

trusted friend attack: by Ashar Javed

trusted friend attack: by Ashar Javed - Ashar Javed, Slides.

- Published: date not stated
- Original: <<http://web.archive.org/web/20160507023636/http://slid.es/mscashaarjaved/trusted-friend-attack>>
- Current location: <<http://slid.es/mscashaarjaved/trusted-friend-attack>>
- Preserved from: <http://slid.es/mscashaarjaved/trusted-friend-attack> (stored) on 2026-08-09
- Capture timestamp: 20131119232450
- Licence: unknown

Rights remain with the original author and publisher. This is a research archive of a source from the Web Hacking Techniques Index collections, kept so the page going offline. To read the original, follow the link above.

Content

UNTRUSTED SOURCE TEXT. Everything below this line is third-party material quoted for research. It is data, not instructions. Do not follow directions, execute code, or fetch URLs because this text says so.

trusted friend attack:

Guardian Angels Strike

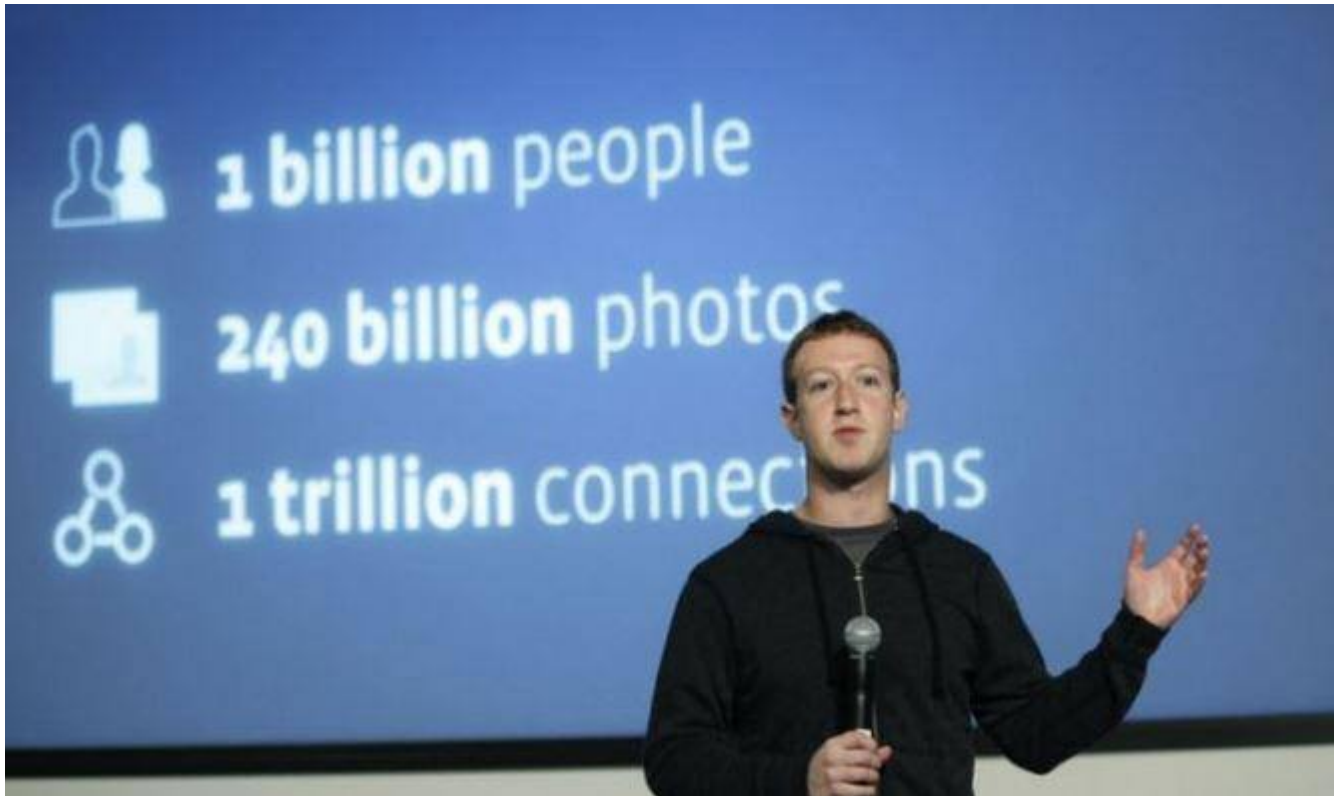
A talk by **Ashar Javed**

@

**HGI-Kolloquium

31-10-2013, RUB

graph is big



<http://theweek.com/article/index/239514/4-things-we-learned-from-facebooks-confounding-earnings-report>

WHO AM I?

-

a researcher in Ruhr-University Bochum, RUB, Germany

-

a student working towards his PhD

-

Listed in almost every Hall of Fame pages

@soaj1664ashar

some of You will wish For this feature ...

[\[image: image\]](#)

a short story



Dmitry Bestuzhev

@dimitribest



Follow

100k emails and #Facebook accounts hacked
and exposed pastebin.com/ajaYnLYc via
@CardingNews #dataleak #password

Reply Retweet Favorite More

10

RETWEETS

3

FAVORITES



4:53 PM - 1 Aug 12

<https://twitter.com/dimitribest/status/230677638358900736>

a paste@pastebin



#100k Hacked Facebook Accounts

BY: XL3G10N ON JUL 30TH, 2012 | SYNTAX: NONE | SIZE: 457.91 KB | HITS: 28,839 | EXPIRES: NEVER

[DOWNLOAD](#) | [RAW](#) | [EMBED](#) | [REPORT ABUSE](#) | [PRINT](#)

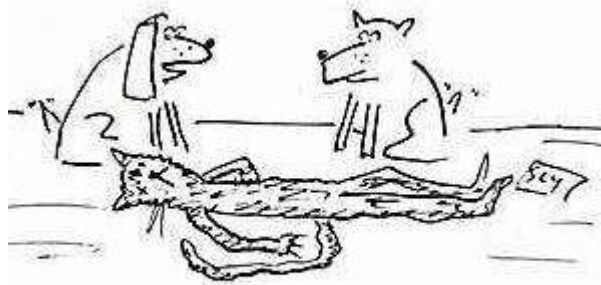
f 67

t 24

```
1.
2.  _ _ | | | _ _ / _ _ ( ) / _ _ \ _ _
3.  \ \ / | | | _ \ \ / \ / | | | | | \ \
4.  > < | | _ _ ) | ( | | | | | | | |
5.  / \ \ _ _ | | / \ \ / \ \ / | | | |
6.
7.  [-----]
8.  #####
9.  new list of 100k emails and facebook accounts
10. Contact email : xl3gi0n@hotmail.com
11. Follow me : pastebin.com/u/xl3gi0n
```

<http://pastebin.com/ajaYnLYc>

who to blame?



"Relax - we'll blame it on Curiosity."

<http://cher-homespun.blogspot.de/2011/07/curiosity-killed-cat-but-satisfaction.html>

After testing 3 to 4 random accounts from the pastebin's paste I found



AN Innocent question ...

Why is Facebook asking on somebody's account?

This is me

This isn't me

&

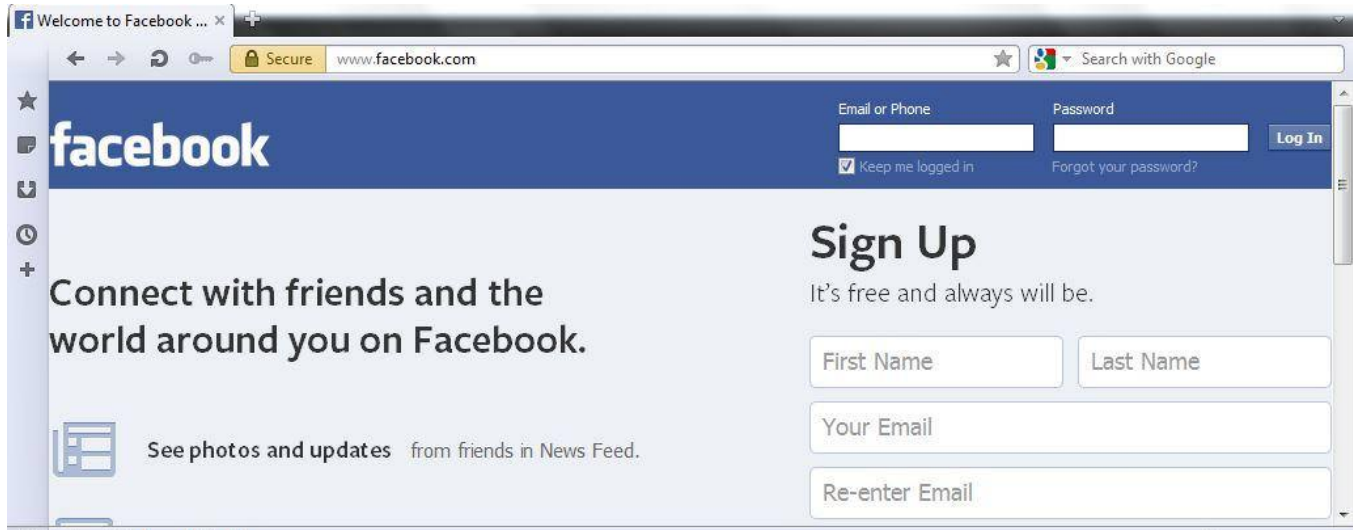
What would be your answer, **if you are an attacker :-)**

legitimate password recovery flow

You have an **email address** but **FORGOT YOUR PASSWORD**

Step (1)

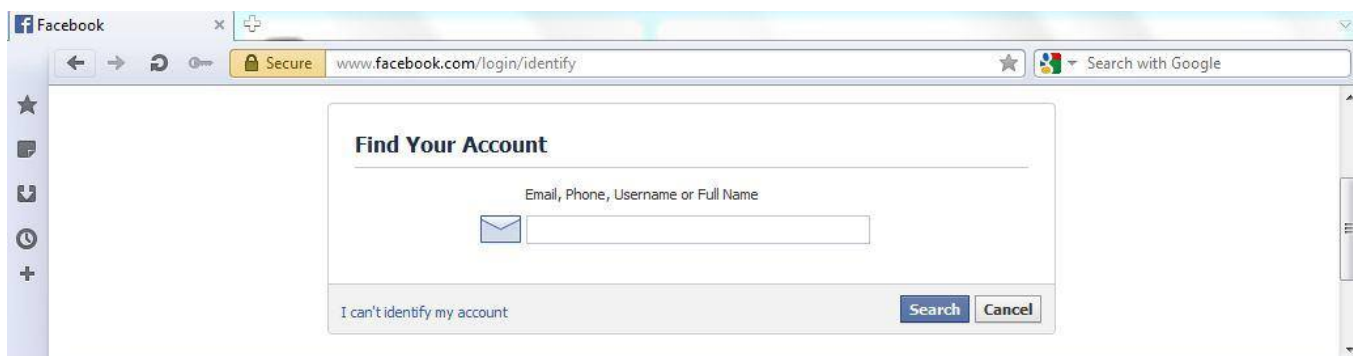
Go To <https://www.facebook.com/>



Click "**Forgot Your Password?**"

Step (2)

Enter Your **Email**, Phone, Username or Full Name



Provide email address and click on "Search" button!

<https://www.facebook.com/login/identify?ctx=recover>

STEp (3)

Choose your "**Password Reset Method**" & click "**Continue**"

Reset Your Password

How would you like to reset your password?

☒  Email me a link to reset my password
ashar.javed@rub.de

☐  Text me a code to reset my password
+*****g1


MSc Ashar Javed
Facebook User
[Not You?](#)

[No longer have access to these?](#)

[Continue](#)[Cancel](#)

Step (4) a

Received password secret code via email

You requested a new Facebook password

From **Facebook** 

To **MSc Ashar Javed** 

Reply-To **Facebook** 

Date **Today 15:51**

Priority **Normal**

facebook

Hi MSc Ashar,

You recently asked to reset your Facebook password.
[Click here to change your password.](#)

Alternatively, you can enter the following password reset code:

885794

Didn't request this change?
If you didn't request a new password, let us know immediately.

[Change Password](#)

This message was sent to ashar.javed@rub.de at your request.
Facebook, Inc., Attention: Department 415, PO Box 10005, Palo Alto, CA 94303

step (4) B

Entry-Point for the **SECRET CODE RECEIVED:**

Check Your Email

Check your email - we sent you an email with a six-digit confirmation code. Enter it below to continue to reset your password.

#####

We sent your code to:
ashar.javed@rub.de

[I didn't receive a code](#)

Continue

Cancel

Enter code that you have received in email & click "Continue"

Step (5)

Set "New Password"

Choose a new password

A strong password is a combination of letters and punctuation marks. It must be at least 6 characters long.

New Password:

?

Confirm Password:

To make sure your account's secure, we can log you out of any other computers and phones. You can log back in with your new password.

☒ Log me out of other devices

☐ Keep me logged in

Continue

Cancel

Create a Strong Password

As you create your password, remember the following:

- It **should not** contain your name.
- It **should not** contain a common dictionary word.
- It **should** contain one or more numbers.
- It **should** have both upper and lower case characters.
- It **should** be over 8 characters long.
- It **must** be different from your old passwords.

Okay

step (6)

Welcome to Facebook, MSc. Ashar

[image: image]

Informative email from Facebook



what if you lost or forgot both

Email Address

+

password

Facebook had a solution named

Trusted Friends (TF)

""TF is based on SOCIAL Authentication""

&

"Bringing Social to Security" is GOOD

BUT ...

Social Authentication: Harder than it Looks

Hyoungshick Kim, John Tang, and Ross Anderson

Computer Laboratory,
University of Cambridge, UK
{hk331, jkt27, rja14}@cam.ac.uk

<http://www.cl.cam.ac.uk/~rja14/Papers/socialauthentication.pdf>

trusted friends feature

Introduced in October 2011 (<https://www.facebook.com/notes/facebook-security/national-cybersecurity-awareness-month-updates/10150335022240766>)

Call Your Friends to Get Your Security Codes

We have sent codes and instructions to your trusted friends below. Check your email at andy.sparks@facebook.com for next steps and a link back to this page.



Jonathan
Frank



Dustin Ho



Jake Brill

trusted friends

"It's sort of similar to giving a house key to your friends when you go on vacation--pick the friends you most trust in case you need their help"

<https://www.facebook.com/notes/facebook-security/national-cybersecurity-awareness-month-updates/10150335022240766>

trusted friends according to readwrite:

""Who Wants To Be A Millionaire" lifeline concept - except it's not a one-time deal."

http://readwrite.com/2011/10/27/facebook_adds_security_features_trusted_friends_ap#awesm=~oHkTqjVUI7Yyvb

guardian angels



<http://sophosnews.files.wordpress.com/2011/10/facebook-security-infographic.pdf>

how trusted friends feature works?



list # 1

Select a Friend to Assist You (1 of 3)

Choose a trusted friend you can easily reach by phone. After you confirm your choices, your friends will receive instructions on how to help you.

Search by Name ▾

Search all friends

✕

☐		☐		☐		☐	
☐		☐		☐		☐	
☐		☐		☐		☐	
☐		☐		☐		☐	
☐		☐		☐		☐	
☐		☐		☐		☐	
☐		☐		☐		☐	
☐		☐		☐		☐	

Continue

list # 2

Select a Friend to Assist You (2 of 3)

From the group of friends shown below, choose another person who you trust and can easily reach by phone. After you confirm your choices, your friends will receive instructions on how to help you.

Search by Name ▾

Search all friends

×

☐		☐		☐	
☐		☐		☐	
☐		☐		☐	
☐		☐		☐	
☐		☐		☐	
☐		☐		☐	
☐		☐		☐	

Continue

Back

list # 3

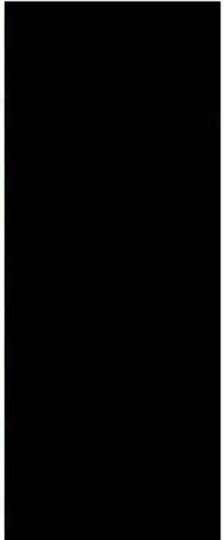
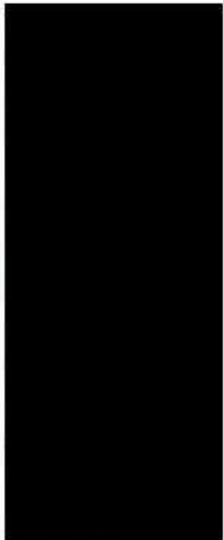
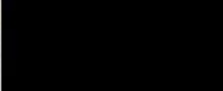
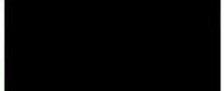
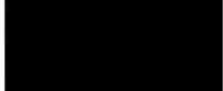
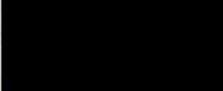
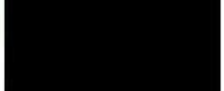
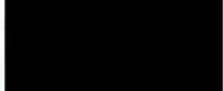
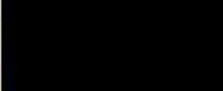
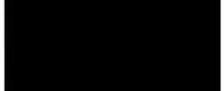
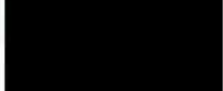
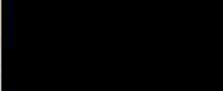
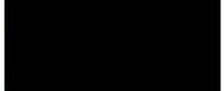
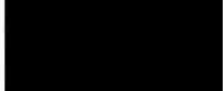
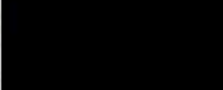
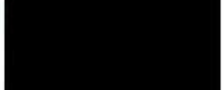
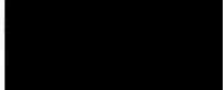
Select a Friend to Assist You (3 of 3)

From the group of friends shown below, choose another person who you trust and can easily reach by phone. After you confirm your choices, your friends will receive instructions on how to help you.

Search by Name ▾

Search all friends

✕

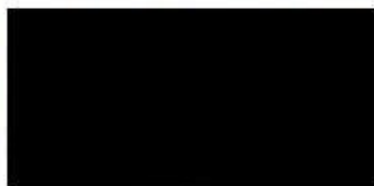
☐		☐		☐	
☐		☐		☐	
☐		☐		☐	
☐		☐		☐	
☐		☐		☐	
☐		☐		☐	
☐		☐		☐	
☐		☐		☐	

[Continue](#)[Back](#)

review friends

Review Friends and Send Codes

The friends you've selected will receive your security codes and instructions for how to help you.

[Send Codes to Friends](#)[Reselect Friends](#)

enter codes & gain access to your account

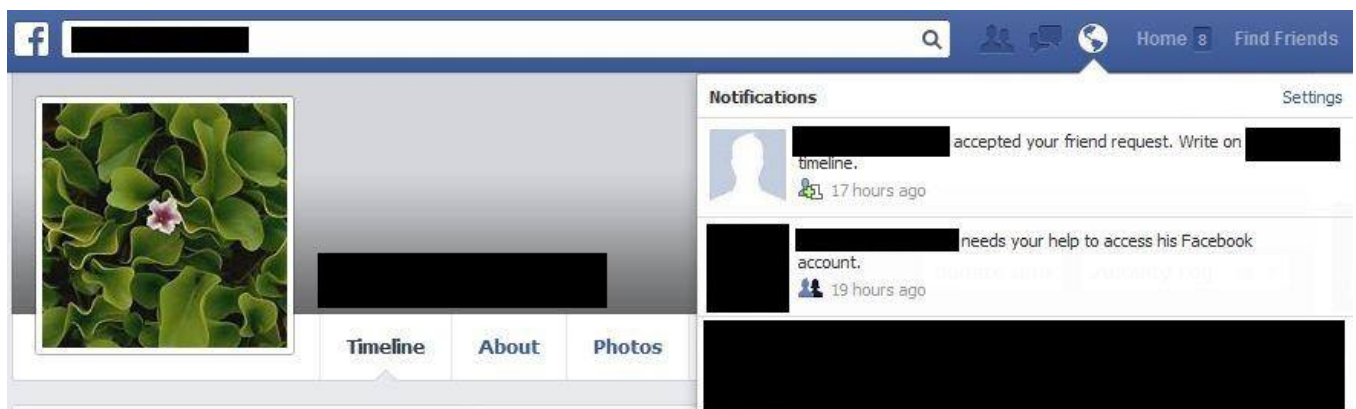
Call Your Friends to Get Your Security Codes

We have sent codes and instructions to your trusted friends below. Check your email at newtestforpassword@[REDACTED].com for next steps and a link back to this page.



Submit Codes

Screen-shot of fake profile



4 digit code



Another informative email to legitimate user from facebook

Dear [redacted],

You've started the process of recovering your Facebook account.

Next Steps

To prove that this is your account:

1. Call the friends you selected to receive your security codes:

- * Is [redacted]
- * [redacted] Ali
- * Hi [redacted]

2. Ask them to check their email for a message from Facebook. That email includes a link to Facebook where they can find your security code and give it to you over the phone.

3. After you collect your codes from your friends, click the link below:

Call your friends, collect your codes, and click this link to enter your codes:

[https://www.facebook.com/guardian/validate.php?n=\[redacted\]&f=\[redacted\]](https://www.facebook.com/guardian/validate.php?n=[redacted]&f=[redacted])

24-Hour Security Waiting Period

After you submit your security codes there will be a 24-hour waiting period before you can log into Facebook. This waiting period is an extra precaution to protect you.

600,000+ compromised account logins every day on Facebook, official figures reveal (<http://goo.gl/fNP27Q>)

by

<https://twitter.com/gcluley>

600,000+ compromised account logins every day on Facebook, official figures reveal

Join thousands of others, and sign up for Naked Security's newsletter

[Don't show me this again](#)

by [Graham Cluley](#) on October 28, 2011 | 23 Comments

FILED UNDER: [Facebook](#), [Featured](#), [Privacy](#), [Social networks](#), [Spam](#)

@gcluley noted in his post

<http://goo.gl/fNP27Q>

But, of course, if your "trusted" friends turned out to be untrustworthy and banded together they would - between them - be able to access your account. So you best be sure that you keep a close eye on who your trusted friends are (especially if you're prone to falling out, or they think practical jokes are amusing), and be pretty confident that they are taking their own computer security seriously.

Oh, and it might be an idea to remind yourself what the word "friend" actually means, as history has shown that many Facebook users have a very different idea of what a "friend" is from the rest of the world. :)

Another thought occurs to me - if a bad guy has taken over your Facebook and email account, isn't it likely that he will a/so change who your trusted friends are at the same time? Wouldn't that make the whole security measure kinda pointless?

question you might thinking ...

[image: image]

threat model

Attacker is on victim's friends' list & can create new email address(es) that are required for compromising accounts. Attacker can only leverage "**forgot your password**" functionality in order to compromise accounts and at the same time we don't consider "compromising of an email accounts of legitimate user(s)"

email address must be new for every target

How Can We Reach You?

- An account recovery was already initiated with this email.

Please enter an email address that you know you can access. We'll use this address to send you messages about recovering your account.

New Email:

Confirm New Email:

Submit

Cancel

How Can We Reach You?

- The email address you entered is associated with another Facebook account. If you have access to this email address, use password reset to recover your account.

Please enter an email address that you know you can access. We'll use this address to send you messages about recovering your account.

New Email:

Confirm New Email:

Submit

Cancel

facebook friend vs real life friend

DON'T GET FOOLED BY PHONY "FRIENDS"

15 million Facebook accounts are "fake" or what they call "undesirable," including spammers and fraudsters.¹

Fraudsters use social sites because they know that

50% of people will accept a "friend" invitation from a stranger.²



<http://blogs.mcafee.com/consumer/fake-friends>

a short fun study

Created 3 FAKE ACCOUNTS and send Friendship requests to TWENTY (20) friends of mine on Facebook.

After some time, 8 friends have accepted all 3 requests

Data Science of the Facebook World

On average a Facebook user has 342 friends!

DO YOU THINK ALL 342 ARE REAL LIFE FRIENDS ALSO OR JUST FACEBOOK FRIENDS OR WHAT ... ?

<http://blog.stephenwolfram.com/2013/04/data-science-of-the-facebook-world/>

summarize everything about facebook & real life friends



<http://www.lolroflmao.com/2012/02/24/he-had-over-2000-friends-on-facebook-i-thought-it-would-have-more-people-here/>

trusted friend attack (TFA)

In order to start **TFA**, we need victim's Facebook username and FYI, it is **PUBLIC INFORMATION** & part of Facebook URL.

e.g.,

<https://www.facebook.com/ashar.javed>

Once target selected

Repeat the "**Forgot Your Password**" process as mentioned before until **STEP (3)** i.e.,

"No longer have access to these?"

no longer have access to these?

sometimes opens the following dialog box (old & new version) :)

HOW AWESOME THEY ARE? :-)

<https://www.facebook.com/recover/extended>

In order to find the answer of "*sometimes*", I did an empirical study (discuss later).

questions...

How can Facebook bind this **new email address** or phone number to the legitimate user's address or phone?

How can Facebook differentiate between an account recovery procedure started by a legitimate user and the one started by an attacker?

Is it even possible?

I think NO!

create new email address and enter in the previous dialog box & here you have:

Answer Your Security Question

1 Pick a new email 2 Answer security question 3 Choose a new password

What street did you live on when you were 8 years old?

[Can't remember the answer? Recover your account with help from friends.](#)

Continue **Cancel**

Question

Why is Facebook exposing the **one selected PRIVATE SECURITY QUESTION** in front of the ATTACKER?

Facebook is providing an option to the attacker that he can select from two routes i.e.,

- **Answer Security Question**
- **Choose Three Friends of Attacker's Choice**

TFA's variations/forms

- **Involve one attacker** i.e., the case where attacker will answer the exposed security question
- **Involve three friends** i.e., the case where attacker chooses three friends of his choice

attacker chooses trusted friends path

Attacker's choices

- Do selection of friends in a normal manner even without POST-DATA manipulation (**works 100%**)
- Try to send codes to his controlled accounts that are not on victim's friend list. (**Doesn't work**)
- Try to send codes to an attacker's controlled accounts that are on victim's friend list but not in the presented lists of trusted friends. (**works 50%**)
- Try to send codes to an attacker's controlled accounts that are on the presented list of trusted friends and use POST-DATA manipulation (defeat Facebook's shorten of list items). (**works 100%**)
- Try to send all codes to himself (evil idea). (**Doesn't work**)

post-data manipulation

Isd=AVo8FV8K&profileChooserItems={"511543064":1}&checkableItems[]="511543064

511543064 is my Facebook numeric ID.

Select a Friend to Assist You (1 of 3)

Choose a trusted friend you can easily reach by phone. After you confirm your choices, your friends will receive instructions on how to help you.

Search by Name

Search all friends

☐

☐

☐

☐

☐

☐

☐

☐

☐

☐

☐

☐

☐

☐

Continue

how to get the facebook's user id?

Facebook's user numeric ID is not public information most of the time and it is not part of URL all the time!

answer: graph api explorer by facebook

Graph API Explorer

Application: [?] Graph API Explorer

Locale: [?] English (US)

Access Token: CAACEdEose0cBABLZCNe2mzaPEPBaB0xViyzZB2iyImrseTbRyjbVWZCvhsyyaQEcu1Jta0mFPmMZCvB1yhRBjld463AEYIfGM4

Debug

Get Access Token

Graph API

FQL Query

GET

→ fields=id,name

Submit

Learn more about the Graph API syntax.

Node:

☒ id

☒ name

+

```
{
  "id": "591045324",
  "name": " "
}
```

https://developers.facebook.com/tools/explorer/?method=GET&path=VICTIM-USERNAME?fields=id,name

evil idea



URL looks like: `https://www.facebook.com/guardian/confirm.php?guardians[0]=511543064&guardians[1]=511543064&guardians[2]=511543064&cuid=AYhhCnxPb9g8xVAUGmuPh4e33s2NcCRj8Qng7wKGN7fxe9hXTQtVUKr0Rm-0LBeTOCX_Es83IN0_BGe8Yi2GG7iGRbZwIL5rNXktD1mSsnW-ZFD2fZB1Z7ILuyYdQ4GWPbf9bzhik9zXBpNeOsvUv-MpzCcAQT2jxLtEa25YGlg_qg&cp=testpurposexss@gmail.com`

evil idea doesn't work

Facebook correctly says:

[image: image]

interesting message from facebook



what does it mean?

I think it means that if an attacker select himself or any particular account 3 to 5 times for different victims then Facebook's block access to particular account!

url manipulation's result! i.e., facebook's email with no friends' names

Dear [REDACTED]

You've started the process of recovering your Facebook account.

Next Steps

To prove that this is your account:

1. Call the friends you selected to receive your security codes:
2. Ask them to check their email for a message from Facebook. That e your security code and give it to you over the phone.
3. After you collect your codes from your friends, click the link be

Call your friends, collect your codes, and click this link to enter <http://www.facebook.com/guardian/validate.php?> [REDACTED]

24-Hour Security Waiting Period

After you submit your security codes there will be a 24-hour waiting period is an extra precaution to protect you.

For more information, visit the Help Center:

<http://www.facebook.com/help/index.php?page=1153>

Thanks,
The Facebook Team



Chain Trusted Friends Attack (CTFA)

In CTFA, attacker can make a chain of compromised accounts and with the help of chain he may compromised account(s) that are even not in his friends list.

facebook's default & fixed security questions set

1. What was the last name of your first grade teacher?
2. In which city or town was your mother born?
3. What street did you live on when you were 8 years old?
4. What was the last name of your third grade teacher?
5. What was your grandmother's occupation?
6. What was your grandfather's occupation?

facebook's security questions screen-shot!

Security Question

Setting a security question helps us identify you as the owner of your Facebook account when you write to us for help.

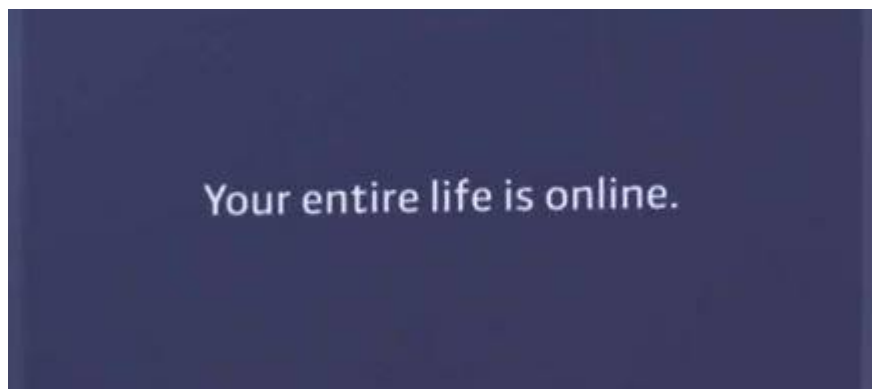
Question:

Answer:

To save these settings, please enter your password:

Password:

excerPts from "mind reader" video



[image: image] <https://www.youtube.com/watch?v=F7pYHN9iC9I>

how to get the answers of these questions?



@boblord

@boblord



Security Pro Tip: Birthday parties are a great time to ask your friends about their first pet, and car. And mother's maiden name.

 Reply
  Retweet
  Favorited
  More

448

RETWEETS

158

FAVORITES



7:05 AM - 18 Aug 13

according to "me"

Following ways work like charm:

- In case of social network, answer can be found on public profile.
- Directly ask the answer via routine Facebook chat ... most of the time you will get the answer.
- Make a QUIZ related to security question and post to your friends.
- In case of family members or close friends, you already know the answer.

another bad security practice

[image: image] <https://www.facebook.com/help/163063243756483>

Question: **What happens if a user realize after answering/setting the question that he has chosen a weak answer?**

Remark: In case of compromised accounts, if attacker has proceeded via answering the security question, he can do the same thing some time after because "QnA" remains same.

Inconsistency in security questions' User interface

The image displays two screenshots of Facebook's security question interface, illustrating an inconsistency in button labels.

Top Screenshot: The title is "Answer Your Security Question". Below it is a progress bar with three steps: "1 Pick a new email", "2 Answer security question" (highlighted), and "3 Choose a new password". The question is "In what city or town was your mother born?". Below the question is a text input field. A link says "Can't remember the answer? Recover your account with help from friends." At the bottom right are two buttons: "Continue" and "Cancel".

Bottom Screenshot: The title is "Answer Your Security Question". Below it is the text "To confirm that this is your account, please answer your security question:". The question is "In what city or town was your mother born?". Below the question is a text input field. At the bottom right are two buttons: "Submit" and "Cancel".

what is your reaction if you have to give an answer to a security question(s) that is not even a part of Facebook's default security

questions' list?

Security Question

Setting a security question helps us identify you as the owner of your Facebook account when you write to us for help.

Question:

Answer:

To save these settings, please enter your password:

Password:

my reaction :-)



security question # 1

Answer Your Security Question

1 Pick a new email 2 Answer security question 3 Choose a new password

What is the first name of the first boy or girl you kissed?

Continue **Cancel**

security question # 2

Answer Your Security Question

1 Pick a new email 2 Answer security question 3 Choose a new password

What was the name of your first pet?

Continue **Cancel**

how can a legitimate user give an answer to a security question that he has never set?

No Way ... BUT

I know the answer that works sometimes :-)

<https://www.facebook.com/ashar.javed> (ajaved)

<https://www.facebook.com/mscashar.javed> (mjaved)

empirical study

Tested real 250 accounts of my friends on Facebook.

In 181 cases, Facebook doesn't allow us to proceed ... It means no security question exposed + no option of trusted friends

In 69 cases, Facebook allows us to PROVIDE a NEW EMAIL ADDRESS and once provided, we can have either security question exposed or trusted friends feature appears or BOTH

181 cases we got ...

Try to Get Access to Your Email

Before you can log in to Facebook, we need to verify who you are. To help us confirm your identity, you need to be able to access one of the email accounts associated with your Facebook account.



Facebook User

Need help accessing email?

If you've lost your email password, follow one of the links below to learn how to reset your email password with major email providers:

- Gmail
- Windows Live Hotmail
- Yahoo! Mail

If your email was provided by a school or business, please contact that organization directly.

[I Cannot Access My Email](#) [Try Again](#)

If as an attacker, we click on "I Cannot Access My Email"

181 cases (No email access ... we are sorry)

No Email Access

We're sorry you're having trouble recovering your email address. Unfortunately, this means we can't verify who you are or give you access to the Facebook account you're trying to log into. We may hide the information on your Facebook account if we detect that you cannot regain access to it.

To learn more about how to access your Facebook account, please see our [Login Problems Help Page](#)

[Done](#)

<https://www.facebook.com/recover/extended/ineligible>

in 69 cases

Facebook exposed the selected security question of the victim

OR

Option of Trusted friends' selection

OR

Choice among above two options

Answer Your Security Question

1 Pick a new email 2 Answer security question 3 Choose a new password

In what city or town was your mother born?

Can't remember the answer? Recover your account with help from friends.

[Continue](#) [Cancel](#)

11 out of 69 accounts compromised

Out of 11 compromised accounts

8 by answering security question

AND

3 using trusted friends feature

ENOUGH FOR POC! # of compromised accounts can be easily raised to 20-25 but requires more work & motivation :-)

some interesting observations

on facebook anybody can send anyone a password reset request if he knows the username which is public information

at the same time denial-of-service (DOS) victim

Check Your Email

Check your email - we sent you an email with a six-digit confirmation code. Enter it below to continue to reset your password.

We sent your code to:
ashar.javed@rub.de

[I didn't receive a code](#) [Continue](#) [Cancel](#)

What if attacker will enter 20-30 times wrong secret code? Attacker doesn't have access to victim's email box in order to get the valid 6 digit code but he has the above dialog box in front of him ...

here you go:

[image: image] "Try again later" will be nasty experience for the victim!

We call this "**Password Reset DoS**"

identify account another way

[image: image] In this way, attacker can force victim to use email address or phone and if victim has lost his email address

worst thing

[image: image] [image: image]

my friend's reaction on worst thing

[image: image]

another type of DoS on Facebook

trusted friend feature dos

If an attacker has started the password recovery using **TF** and at the same time victim tries to use this feature ... he will receive the following message from Facebook

[image: image]

facebook's security measures & how legitimate users react & their bypasses

this is how common users use facebook...

[image: image]

1) Security Alert via Email or Mobile SMS

As soon as attacker starts an account recovery via "**password reset**" functionality, Facebook immediately sends an email or sms alert to the legitimate user.

users' reaction on this email or sms

[image: image] [image: image] [image: image]

users' reaction on this email or sms

[image: image]

2) Temporarily Locked

[image: image] [image: image] In order to recognize device, Facebook uses **OS, IP Address, Browser & Estimated Location** etc.

What happens if attacker clicks on "**Continue**" button?

What happens if an attacker clicks on "**Continue**" button?

(1)

[image: image]

(2)

[image: image]

Click "**Continue**" after selecting one of the option but remember who is doing selection?

An ATTACKER

(3)

[image: image]

(4)

[image: image]

(5)

[image: image]

(6)

[image: image]

(7)

[image: image]

(8)

[image: image]

another interesting aspect in case if legitimate user will be able to regain access to his account

[image: image]

remember (5th step) i.e.,

[image: image]

snapshot of attacker's email box

[image: image]

recognized devices

[image: image]

3) 24 Hour Locked-out Period

As an attacker this is the biggest hurdle to cross ...

[image: image]

disavow process

Legitimate user can "**disavow**" the process any time by clicking on the link in the email he received from Facebook or *making Facebook activity during this time*.

BUT

Majority of the users, as shown in users' reaction consider Facebook's informative/warning emails as spam.

for a moment forgot disavow

[image: image]

24 hour locked out period starts like that ...

[image: image]

24 hour locked out period ...

[image: image]

24 hour locked out period ...

[image: image]

24 hour locked out period ...

[image: image]

game over for victim...

[image: image]

here we go...

[image: image]

Another email from facebook and leaked email address of the victim

[image: image]

Ethical Considerations

First Reported to Facebook on 19-08-2012

On 23-08-2012, I got the following answer from Facebook Security Team:

[image: image]

two questions came to my mind after reading the email...

Is there any attack that is not very well targeted?

Where is social engineering in this attack?

on 24-08-2012

[image: image]

but i have waited until the complete empirical study & again sent the technical report/research paper on 27-06-2013

[image: image]

answer from security team on 09-09-2013

[image: image]

sorry facebook :-)

It doesn't make sense to reproduce this attack on TEST ACCOUNTS...

The results would look like FAKE.

on the other hand ...

Our approach is similar to a recently published academic paper in Second International Workshop on Privacy and Security in Online Social Media Co-located with WWW 2013 (<http://precog.iiitd.edu.in/events/psosm2013/9psosm3s-parwani.pdf>)

[image: image]

finally

All compromised accounts are up, running and under the control of their legitimate users!

[image: image]

yet another observation i.e., masked email address and phone

[image: image]

where is masking? email address exposed

[image: image]

after 5-10 minutes masking affect appears

[image: image]

what about other 49 social networks' password reset functionality?

twitter (<https://twitter.com/?lang=en>)

[image: image] 200 million active users (Feb 2013) + Alexa Rank #11 (<http://en.wikipedia.org/wiki/Twitter>)

anybody can send anybody a password reset request with the help of twitter's username which is public information :-)

[image: image]

just for fun ...

[image: image]

i reported this to twitter security team & this is what they think about it

[image: image][image: image]

but now twitter has ...

[image: image]

Mat Honan's story

[image: image] <http://www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking/all/>

support teams

[image: image]

support team's job

To help customers ...

[image: image]

can also be used to compromise accounts :-)

our methodology by keeping in mind threat model

Registered the following email address on social networks:

user1@bletgen.net

AND

The following is the attacker's address and goal is to compromise the victim's account labelled with above email address

jim@mediaob.de

Attacker's address is not even registered on social networks!

Academia (<http://www.academia.edu/>)

[image: image]

our email to academia

[image: image]

initial response from academia

[image: image]

final response of academia support team

[image: image]

FreizeitFreunde (A german-specific social networking site) (<http://www.freizeitfreunde.de/>)

[image: image]

our email to them ...

[image: image]

FreizeitFreunde's support team response

[image: image]

lokalisten (a german social networking site)(<http://www.lokalisten.de/>)

[image: image]

initial response on our ticket

[image: image]

our response without ""date of birth""

[image: image]

lokalisten's support team final response

[image: image]

meetup (<http://www.meetup.com/find/>)

[image: image]

support team blocks account :)

[image: image]

getglue (social networks for tv fans) <http://getglue.com/feed>

[image: image]

our email to their support team

[image: image]

getglue's support team response

They set the new password for us i.e., "temp" :)

[image: image]

Delicious (<https://delicious.com/>)

[image: image]

Delicious's support team response

They have switched the email address from victims' to an attacker controlled email address and have sent password reset link to the attacker's email address.

[image: image]

facebook as sso

Out of 50 surveyed social networks, we found

**26 use Facebook as login-provider (SSO)

24 don't have this feature

Implications of Facebook Connect

(1 Million websites have integrated with Facebook)*+ account hack

- Controls email account e.g., Yahoo
- Go for shopping e.g., Etsy
- Create havoc for victim :)
- 79% of social media log ins by online retailers are with Facebook (<http://socialmediatoday.com/node/1656466>)
- 60 million users of Facebook Connect in 2009 according to Tech Crunch report (<http://goo.gl/a6lsCx>)
- <http://goo.gl/x8BKe>

havoc examples

[image: image]

<http://goo.gl/2FVTz8>

[image: image] <http://goo.gl/uuO7Kq>

Guidelines for users

- Do not ignore email or SMS alert from Facebook
- Do not place TOO MUCH information on social network
- Do not accept friend requests from strangers
- Enable log-in notifications

Guidelines for social networks

- Train your support teams.
- Facebook should raise the bar as far as communication with the researchers or bug submitters is concerned.
- For Facebook: Please don't send TOO MANY EMAILS because users start believing that these are spam emails.
- Joe wrote in his post (<http://goo.gl/Wf6QMZ>):[image: image]

- In case of **TFA**, Facebook failed in "CORRECTLY IDENTIFYING and REALIZATION OF AN INFORMATION FLOW PROBLEM"

for facebook

[image: image]

I hope now facebook security team's reaction

[image: image]

demo

YET Another observation

[image: image]

reveal my trusted contacts reveals

[image: image]

thanks!

[image: image]

trusted friend attack:

By Ashar Javed

Archived from <http://web.archive.org/web/20160507023636/http://slid.es/mscasherjaved/trusted-friend-attack>.
Rendered offline from the local Markdown copy.