving Social Networking Over Untrusted Networks. Jonathan Anderson, Joseph Bonneau, Claudia Diaz, Frank Stajano. *WOSN 2009: The Second ACM SIGCOMM Workshop on Online Social Networks*, 2009.
- And several hacks on www.lightbluetouchpaper.org