TRUSTED FRIEND
ATTACK:
GUARDIAN ANGELS STRIKE

A talk by Ashar Javed
@
Hack In The Box, 14 - 17 October 2013
Kuala Lumpur, Malaysia (HITBSecConf2013)
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

Password Reset Unavailable

Password reset is unavailable for this user. If you think this is an error, please go back and try searching for your account again.

Try again  Cancel
A SHORT STORY

https://twitter.com/dimitribest/status/230677638358900736
#100k Hacked Facebook Accounts


DOWNLOAD | RAW | EMBED | REPORT ABUSE | PRINT

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."

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"
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

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:

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

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.
STEP (6)
Welcome to Facebook, MSc. Ashar
Hi MSc Ashar,

Your Facebook password was reset using the email address ashar.javed@rub.de on Friday, September 13, 2013 at 4:04pm (UTC+02).

Operating system: Windows
Browser: Opera
IP address: [Redacted]
Estimated location: Witten, NW, DE

If you did this, you can safely disregard this email.

If you didn't do this, please secure your account.

Thanks,
The Facebook Security Team
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

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"

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

If you lose access to your account or are having problems logging in, a code can be sent to your friends to help you get back into your account. You can pre-select these friends from the Account Settings page.

How Trusted Friends Feature Works?

Recover Your Account Through Friends

The only way to prove that this is your account is to show that your friends know you. More

You’ll need to:

Step 1  Choose 3 trusted friends
Step 2  Call your friends to get security codes.
Step 3  Recover your account.

This process takes a few minutes for your friends.

To learn more about this process, visit our Help Center.

Continue  Cancel
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
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

[Image: Screen showing a list of friends with checkboxes]
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@XXX.com for next steps and a link back to this page.
Call [REDACTED] and give him this code.

Security Code: 8120

[REDACTED] (or someone impersonating [REDACTED]) has requested access to your Facebook account. To help confirm who owns this account, please call [REDACTED] and give him this code.

For [REDACTED]'s security, please be sure to talk to him in person or on the phone. Don't send this code by email or SMS.
Dear [Name],

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:
   * [Redacted]
   * [Redacted]
   * [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]&if=[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

you@example.com

Do it!

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 also change who your trusted friends are at the same time? Wouldn't that make the whole security measure kinda pointless?
QUESTION YOU MIGHT THINKING ...

WHERE IS THE PROBLEM?
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
FACEBOOK FRIEND VS REAL LIFE FRIEND

DON’T GET FOOLLED BY PHONY “FRIENDS”

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

Fraudsters use social sites because they know that 50% of people will accept a “friend” invitation from a stranger.

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.
On average a Facebook user has 342 friends!

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

He had over 2000 Facebook friends. I was expecting a bigger turnout.
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) :) 

![Dialog Box](https://www.facebook.com/recover/extended)

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.
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.,

1. Answer Security Question
2. Choose Three Friends of Attacker's Choice
1. **Involve one attacker** i.e., the case where attacker will answer the exposed security question
2. **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

lsd=AVo8FV8K&profileChooserItems={"511543064":1}&checkableitems[]=511543064

511543064 is my Facebook numeric ID.
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!
EVIL IDEA

URL looks like:
https://www.facebook.com/guardian/confirm.php?
cuid=AYhhCnxPb9g8xVAUGmuPh4e33s2NcCRj8Qng7wKGN7fxe9hXTQtVUKr0Rm-0LBeTOCX_Es83IN0_BGe8Yi2GG7iGRbzwl5rNXktD1mSsnW-ZFD2fZB1Z7IlyyYdQ4GPbf9bzhik9zXBpNeOsvUv-MpzCcAQT2jxLte25YGlq_gq&cp=testpurposexss@gmail.com
EVIL IDEA DOESN’T WORK

Facebook correctly says:

The link you clicked is invalid or expired.
INTERESTING MESSAGE FROM FACEBOOK


For security reasons, you cannot choose this person. Please select a different friend.
I think it means that if an attacker selects himself or any particular account 3 to 5 times for different victims, then Facebook's block access to the particular account!
Dear [Name],

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 email includes 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:
http://www.facebook.com/guardian/validate.php

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:

Thanks,
The Facebook Team
COMBINING THE PIECES OF ATTACK

Post Data Manipulation
+
URI Manipulation

Victim has no idea who has started the recovery procedure, whom should I contact for secret codes ...
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!
EXCERPTS FROM 'MIND READER' VIDEO

Your entire life is online.

And it might be used against you.

https://www.youtube.com/watch?v=F7pYHN9iC9I
HOW TO GET THE ANSWERS OF THESE QUESTIONS?

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

Can I update my security question?
We want to make sure that your account and the information in it stays safe, so once you set up a security question on your account there's no way to update it. Sorry for the inconvenience.

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**

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

Answer Your Security Question

To confirm that this is your account, please answer your security question:

In what city or town was your mother born?

Submit  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?
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?

[Input field]

[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 :-)
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 ...

If as an attacker, we click on "I Cannot Access My Email"
181 CASES (NO EMAIL ACCESS ... WE ARE SORRY)

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
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.
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 ...

AT THE SAME TIME DENIAL-OF-SERVICE (DOS) VICTIM

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:

"Try again later" will be nasty experience for the victim!

We call this "**Password Reset DoS**"
In this way, attacker can force victim to use email address or phone and if victim has lost his email address ....
Finally got my FB account back
Phew ..
ANOTHER TYPE OF DOS ON FACEBOOK
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

An account recovery process has already been initiated for this account. Please check the email you provided for further instructions.
FACEBOOK'S SECURITY MEASURES & HOW LEGITIMATE USERS REACT & THEIR BYPASSES
THIS IS HOW COMMON USERS USE FACEBOOK...

1. Click picture
2. Write "jump"
3. See what happens
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

This email look a scam. I have also received such a email few days ago having some of my friends name which i have ignored as facebook has no such service. No one has contacted me in this regard. For further detail u may visit facebook official page https://www.facebook.com/help/?page=211375822230657

Suspicious Emails and Notifications
Facebook Help Center
- Suspicious Emails - Suspicious Notifications -

August 28 at 5:33am · Like · 2

I even got one SMS from "FACEBOOK" on my mobile with a link to reset password, which I Just ignored... the scam is getting hot i think...

about an hour ago · Like · 1

hmm....i just rushed to my laptop....phewwww

August 28 at 10:59am · Unlike · 2
I don't need to change my password or the email address... I request all the friends not to participate in any activity like this on my profile.
2) TEMPORARILY LOCKED

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?
Someone May Have Accessed Your Account

To secure your account, you’ll need to answer a few questions and change your password.

For your protection, no one can see you on Facebook until you finish.

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

**An ATTACKER**
Please Confirm Your Identity

To confirm your identity, please answer your security question:

In what city or town was your mother born?

Answer:  

[Continue] [Back]
Create a Unique Password

Thanks for confirming your identity. Please create a new password that you don’t use on any other site.

New Password

Confirm Password

Continue
Review Your Emails

Please select the emails that belong to you.

☑️ [redacted]@yahoo.com
☑️ testingpasswordnew@hotmail.com

If none of the emails belong to you, you can add a new email instead.

Add a new email: 

Continue
Are you sure this email is secure?

Anyone who knows the password for testingpasswordnew@hotmail.com will be able to hack your Facebook account. Please change the password for your email account if you believe someone else can access it.

☐ Only I know the password for testingpasswordnew@hotmail.com (Change password now)
Review Recent Name Changes

Your name was changed while your account may have been hacked. Please select your name from the list below.

Name: 

Continue
Account Unlocked - Now You Can Log In

Thanks for fixing your account information. Your account is unlocked and your information has been restored.

Turn On Extra Security Features

- [x] Browse Facebook on a secure connection (https) whenever possible
- [ ] Send me an email if someone logs into my account from an unknown device

[Log In]
Another interesting aspect is that in case if a legitimate user will be able to regain access to his account.
REMEMBER (5TH STEP) I.E.,

Review Your Emails

Please select the emails that belong to you.

☐ [Redacted]@yahoo.com
☐ testingpasswordnew@hotmail.com

If none of the emails belong to you, you can add a new email instead.

Add a new email:

Continue
SNAPSHOT OF ATTACKER’S EMAIL BOX
You won't get notified or have to confirm your identity when logging in from these devices:

### This device:

- **new laptop mine**

### Other devices:

- Facebook for iPad
  - April 2, 2013 · Remove
  - January 24, 2013 · Remove
  - December 29, 2012 · Remove
  - December 29, 2012 · Remove
  - December 22, 2012 · Remove
  - December 11, 2012 · Remove
  - August 12, 2012 · Remove
  - June 15, 2012 · Remove
  - May 13, 2012 · Remove
  - April 23, 2012 · Remove
  - March 25, 2012 · Remove
  - March 7, 2012 · Remove
  - March 5, 2012 · Remove
  - November 26, 2011 · Remove
  - October 23, 2011 · Remove
  - September 28, 2011 · Remove
  - September 4, 2011 · Remove
  - August 31, 2011 · Remove
3) 24 HOUR LOCKED-OUT PERIOD

As an attacker this is the biggest hurdle to cross ...
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.
Please check your email

Congratulations, you have successfully proved your identity.

An email was sent to testpurposексs@gmail.com. Click on a link in that email to continue your account recovery process.

If you have not received an email in 30 minutes, see the Help Center.
24 HOUR LOCKED OUT PERIOD STARTS LIKE THAT ...
24 HOUR LOCKED OUT PERIOD ...

Please come back in 5 Hours and 10 Minutes

You’ve successfully confirmed your identity. For your security, you must wait before you can access your account.

Please come back in 5 Hours and 10 Minutes by logging in using your new email and password.
24 HOUR LOCKED OUT PERIOD ...

Please come back in 1 Hour

You've successfully confirmed your identity. For your security, you must wait before you can access your account.

Please come back in 1 Hour by logging in using your new email and password.
24 Hour Locked Out Period ...
GAME OVER FOR VICTIM...
HERE WE GO...
Another email from Facebook and leaked email address of the victim
ETHICAL CONSIDERATIONS

First Reported to Facebook on 19-08-2012
On 23-08-2012, I got the following answer from Facebook Security Team:

Re: Report a Possible Security Vulnerability
From Facebook Security
To ashar.javed@rub.de
Date 2012-08-23 22:46
Priority Normal

Hi Ashar,

We're well aware of the potential weaknesses of security questions in a very targeted attack like you have described below. Unfortunately, they are necessary recovery option for some accounts. Account recovery through the security question is presented as a last resort recovery mechanism. In addition to the 24 hour look out period, it's worth noting that we email and SMS dissavow recovery options to the original account owner.

Despite the disadvantages of security questions, they are an extremely necessary part of our account recovery flows. We are unable to completely support for them at this time. The scenario you are describing requires a considerable amount of social engineering and does not qualify under our bounty program. Sorry.

Thanks, please let me know if you have any questions.

Security
Facebook
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?
Re: Report a Possible Security Vulnerability

From        Facebook Security  
To          ashar.javed@rub.de  
Date        2012-08-24 00:43 
Priority    Normal             

Hi Ashar, 

Please feel free to discuss your research publicly. Thanks!

Security
Facebook
Hi Ms Ashar,

I've looked through the whole paper and plan on following up with some of our Site Integrity engineers about some of the points you raised. But you covered a lot of ground - can you try to condense the primary points that you view as a vulnerability here? Is the main point of this report simply that you believe the 3 friends recovery flow allows for account takeover and thus creates a vulnerability in its present form? Or are there more issues you're raising here?

Thanks,

Security
Facebook
Hi MSc Asfar,

The investigating team asked if you could repro this with new test accounts. Additionally, what is your relationship with the owners of the real accounts that you had compromised?

Thanks,

Security
Facebook
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)
FINALLY

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

We didn’t read any other data from the compromised accounts: We didn’t read any messages or delete any data, we didn’t look at private pictures, we didn’t change passwords, we didn’t make any status updates from these accounts, and we will not disclose the real names of compromised accounts in public.
YET ANOTHER OBSERVATION I.E., MASKED EMAIL ADDRESS AND PHONE #
WHERE IS MASKING? EMAIL ADDRESS EXPOSED
AFTER 5-10 MINUTES MASKING AFFECT APPEARS
WHAT ABOUT OTHER SOCIAL NETWORKS’ PASSWORD RESET FUNCTIONALITY?
TWITTER (HTTPS://TWITTER.COM/?LANG=EN)

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 :-(

---

Forgot your password?

Enter your email address or phone number:

---OR---

Enter your username:

Submit

Need help? Please contact Twitter Support.
John Wilander @johnwilander
I just got a password reset email from Twitter. The problem is I didn't request one. If you start seeing bogus tweets, you know why!

10:37 PM - 20 Aug 12 via Twitter for iPhone · Details
I reported this to Twitter security team & this is what they think about it.

Randy Janinda
@janinda

I'll give this info to the password folks, see what they think. It may be they decided it was an acceptable risk given the use cases.

05:53 PM - 20 Aug 12

Randy Janinda
@janinda

It has been determined to be an acceptable risk since there are other ways to get the info as well. That's all I've been told.

10:55 PM - 23 Aug 12
BUT NOW TWITTER HAS ...

Security and privacy
Change your security and privacy settings.

Security

Login verification

Password reset

☑️ Require personal information to reset my password
By default, you can initiate a password reset by entering only your @username. If you check this box, you will be prompted to enter your email address or phone number if you forget your password.
How Apple and Amazon Security Flaws Led to My Epic Hacking

BY MAT HONAN 08.06.12  8:01 PM

http://www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking/all/
SUPPORT TEAMS
SUPPORT TEAM’S JOB

To help customers ...
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/)
On Fri, Mar 15, 2013 at 6:08 AM, Jim Raynor <jim@mediaob.de> wrote:
Dear Supportteam,

my Email user1@bletgen.net were hacked and my academia password were changed.

Is there anyway for me recovering my account?

Regards, Jim
Hi Jim,

Which email would you like on your account: http://rub.academia.edu/JimRaynor
Once you send me the email you would like, I can edit this information for you. Then we can work on a new password.

Thanks for contacting Academia.edu,
Hi Jim,

I have changed your email on your account to: jim@mediaob.de
Now you can request for a reset password link here: http://www.academia.edu/reset_password
Remember that the link you will be sending to your email will only work once.

Thanks for contacting Academia.edu,
FREIZEITFREUNDE (A GERMAN-SPECIFIC SOCIAL NETWORKING SITE)
(HTTP://WWW.FREIZEITFREUNDE.DE/)
-----Ursprüngliche Nachricht-----
Von: kontakt@freizeitfreunde.de [mailto:kontakt@freizeitfreunde.de] im Auftrag von: jim@mediaob.de
An: Freizeitfreunde
Betreff: freizeitfreunde.de: Technik: Account

Jim Raynor hat über das Kontaktformular
(http://www.freizeitfreunde.de/de/footer/kontakt/kontakt.html) folgende Nachricht versendet:

Hallo liebes Support-Team,
ich habe leider keinen Zugang mehr zu meiner Emailadresse user1@bletgen.net, da sie gehackt wurde. Sogleich wurde auch mein Kennwort für FF geändert. Ist es möglich ein temporäres Kennwort für FF zu erhalten, so dass ich mich wieder anmelden kann?

Danke und Gruß
Jim
Sehr geehrter Herr Raynor,

gerne kommen wir Ihrer Bitte nach. Ihr neues Passwort lautet: jray022

Mit freundlichen Grüßen
Ihr Freizeitfreunde-Team
LOKALISTEN (A GERMAN SOCIAL NETWORKING SITE)

(HTTP://WWW.LOKALISTEN.DE/)
hallo,

für den Fall, dass du keinen Zugriff mehr auf deinen Account hast, benötigen wir folgende Daten von dir, um deine Email-Adresse zu ändern:

- deinen Spitznamen,
- deine bei der Registrierung angegebene und aktuelle Email-Adresse
- deine aktuelle Email-Adresse.

Zur Verifizierung bitten wir dich um die Angabe deines vollständigen Namens, deines Wohnortes und deines Geburtsdatums.

Wir können dann die Email-Adresse in das Profil eintragen und du kannst dir dann ein neues Passwort setzen.

Viele Grüße

Dein Lokalisten Team
Jim Raynor <jim@mediaob.de> schrieb:

Hallo,

mein spitzname ist JimRaynor. Alte Email user1@pletgen.net, neue Email jim@mediaob.de, mein Wohnort ist Berlin.

Viele Grüße
hallo,

wir haben gerade deine neue emailadresse ins profil eingetragen.

viele grüße
dein lokalisten team
MEETUP

(HTTPS://WWW.MEETUP.COM/FIND/)
Hello Jim,

Thanks for contacting us about this, and I'm sorry to hear this.

I've gone ahead and blocked the account that was associated with the email address you reference here. In this case, your best bet will be to create a new Meetup account associated with a brand new email address. Please be sure to create a new password as well and be sure not to share that information with anyone.

I hope this helps, and again I'm sorry to hear about this. Please let us know if there's anything else we can help with from here.

Sincerely,

[Redacted]

Community Specialist
Meetup HQ
GETGLUE (SOCIAL NETWORKS FOR TV FANS)  
HTTP://GETGLUE.COM/FEED
Dear Supportteam,

my Email user1@bletgen.net were hacked and my GetGlue password were changed. Is there anyway for me recovering my account?

Regards,
Jim
GETGLUE’S SUPPORT TEAM RESPONSE

They set the new password for us i.e., "temp" :)
“Delicious has been essential for me. The more bookmarks I save, the more valuable the service becomes.”

—Charlie Hoehn, Writer and Marketing Strategist

Create a free account or learn more about how Charlie uses Delicious.

Delicious is an easy, free tool to save, organize, and
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.

Hi Jim,

Not a problem! We've switched your account's email address to jim@mediaob.de and send you a reset link there instead.

Cheers,
Team Delicious
Out of 50 surveyed social networks, we found 26 use Facebook as login-provider (SSO) and 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

http://goo.gl/2FVTz8

Facebook Causing Divorce Numbers To Skyrocket

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):

  I’ve reviewed our communication with this researcher, and I understand his frustration. He tried to report the bug responsibly, and we failed in our communication with him. We get

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

Upload a photo ID

To make sure this is your account, we need you to upload a color photo of your government-issued ID. Your ID should include your name, birthday and photo.

Acceptable IDs include your:
- Passport
- Driver's license
- State-issued ID card
- Military ID card
- Immigration ID with signature

We won't accept:
- Your profile picture
- Everyday pictures
- Clip art

I don't have an ID

Continue  Go Back
I HOPE NOW FACEBOOK SECURITY TEAM’S REACTION

OHH

NOW WE GOT IT!
THANKS!