Why Do Hackers Want Your Facebook Data

Late in 2011, Max Schrems asked Facebook for a profile the social networking company assembled based on his posts, likes and friends. Max received a 1200 page PDF file with lots of personal details. Being a law student, understandably, Max examined the information from a privacy perspective. But what about security? We examined the content from Max's report and asked:

- What Facebook data do hackers find interesting?
- How can hackers go about and obtain that data?

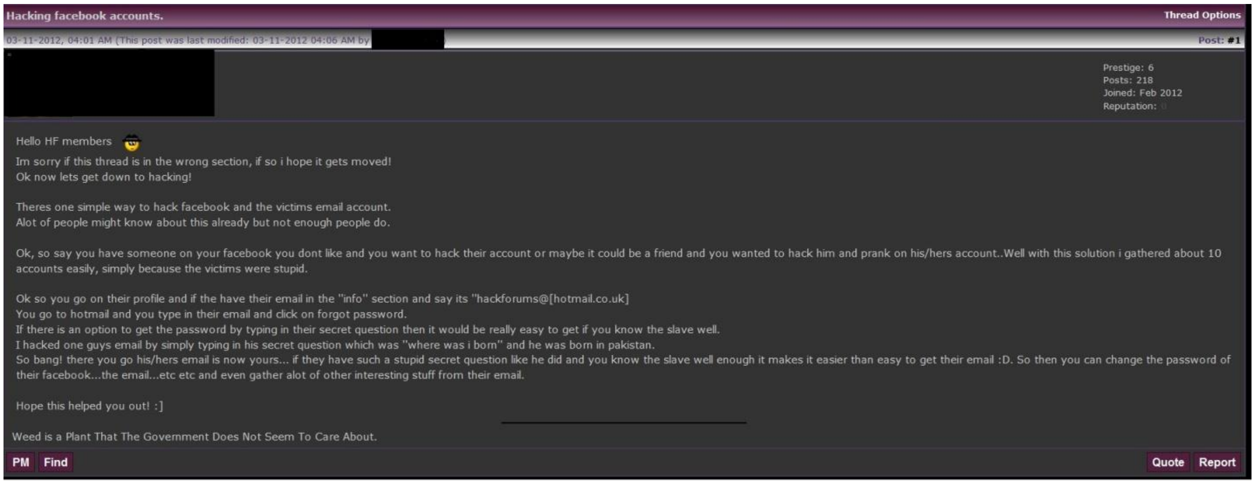
In the first of this two-part series we'll tackle each question respectively. But before we do, some background on personal information and social media:

- **Facebook contains much more data than most people realize**. Again, Max Schrems got a 1200 page document from Facebook. Max noted that the document contained not just a lot information about him—but on his friends as well.
- **Not all of the user's private data is directly accessible to the user**. Although some of the information is accessible via the application (a user can view their pictures, wall, and so forth), some of the data is not as accessible. For instance, dynamic data (such as unsaved chat logs) or geo info (such as IP addresses) are not typically retrieved. These are the things that Max, an EU citizen, requested to receive. Facebook, complying with EU regulations, obliged Max with all of his "inaccessible" data.
- **The issue is not confined to Facebook alone**. Webmail apps, for example, hold much more revealing personal information. Further, Google's recent privacy policy change allows Google to cross-referencing the content with the user's search queries and GPS location. This type of cross-referencing may potentially have more severe implications, raising many privacy concerns.

So what data does Facebook contain? It is a treasure-trove for information diggers since it contains:

- **Personal Identifiable Information (PII) as well as general personal information.** Included in this category are date of birth, home address, and even the mother's maiden name (and yes, some banks still use this information as an identifier). Even social security numbers can be extrapolated from many Facebook profiles, as shown by researchers at Carnegie Mellon University.

  This type of data can be used for various purposes. With enough gleaned information, a hacker can even gain control of the user's other online accounts. For example, using the "Forgot Password" feature which exists in many systems. This feature requires people to identify themselves by supplying an answer to a pre-determined personal question, such as the name of the user's dog. An information digger can retrieve that type of info from the individual's Facebook profile.



Hacking facebook accounts.

03-11-2012, 04:01 AM (This post was last modified: 03-11-2012 04:06 AM by [redacted]

Post: #1

[redacted]

Prestige: 6
Posts: 218
Joined: Feb 2012
Reputation:

Hello HF members
Im sorry if this thread is in the wrong section, if so i hope it gets moved!
Ok now lets get down to hacking!

Theres one simple way to hack facebook and the victims email account.
Alot of people might know about this already but not enough people do.

Ok, so say you have someone on your facebook you dont like and you want to hack their account or maybe it could be a friend and you wanted to hack him and prank on his/hers account..Well with this solution i gathered about 10 accounts easily, simply because the victims were stupid.

Ok so you go on their profile and if the have their email in the "info" section and say its "hackforums@[hotmail.co.uk]
You go to hotmail and you type in their email and click on forgot password.
If there is an option to get the password by typing in their secret question then it would be really easy to get if you know the slave well.
I hacked one guys email by simply typing in his secret question which was "where was i born" and he was born in pakistan.
So bang! there you go his/hers email is now yours... if they have such a stupid secret question like he did and you know the slave well enough it makes it easier than easy to get their email :D. So then you can change the password of their facebook...the email...etc etc and even gather alot of other interesting stuff from their email.

Hope this helped you out! :]

Weed is a Plant That The Government Does Not Seem To Care About.

Other uses hackers do away with this information is creating more credible phishing emails. The email may contain a personalized message requesting that the user click on a link which actually refers to an attacker-controlled site, or even download a malware-laden file.

Hackers can also use this information for extortion purposes. A student in Pennsylvania, for example, was told by hackers that they would post a private video of online unless he wired $500 to a man in Morocco.

Finally, professional identity thieves can use much of this data to build a better profile of the victim.

- **Passwords.** Although this may also be considered PII, we found it reasonable to include it as a separate section due to its sensitivity. Gaining access to the victim's account ultimately gives the hacker the knowledge and control over the user's password. Consumers are notorious for using the same password across multiple sites, and the Facebook password may just as well be the same password to other online services. In effect, allowing the hacker to impersonate the users to other services.

- **Friend-Mapping**. Facebook is all about "Friends". From a hacker's perspective, this means that getting hold of a victim's account will also provide the knowledge of the user's circle of friends. Once in a circle of friends, a hacker posing as a trusted friend can cause mayhem:
    - This allows hackers to create better scams (aka "419 scams"). For example, a message could seem to come from a friend requesting the transfer of monetary funds ("This is your friend, Tom. I am stranded in the middle of Paris with no money"). These phishing messages could be similar to those described above - containing links to malware or include malware-laden files. Since they

purportedly come from the victim's friend, the victim may be more susceptible to follow those links.

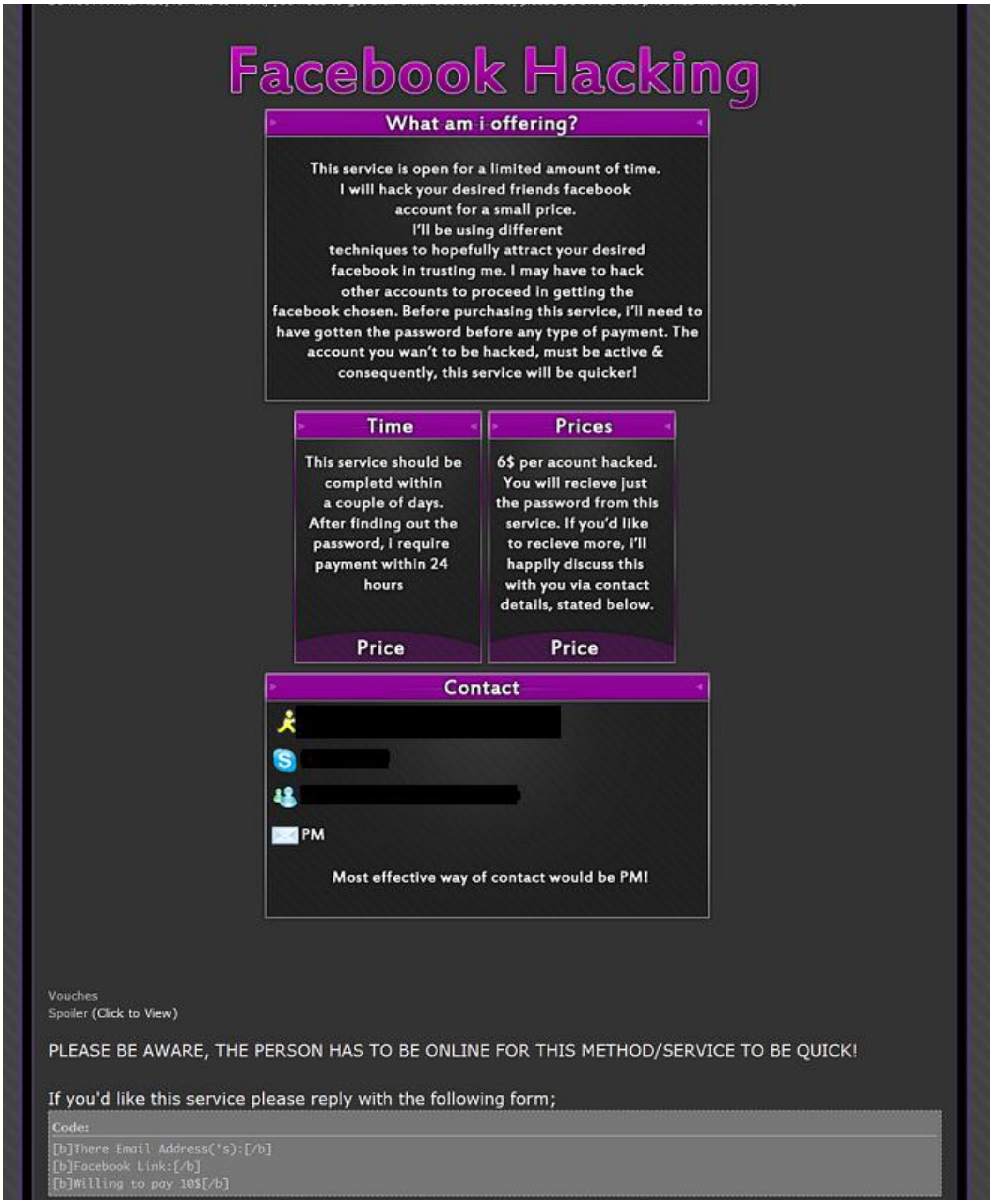
  - Through friends-mapping, a hacker can also gain enough personal information on the user which can also be used for extortion purposes. For instance, MIT researchers released a piece of software which can determine a user's sexual orientation according to their circle of friends. Many raised the implications of this to the outing of closeted individuals. The same approach could be applied to race or religion.

- **Organizational structure**. Similarly to friends-mapping, hackers can analyze the interleaved connections between individuals and analyze them in order to map out the structure of members of different organizations – as well as units within the organization. This is a stronger concern with other social networks, such as LinkedIn. However, this type of mapping can also be applied in Facebook, especially with businesses adopting "Fan" pages. The organizational structure can be used for corporate espionage, foreign-government and even military intelligence.

- **Business plans.** As a professional social network, LinkedIn provides a hotbed for competitive intelligence. But even Facebook provides enough info which is usable for competitive intelligence. In fact, different companies exist which offer exactly this kind of service. Users can follow what their competitors are discussing and what conversations they are participating in.
- **Geo Location information.** Through geo-location information, a hacker can build a profile of the victim's whereabouts. There were cases where law enforcement agencies actually were able to use this type of information to find and capture fugitives. Geo location data is all together more valuable when cross-referencing it with the organizational structure. This can be very useful, say, to gain military intel on the location of the adversary's military units. In fact, last year an IDF operation was cancelled following a soldier's status update of the operation's time and location.

Who then are the hacking groups who would attempt to use or hack Facebook?

- **Private hackers:** This is your regular hacking for profit types. They just want to make money by duping consumers. As such, their focus is more on gleaning PII and passwords. Private hackers have also been known to perform extortion.



Facebook Hacking

What am i offering?

This service is open for a limited amount of time. I will hack your desired friends facebook account for a small price. I'll be using different techniques to hopefully attract your desired facebook in trusting me. I may have to hack other accounts to proceed in getting the facebook chosen. Before purchasing this service, i'll need to have gotten the password before any type of payment. The account you wan't to be hacked, must be active & consequently, this service will be quicker!

Time

This service should be completd within a couple of days. After finding out the password, I require payment within 24 hours

Price

Prices

6$ per acount hacked. You will recieve just the password from this service. If you'd like to recieve more, I'll happily discuss this with you via contact details, stated below.

Price

Contact

[redacted]

[redacted]

[redacted]

✉ PM

Most effective way of contact would be PM!

Vouches
Spoiler (Click to View)

PLEASE BE AWARE, THE PERSON HAS TO BE ONLINE FOR THIS METHOD/SERVICE TO BE QUICK!

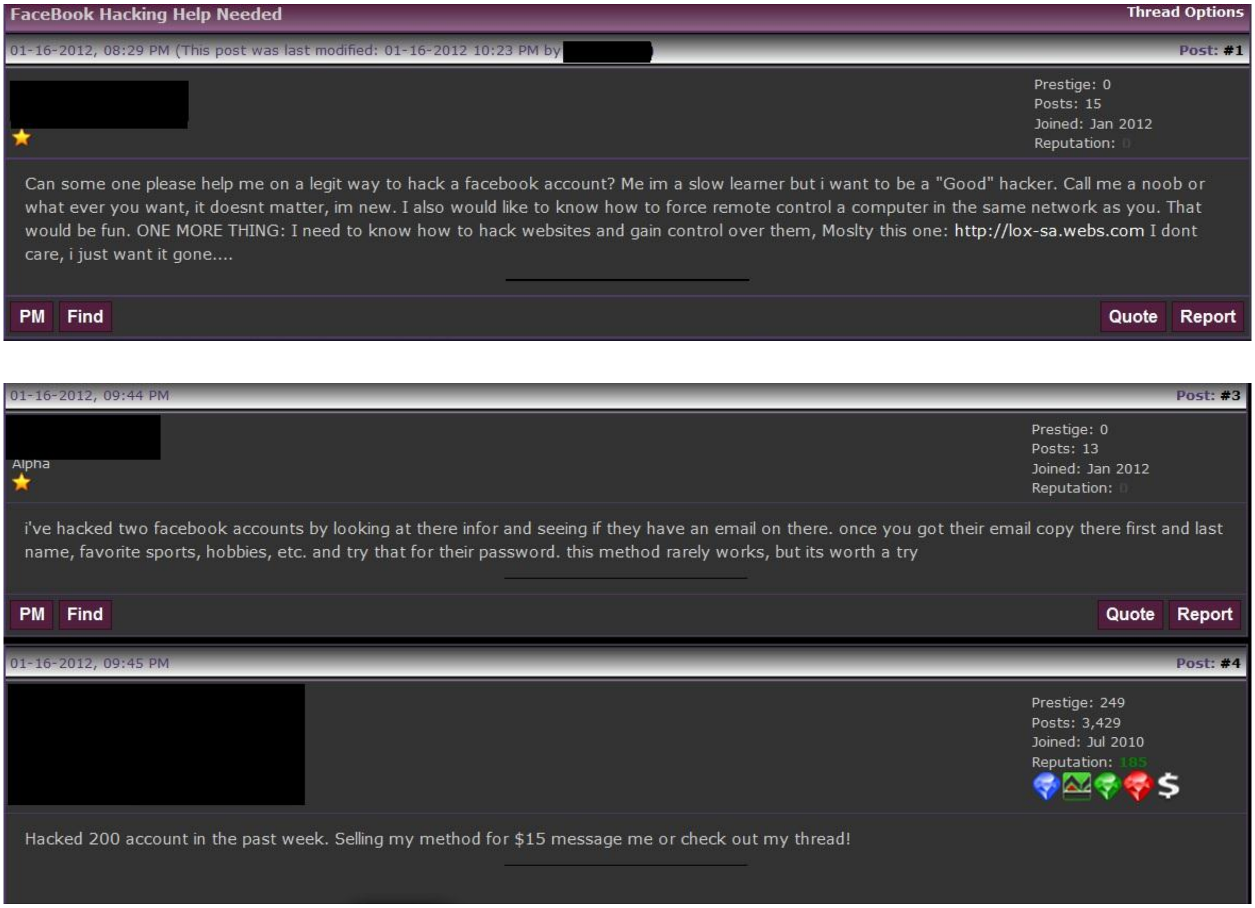
If you'd like this service please reply with the following form;

```
Code:
[b]There Email Address('s):[/b]
[b]Facebook Link:[/b]
[b]Willing to pay 10$[/b]
```

- **Government-sponsored hackers:** These hackers work for governments with the purpose of advancing some national agenda. They may use Facebook data for military intel purposes, uncover dissidents, and squashing dissention.
- **Corporate-espionage hackers:** These hackers may work for a certain organization or independently. The independent hackers may attempt to glean sensitive business information over time and then sell it to interested competitors. These hackers are mostly focused on corporate structure, business plans, and gaining enough information which will lead them to access other accounts (for you *Girl With a Dragon Tattoo* fans, think Lisbeth Sander).
- **Hactivists:** So far, hacktivists have used Facebook as a means of communication as opposed to a resource for taking data. For example, Anonymous claims to have taken

some “revealing” photos of BART spokesperson Linton Johnson from Facebook. As hacktivism evolves, this will likely change. For example, we could see Facebook data exposed by hacktivists designed to embarrass individuals or an organization.

How Do Hackers Hack Your Facebook Account?



01-16-2012, 08:29 PM (This post was last modified: 01-16-2012 10:23 PM by [redacted]) Post: #1

[redacted]

Prestige: 0
Posts: 15
Joined: Jan 2012
Reputation: 0

Can some one please help me on a legit way to hack a facebook account? Me im a slow learner but i want to be a "Good" hacker. Call me a noob or what ever you want, it doesnt matter, im new. I also would like to know how to force remote control a computer in the same network as you. That would be fun. ONE MORE THING: I need to know how to hack websites and gain control over them, Moslty this one: http://lox-sa.webs.com I dont care, i just want it gone....

01-16-2012, 09:44 PM Post: #3

[redacted]
Alpha

Prestige: 0
Posts: 13
Joined: Jan 2012
Reputation: 0

i've hacked two facebook accounts by looking at there infor and seeing if they have an email on there. once you got their email copy there first and last name, favorite sports, hobbies, etc. and try that for their password. this method rarely works, but its worth a try

01-16-2012, 09:45 PM Post: #4

[redacted]

Prestige: 249
Posts: 3,429
Joined: Jul 2010
Reputation: 185

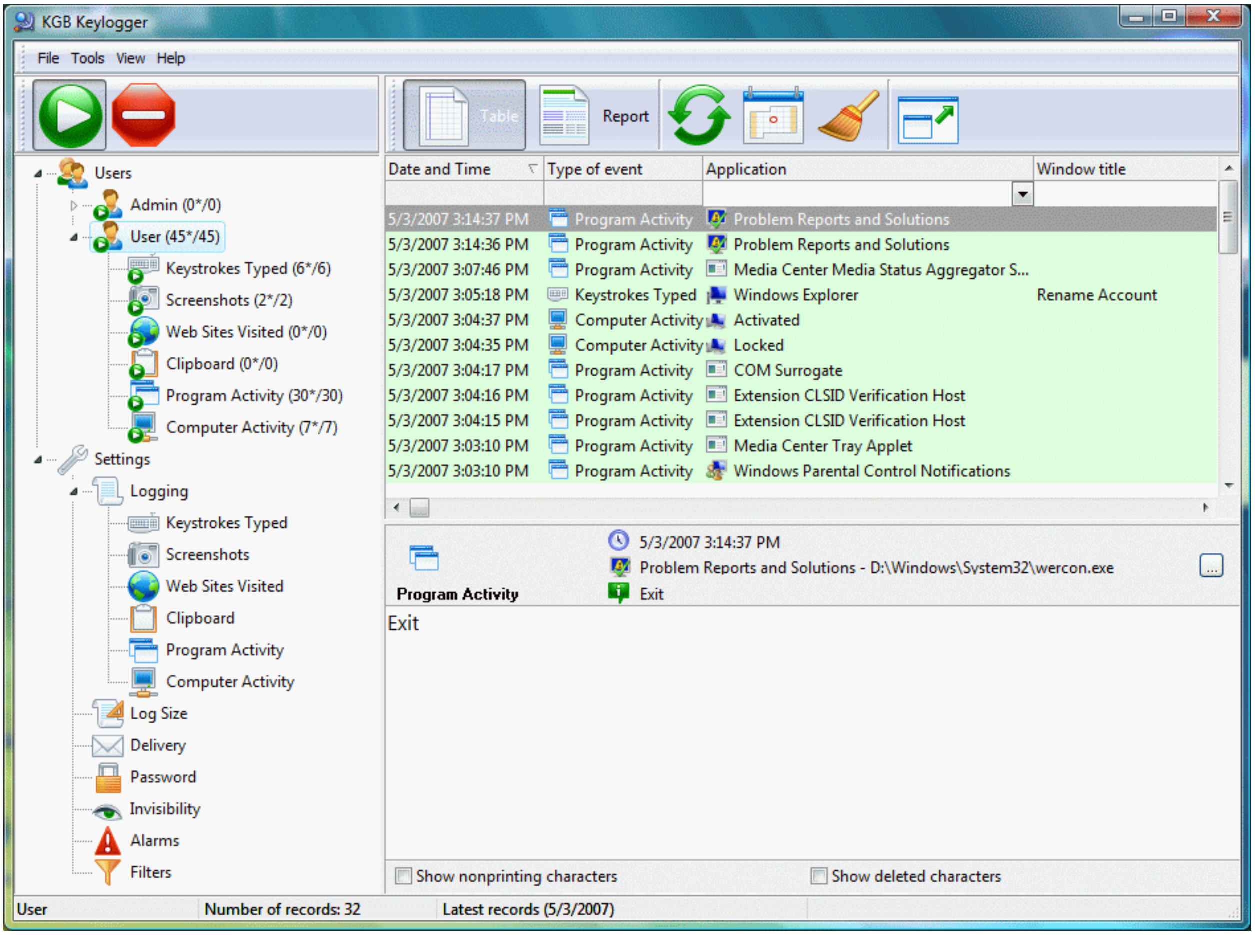
Hacked 200 account in the past week. Selling my method for $15 message me or check out my thread!

Hacking Facebook discussions on hacker forums

In the first of this two-part series, we showed how Facebook profile data is very attractive to different of hackers. But how do hackers gain this information?

The main method to gain access to the Facebook account of a specific user is getting the password. This can be done in myriad ways:

- **Malware**. These are different keystroke loggers which record the user’s activity, including passwords to different applications. The malware is typically installed by employing different social engineering techniques which implore the user to download a particular “cool” but, in reality, malicious) app. Malware may also be installed using drive-by-download techniques where the browser is instructed to download malware in an attacker’s controlled server. Obviously, there are also physical ways such as accessing the victim’s machine when the user’s device is left unlocked and unattended.



Date and Time	Type of event	Application	Window title
5/3/2007 3:14:37 PM	Program Activity	Problem Reports and Solutions	
5/3/2007 3:14:36 PM	Program Activity	Problem Reports and Solutions	
5/3/2007 3:07:46 PM	Program Activity	Media Center Media Status Aggregator S...	
5/3/2007 3:05:18 PM	Keystrokes Typed	Windows Explorer	Rename Account
5/3/2007 3:04:37 PM	Computer Activity	Activated	
5/3/2007 3:04:35 PM	Computer Activity	Locked	
5/3/2007 3:04:17 PM	Program Activity	COM Surrogate	
5/3/2007 3:04:16 PM	Program Activity	Extension CLSID Verification Host	
5/3/2007 3:04:15 PM	Program Activity	Extension CLSID Verification Host	
5/3/2007 3:03:10 PM	Program Activity	Media Center Tray Applet	
5/3/2007 3:03:10 PM	Program Activity	Windows Parental Control Notifications	

Program Activity

5/3/2007 3:14:37 PM
Problem Reports and Solutions - D:\Windows\System32\wercon.exe
Exit

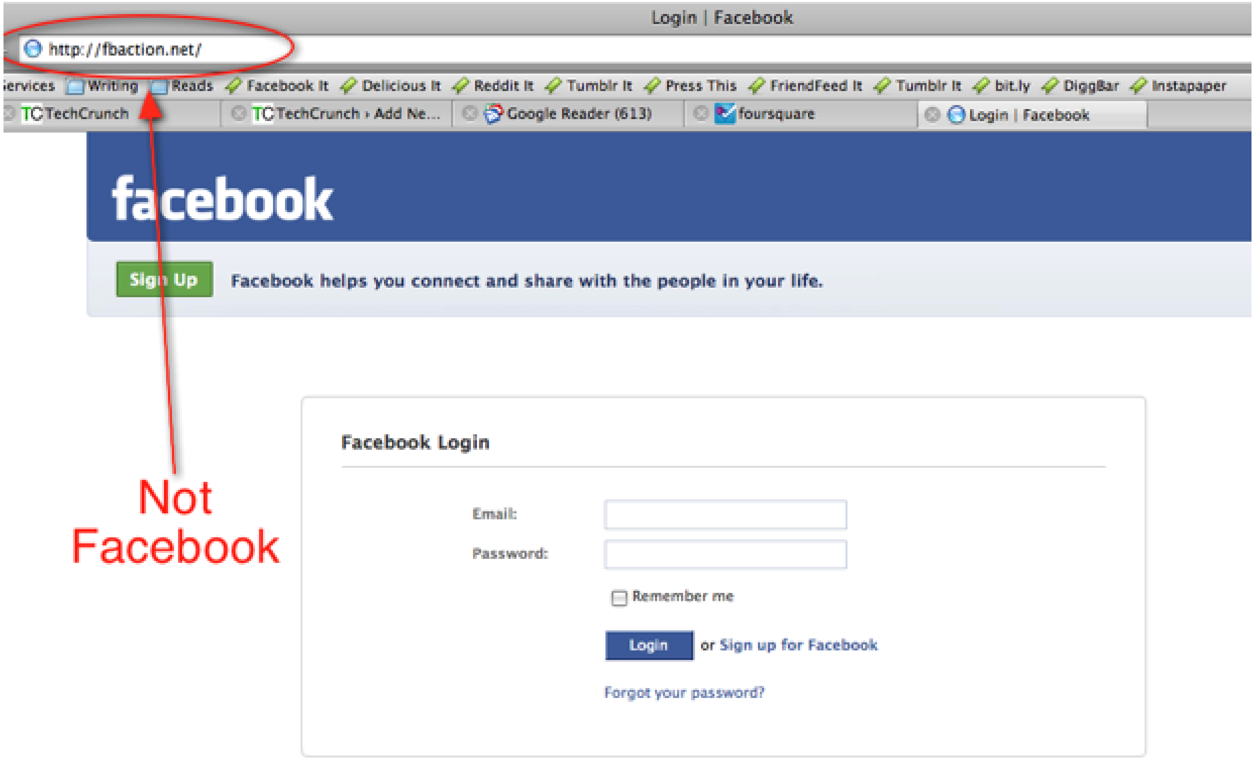
Exit

☐ Show nonprinting characters ☐ Show deleted characters

User | Number of records: 32 | Latest records (5/3/2007)

http://www.securitystronghold.com/gates/kgb-keylogger.html

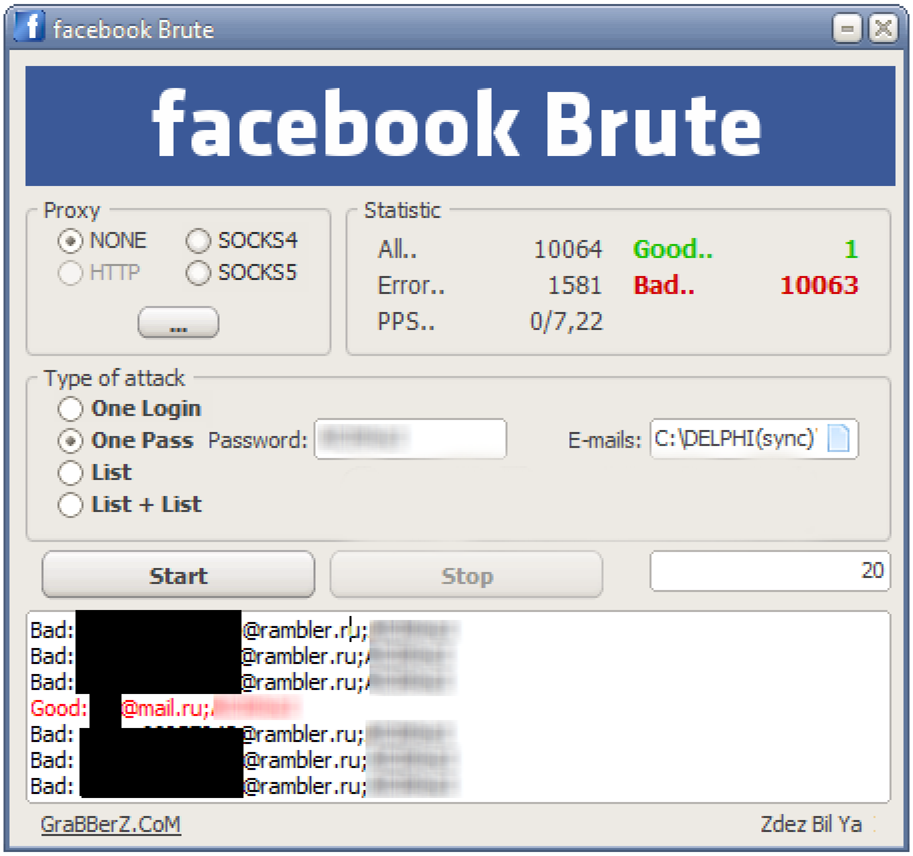
- **Phishing**. This method attempts to deceive the user to divulge their credentials by mocking the Facebook login page. In a past entry of ours, we provided an example of such a phishing kit which creates fake Facebook - as well as about a dozen more - sites. This particular kit became quite popular, whereas the hacker boasted more than 200K downloads.



Facebook helps you connect and share with the people in your life.

http://1.bp.blogspot.com/_kJrHh3L8mag/TUrvYbTnv4I/AAAAAAAAABc/ktFIc2_L6iM/s1600/fbfake.png

- **Bruteforce**. The attacker repeatedly attempts the guess the user’s password. This technique is particularly effective against users who tend to use easy and guessable passwords. This YouTube video presents the “Facebreak” bruteforcer.



Proxy
● NONE ○ SOCKS4
○ HTTP ○ SOCKS5

Statistic
All.. 10064 Good.. 1
Error.. 1581 Bad.. 10063
PPS.. 0/7,22

Type of attack
○ One Login
● One Pass Password: [redacted] E-mails: C:\DELPHI(sync)
○ List
○ List + List

20

```
Bad: [redacted]@rambler.ru;[redacted]
Bad: [redacted]@rambler.ru;[redacted]
Bad: [redacted]@rambler.ru;[redacted]
Good: [redacted]@mail.ru;[redacted]
Bad: [redacted]@rambler.ru;[redacted]
Bad: [redacted]@rambler.ru;[redacted]
Bad: [redacted]@rambler.ru;[redacted]
```

http://hackingmagazine.blogspot.com/2011/01/new-facebook-brute-force.html

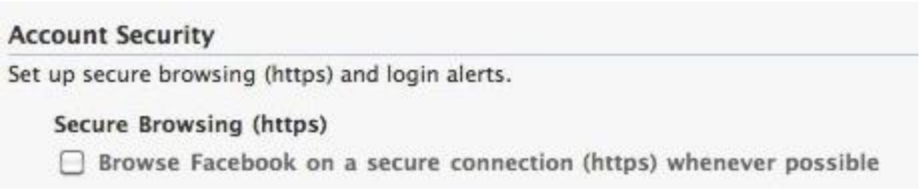
Hacking methods by individuals is not only confined to password-grabbing. Other methods have shown to be successful in the past:

- **Hacking a Facebook's admin rights**. Although this requires more effort on the hacker side and so is not as prevalent, this type of an attack stands out. It is the "holy grail" of attacks as it provides the hacker also with all that "inaccessible" data. Not only of a single user – but of all users. Attackers can achieve these rights by hacking into Facebook's systems, submitting court orders (see below), or even bribing a Facebook administrator. Recently, a hacker was sentenced after hacking into Facebook's internal system and extracting parts of Facebook's source code.
- **Building a data-slurping application**. Last year a bug in Facebook allowed applications to access users' private data. Further, Facebook allows the users to set what applications have access to what data. So, even if an application does not initially have permissive rights to access the user's data, a hacker can entice the user to open up access to these applications.
- **Stealing a user's Facebook cookie**. Such a "cookie" contains sensitive information such as the user's username and password. Consequently, a hacker who steals the cookie can impersonate the real user. In fact, the ultra-popular application, Firesheep, released last year demonstrated how easy it is to steal a user's cookie. Firesheep's simple GUI gave

people - including those “clueless” in hacking – the ability to steal Facebook cookies from individuals connecting to public terminals, such as in Starbucks.

The next two methods can also be carried out by lone hackers, private investigators, and simple cyber-voyeurs. While government-sponsored hackers can use these same tactics on a great scale since they have greater advanced communication interception capabilities.

- **Eavesdropping.** Although Facebook login information are sent in encrypted format- which prevents eavesdroppers from gaining the credentials, the rest of Facebook’s online activities are not usually encrypted. This means that eavesdropping is as simple as “listening” to open WiFi networks. To respond to this issue, Facebook recently (Jan 26th 2012) Facebook added the option to opt in for SSL for other activities too, see http://www.facebook.com/blog/blog.php?post=486790652130.



Account Security

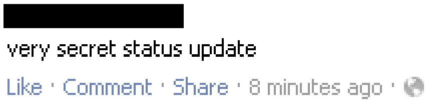
Set up secure browsing (https) and login alerts.

Secure Browsing (https)

□ Browse Facebook on a secure connection (https) whenever possible

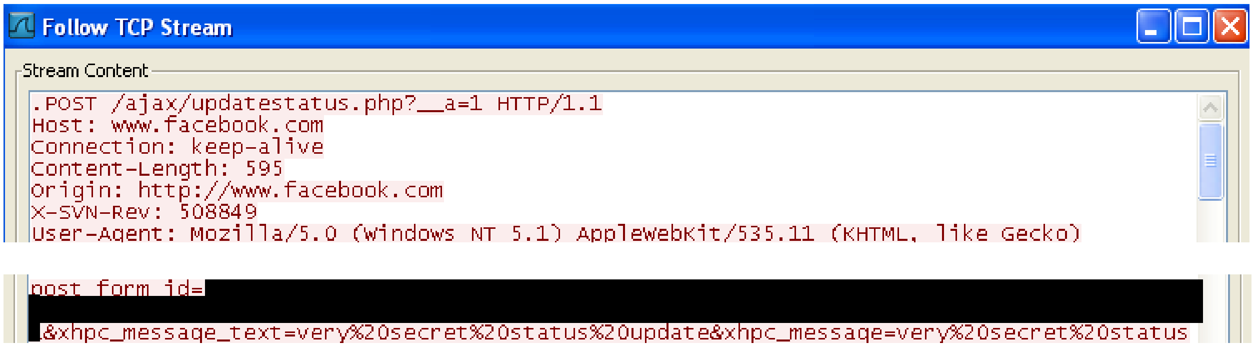
We recommend FB users to enable that option, as leaving traffic unencrypted may allow the hackers to listen into the rest of the communication.

Here’s how a hacker could track this information:



[redacted]

very secret status update



```
.POST /ajax/updatestatus.php?__a=1 HTTP/1.1
Host: www.facebook.com
Connection: keep-alive
Content-Length: 595
Origin: http://www.facebook.com
X-SVN-Rev: 508849
User-Agent: Mozilla/5.0 (Windows NT 5.1) AppleWebKit/535.11 (KHTML, like Gecko)
```

```
post_form_id=[redacted]
&xhpc_message_text=very%20secret%20status%20update&xhpc_message=very%20secret%20status
```

- **Monitoring communications.** We put this as a separate technique than eavesdropping since eavesdropping includes the connotation of doing something surreptitiously without ever wanting to be caught. But what about public communications? Facebook is huge and can provide a lot of information if someone can discern noise from something interesting. Note how recently the FBI issued an RFI to monitor social media. Further if the info is public then anyone can crawl it. For example, on 2010 an individual collected the public profiles of 100 million Facebook users and published it online in a single downloadable file. The consequence is that even if a user had changed their settings after the scraping of their profile – this was too late since people already had their profile details.

In addition to the above methods, government-sponsored hackers have that extra power which allow them to obtain users' Facebook data – including the "inaccessible" portions:

- **Altering the Facebook communication.** As mentioned, Facebook credentials are typically sent encrypted under the SSL protocol. However, Tunisia got around this obstacle by injecting Javascript code to the applications' login page. That extra piece of code allowed all credentials to be re-routed to a Tunisian controlled site. In another case, the Iranian government was able to spoof SSL and act as a man-in-the-middle tapping into users' Facebook communications. In Tunisia, for example, targets found that Facebook groups they founded were deleted, as were pictures of protests.
- **Legal means.** Of course, there are legal routes to obtain the data. Facebook lists the required guidelines for law enforcement to access records. For instance, in the US, the agency must have a subpoena or court order. And, there's also Max Schrem's way – simply ask for it under the European data protection law.