Why I’m not (yet) Friends with Facebook

David Aspinall

LFCS

28th April 2009

Statistics

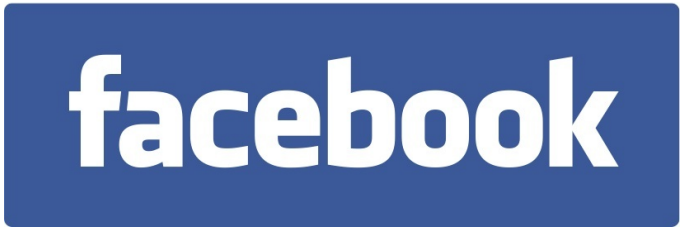
Growth
- 200 million active users
  04.07: 20m, 10.07: 50m, 09.08: 100m
- 100 million users log on/day

Users
- Average user has 120 friends on the site
- 3.5 billion minutes/day are spent
- 20 million users their statuses daily

Apps
- 850 million photos uploaded/month
- 8 million videos uploaded/ month

I18n
- 40 translations, 50 in development
- 70% of users outside the United States

Platform
- 660k developers; 52k applications
- 5k apps have 10k active users/month



See http://www.facebook.com/press/info.php?statistics

Outline

It’s about the privacy...

Facebook Security Timeline Sampler

03.2005 personal data freely downloadable

Facebook Security Timeline Sampler

03.2005 personal data freely downloadable

09.2006 move to open-door; News Feed aggregation

Facebook Security Timeline Sampler

03.2005 personal data freely downloadable

09.2006 move to open-door; News Feed aggregation

05.2007 introduction of Facebook/f8 app platform

Facebook Security Timeline Sampler

- 03.2005 personal data freely downloadable
- 09.2006 move to open-door; News Feed aggregation
- 05.2007 introduction of Facebook/f8 app platform
- 06.2007 privacy settings & search inconsistency

Facebook Security Timeline Sampler

03.2005	personal data freely downloadable
09.2006	move to open-door; News Feed aggregation
05.2007	introduction of Facebook/f8 app platform
06.2007	privacy settings & search inconsistency
08.2007	PHP source spontaneously appears on site

Facebook Security Timeline Sampler

03.2005 personal data freely downloadable

09.2006 move to open-door; News Feed aggregation

05.2007 introduction of Facebook/f8 app platform

06.2007 privacy settings & search inconsistency

08.2007 PHP source spontaneously appears on site

09.2007 *public seach listings made available*

Facebook Security Timeline Sampler

03.2005 personal data freely downloadable

09.2006 move to open-door; News Feed aggregation

05.2007 introduction of Facebook/f8 app platform

06.2007 privacy settings & search inconsistency

08.2007 PHP source spontaneously appears on site

09.2007 *public seach listings made available*

11.2007 *Beacon Social Ads publish purchase details*

Facebook Security Timeline Sampler

03.2005 personal data freely downloadable

09.2006 move to open-door; News Feed aggregation

05.2007 introduction of Facebook/f8 app platform

06.2007 privacy settings & search inconsistency

08.2007 PHP source spontaneously appears on site

09.2007 *public seach listings made available*

11.2007 *Beacon Social Ads publish purchase details*

02.2008 *profile deletion policy relaxed*

Facebook Security Timeline Sampler

03.2005 personal data freely downloadable

09.2006 move to open-door; News Feed aggregation

05.2007 introduction of Facebook/f8 app platform

06.2007 privacy settings & search inconsistency

08.2007 PHP source spontaneously appears on site

09.2007 *public seach listings made available*

11.2007 *Beacon Social Ads publish purchase details*

02.2008 *profile deletion policy relaxed*

03.2008 URL guessing can download private photos

Facebook Security Timeline Sampler

03.2005 personal data freely downloadable

09.2006 move to open-door; News Feed aggregation

05.2007 introduction of Facebook/f8 app platform

06.2007 privacy settings & search inconsistency

08.2007 PHP source spontaneously appears on site

09.2007 *public seach listings made available*

11.2007 *Beacon Social Ads publish purchase details*

02.2008 *profile deletion policy relaxed*

03.2008 URL guessing can download private photos

05.2008 BBC points out malicious apps vulnerability

Facebook Security Timeline Sampler

03.2005	personal data freely downloadable
09.2006	move to open-door; News Feed aggregation
05.2007	introduction of Facebook/f8 app platform
06.2007	privacy settings & search inconsistency
08.2007	PHP source spontaneously appears on site
09.2007	*public seach listings made available*
11.2007	*Beacon Social Ads publish purchase details*
02.2008	*profile deletion policy relaxed*
03.2008	URL guessing can download private photos
05.2008	BBC points out malicious apps vulnerability
08.2008	session stealing via scripting vulnerability

Facebook Security Timeline Sampler

03.2005 personal data freely downloadable

09.2006 move to open-door; News Feed aggregation

05.2007 introduction of Facebook/f8 app platform

06.2007 privacy settings & search inconsistency

08.2007 PHP source spontaneously appears on site

09.2007 *public seach listings made available*

11.2007 *Beacon Social Ads publish purchase details*

02.2008 *profile deletion policy relaxed*

03.2008 URL guessing can download private photos

05.2008 BBC points out malicious apps vulnerability

08.2008 session stealing via scripting vulnerability

02-04.2009 Ts&Cs controversy, “Democracy Theatre”

Facebook Security Timeline Sampler

03.2005 personal data freely downloadable

09.2006 move to open-door; News Feed aggregation

05.2007 introduction of Facebook/f8 app platform

06.2007 privacy settings & search inconsistency

08.2007 PHP source spontaneously appears on site

09.2007 *public seach listings made available*

11.2007 *Beacon Social Ads publish purchase details*

02.2008 *profile deletion policy relaxed*

03.2008 URL guessing can download private photos

05.2008 BBC points out malicious apps vulnerability

08.2008 session stealing via scripting vulnerability

02-04.2009 Ts&Cs controversy, “Democracy Theatre”

Outline

Social Phishing

Risky friends

- 87 of the 200 Facebook users contacted responded to Freddi, a plastic green frog.
- 82 (41%) leaked personal information
- “Curiously [...] very few wanted to engage in casual poking, suggesting that [...] Facebook users are primarily interested in commitment and friendship”
- See: Sophos Security Thread Report 2009.

Identity theft scams

Name: Brian Rutberg
Location: Seattle
Employer: Microsoft
Status:
BRYAN IS IN URGENT NEED OF HELP!!!

- Rutberg was locked out of his Facebook account

Identity theft scams

Name: Brian Rutberg
Location: Seattle
Employer: Microsoft
Status:

BRYAN IS IN URGENT NEED OF HELP!!!

- Rutberg was locked out of his Facebook account
- His friends received e-mail saying he had been robbed at gunpoint while traveling in the UK

Identity theft scams

Name: Brian Rutberg
Location: Seattle
Employer: Microsoft
Status:

BRYAN IS IN URGENT NEED OF HELP!!!

- Rutberg was locked out of his Facebook account
- His friends received e-mail saying he had been robbed at gunpoint while traveling in the UK
- No way to reach Facebook

Identity theft scams

Name: Brian Rutberg
Location: Seattle
Employer: Microsoft
Status:

BRYAN IS IN URGENT NEED OF HELP!!!

- Rutberg was locked out of his Facebook account
- His friends received e-mail saying he had been robbed at gunpoint while traveling in the UK
- No way to reach Facebook
- Wanted to put a message on his wife's wall but she had been de-friended

Identity theft scams

Name: Brian Rutberg
Location: Seattle
Employer: Microsoft
Status:

BRYAN IS IN URGENT NEED OF HELP!!!

- Rutberg was locked out of his Facebook account
- His friends received e-mail saying he had been robbed at gunpoint while traveling in the UK
- No way to reach Facebook
- Wanted to put a message on his wife's wall but she had been de-friended
- No out-of-Facebook way to contact many friends

Identity theft scams

Name: Brian Rutberg
Location: Seattle
Employer: Microsoft
Status:

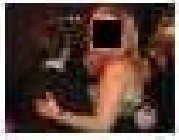
BRYAN IS IN URGENT NEED OF HELP!!!

- Rutberg was locked out of his Facebook account
- His friends received e-mail saying he had been robbed at gunpoint while traveling in the UK
- No way to reach Facebook
- Wanted to put a message on his wife's wall but she had been de-friended
- No out-of-Facebook way to contact many friends
- One sent $1,200 to a Western Union branch in London

Chatting with scammers

Bryan Rutberg
January 21 at 7:07pm

Sorry, the internet connection here sucks and I keep getting kicked out. Well I had to visit a resort here in London for vacation and I got robbed at the hotel i'm staying...Can you help?



Caroli... ...
S
January 21 at 7:08pm

how can I help you? what about Am Ex or the hotel? Not sure what I can do from here...did you call your wife?

Bryan Rutberg
January 21 at 7:30pm

Can you just get some money to us to complete our ticket fee, I tried AMEX and its not going through online and the hotel is just allowing us to stay for free till when we can leave...I'll refund you back as soon as am back home...Let me know please

Bryan Rutberg
Today at 2:58pm

Carolyn - it's me, the REAL Bryan. My account was hacked - I am glad that you did not get scammed. At least one of my friends lost serious $$ to this scam. See this link http://www.techcrunch.com/2009/01/20/latest-facebook-scam-phishers-hit-up-friends-for-cash/ for info. If you want

See http://redtape.msnbc.com/2009/01/post-1.html

Outline

Identity and Authentication

Shared personal data

Challenge Questions rely on personal "*private*" information that is easily remembered.

Shared personal data

Challenge Questions rely on personal "*private*" information that is easily remembered.
Unfortunately it may be easily guessed:

- There is **gradual erosion** of personal data.
  Obtained knowledge increases over time.

  A. Rabkin. *Personal knowledge questions for fallback authentication: Security questions in the era of Facebook.* SOUPS 2008.

Shared personal data

Challenge Questions rely on personal "*private*" information that is easily remembered.
Unfortunately it may be easily guessed:

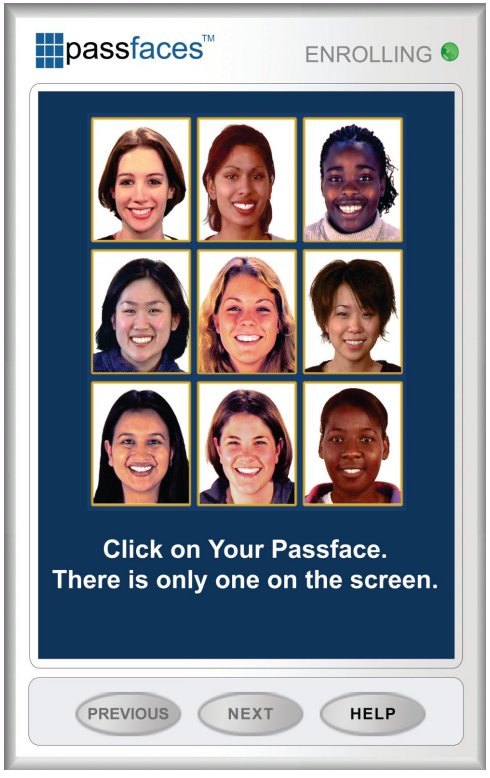
- There is **gradual erosion** of personal data. Obtained knowledge increases over time.

  A. Rabkin. *Personal knowledge questions for fallback authentication: Security questions in the era of Facebook.* SOUPS 2008.

- **User chosen questions** increase the space of available data points: users can choose information not otherwise revealed. (But mostly they don't).

  M. Just and D. Aspinall. *Choosing Better Challenge Questions*. SOUPS 2009.

From Passfaces to Face/Auth

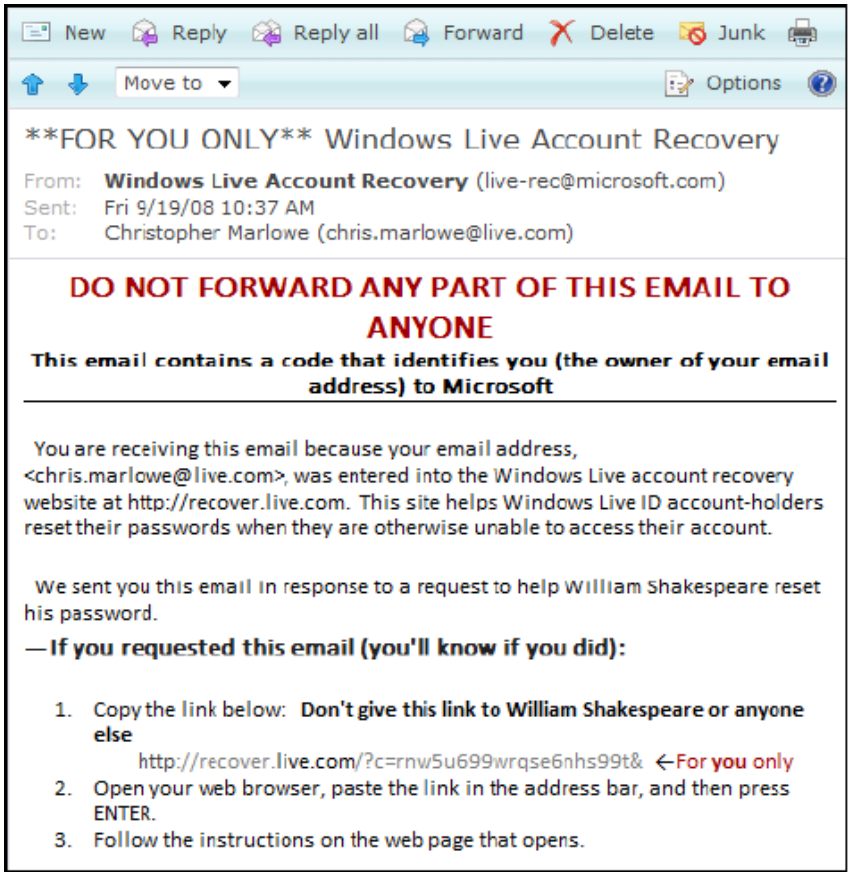


- Idea: can combine several orthogonal weak mechanisms to try to increase security.
- Risky idea: exploit aspects of Facebook data itself in usable ways.

The idea of "Face/Auth" is to implement a Facebook application which can be used to conduct authentication experiments with users to try out and compare different novel user-friendly authentication mechanisms.

MSc project, School of Informatics, 2009.

Social authentication



New Reply Reply all Forward Delete Junk

Move to Options

FOR YOU ONLY Windows Live Account Recovery

From: **Windows Live Account Recovery** (live-rec@microsoft.com)
Sent: Fri 9/19/08 10:37 AM
To: Christopher Marlowe (chris.marlowe@live.com)

DO NOT FORWARD ANY PART OF THIS EMAIL TO ANYONE

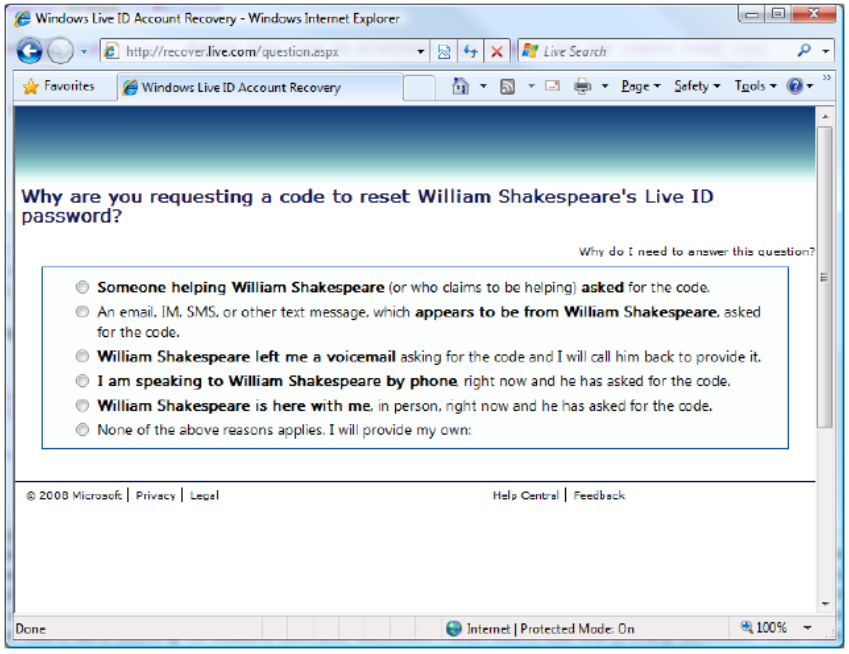
This email contains a code that identifies you (the owner of your email address) to Microsoft

You are receiving this email because your email address, <chris.marlowe@live.com>, was entered into the Windows Live account recovery website at http://recover.live.com. This site helps Windows Live ID account-holders reset their passwords when they are otherwise unable to access their account.

We sent you this email in response to a request to help William Shakespeare reset his password.

—If you requested this email (you'll know if you did):

1. Copy the link below: **Don't give this link to William Shakespeare or anyone else**
   http://recover.live.com/?c=rnw5u699wrqse6nhs99t& ←For you only
2. Open your web browser, paste the link in the address bar, and then press ENTER.
3. Follow the instructions on the web page that opens.



Windows Live ID Account Recovery - Windows Internet Explorer

http://recover.live.com/question.aspx

Favorites | Windows Live ID Account Recovery

Why are you requesting a code to reset William Shakespeare's Live ID password?

Why do I need to answer this question?

- **Someone helping William Shakespeare** (or who claims to be helping) **asked** for the code.
- An email, IM, SMS, or other text message, which **appears to be from William Shakespeare**, asked for the code.
- **William Shakespeare left me a voicemail** asking for the code and I will call him back to provide it.
- **I am speaking to William Shakespeare by phone** right now and he has asked for the code.
- **William Shakespeare is here with me**, in person, right now and he has asked for the code.
- None of the above reasons applies. I will provide my own:

© 2008 Microsoft | Privacy | Legal Help Central | Feedback

Done Internet | Protected Mode: On 100%

Schecter, Egelman and Reeder. *It's Not What You Know, But Who You Know. A social approach to last-resort authentication.* CHI 2009.

Outline

Exposing the network

Mike’s friends

facebook

Remember Me Forgotten your password?

da@dcs.ed.ac.uk Log in

Sign Up Sign up for Facebook to connect with Michael Fourman.

Not the Michael Fourman you were looking for? Search more

Michael Fourman

Add Michael Fourman as a friend | Sent Michael Fourman a message | View Michael Fourman's friends

Here are some of **Michael Fourman's** friends:


Elham Kashefi


Fernanda Ferreira


Colin Adams


Roy Dyckhoff


Rowan Carnihan


Kathryn Hays


Thorsten Altenkirch


Michelle Moran

Michael Fourman is on Facebook.

Sign up for Facebook to connect with Michael Fourman.

Sign Up

It's free and anyone can join. Already a member? Log in to contact Michael Fourman.

Facebook © 2009 English (UK) Log in About Advertising Developers Careers Terms Find Friends Privacy Mobile Help

Phil’s friends

facebook

Remember Me Forgotten your password?

Email address Log in

Sign Up Sign up for Facebook to connect with Philip Wadler.

Not the Philip Wadler you were looking for? Search more

Philip Wadler

Add Philip Wadler as a friend | Sent Philip Wadler a message | View Philip Wadler's friends

Here are some of **Philip Wadler's** friends:


Kenneth McFarlane


Viktor Ivanov


Kuragabus PumpkinPatch


Roberto Bezoari


Sanjiva Prasad


Maxim Cramer


Lavanya Jeyaratnam


Maria Milosavljevic

Philip Wadler is a fan of:

Celebrities/Public Figures

Richard Feynman
Alan Turing
Donald Ervin Knuth
Georg Cantor
George Boole

Products

Haskell
Scheme

Philip Wadler is on Facebook.

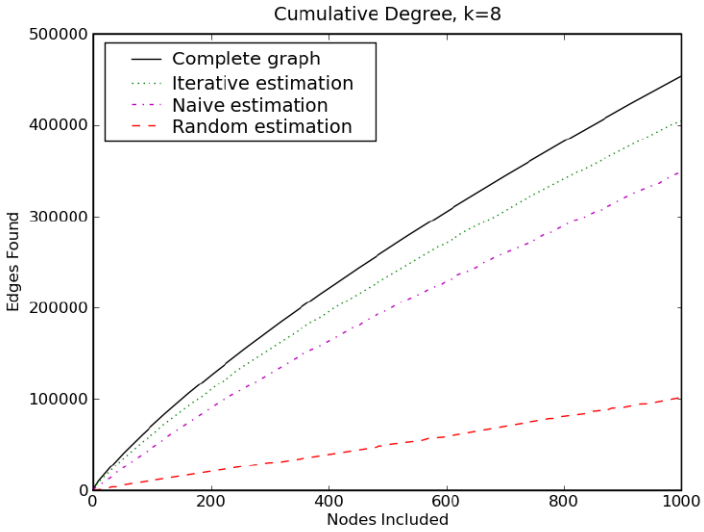
Sign up for Facebook to connect with Philip Wadler.

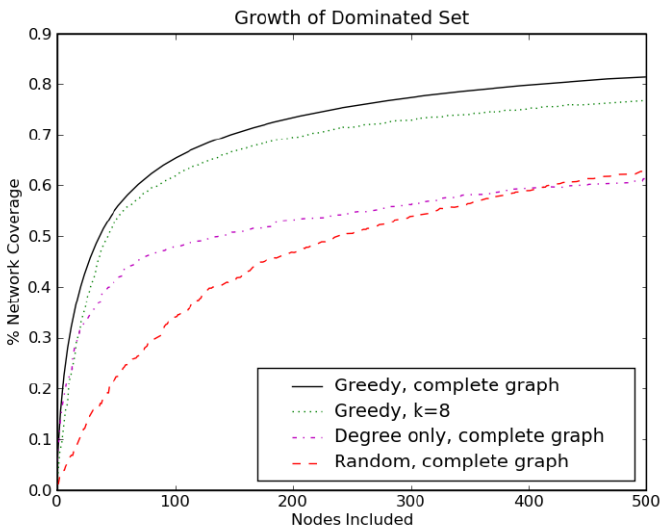
Sign Up

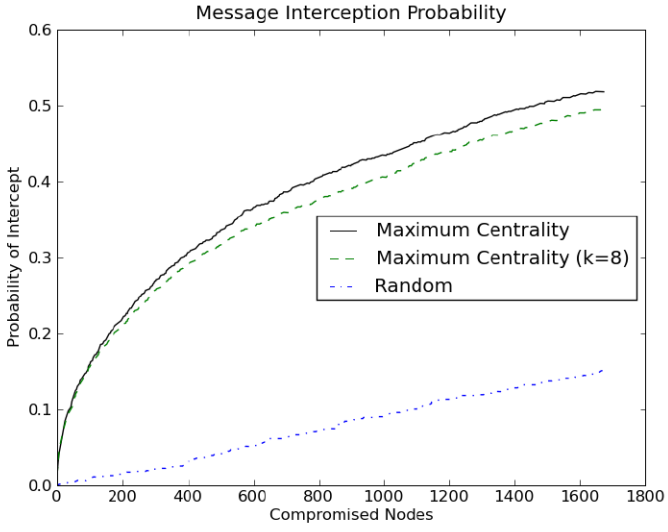
It's free and anyone can join. Already a member? Log in to contact Philip Wadler.

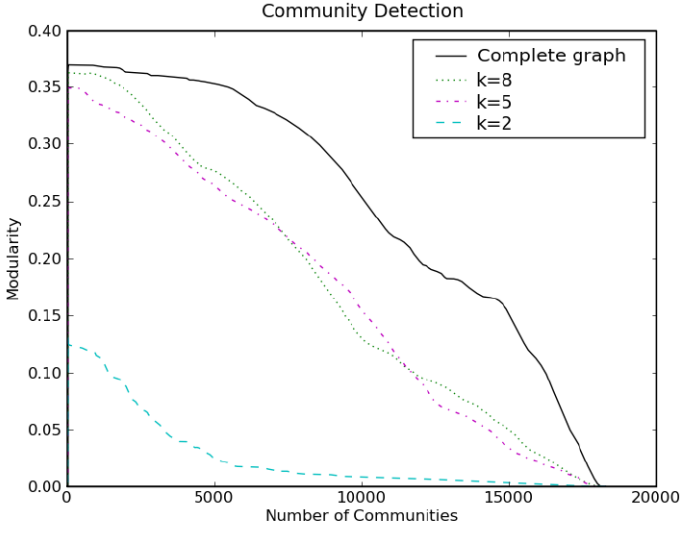
Facebook © 2009 English (UK) Log in About Advertising Developers Careers Terms Find Friends Privacy Mobile Help

Approximating social graphs









Joseph Bonneau, J. Anderson, R. Anderson, F. Stajano. *Eight Friends Are Enough: Social Graph Approximation via Public Listings* SNS 2009.

Outline

Recommendations

Recommendations

See www.allfacebook.com

10 Privacy Settings Every Facebook User Should Know

Posted by **Nick O'Neill** on February 2nd, 2009 11:00 AM

Everyday I receive an email from somebody about how their account was hacked, how a friend tagged them in the photo and they want a way to avoid it, as well as a number of other complications related to their privacy on Facebook. Over the weekend one individual contacted me to let me know that he would be removing me as a friend from Facebook because he was "going to make a shift with my Facebook use - going to just mostly family stuff."

Perhaps he was tired of receiving my status updates or perhaps he didn't want me to view photos from his personal life. Whatever the reason for ending our Facebook friendship, I figured that many people would benefit from a thorough overview on how to protect your privacy on Facebook. Below is a step by step process for protecting your privacy.

1. Use Your Friend Lists

I can't tell you how many people are not aware of their friend lists. For those not aware of what friend lists are, Facebook describes them as a feature which allows "you to create private groupings of friends based on your personal preferences. For example, you can create a Friend List for your friends that meet for weekly book club meetings. You can create Friend Lists for all of your organizational needs, allowing you to quickly view friends by type and send messages to your lists."

There are a few very important things to remember about friend lists:

- You can add each friend to more than one friend group

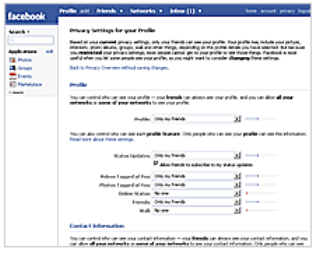
See www.sophos.com

Home › Security › Best practice › Facebook profile

Facebook best practice

Profile privacy settings

Facebook has provided users with powerful controls to protect themselves online, and it is up to individuals to check and ensure that appropriate settings are in place. Sophos has published recommendations for how to configure the settings for each of these privacy areas of Facebook.



Overview of Facebook best practice

Search settings page

Profile (edit)

Option	Sophos recommends	Why?
Profile	"Only my friends"	By default, Facebook allows all of your networks and all of your friends to be able to view your profile. As networks can contain hundreds of thousands of people (and you have no control over who else joins the network), you are instantly revealing personal information to potential identity thieves if you leave this option at its default setting. Sophos advises that it is sensible only to allow your profile to be viewed by your friends, so you should set this option to be: "Only my friends".

The next options further break down who can view different parts of your profile:

Option	Sophos recommends	Why?
Photos Tagged of You	"Only my friends"	Photos and videos should only be shared with friends, not with wider networks on Facebook. If photos and videos may be posted that you think may in the future be embarrassing to you, then tag this option to say only you can view them and ask yourself what can be done to prevent such material being uploaded onto the internet in future. If you are not comfortable with material appearing on your resume or job application then don't post it online.
Videos Tagged of You	"Only my friends"	
Status Updates	"Only my friends" (as a minimum)	As you may change your status to say "Going to hospital for surgery in three days", or "On holiday down south until September 2!" (which may be useful information for criminals) it makes sense not to make your status available to anyone other than approved friends. You should not make it viewable by your networks. Non-friends do not need to know what you are doing minute-by-minute.
Online Status	"No one"	There is no benefit in non-friends knowing whether you are currently logged into Facebook or not. It is sensible to set

Schneier on Privacy

I certainly don't believe that my SMSes, any of my telephone data, or anything I say on LiveJournal or Facebook – regardless of the privacy settings – is private.

Bruce Schneier, Wired, 26.03.09