TRUSTED FRIEND ATTACK:

GUARDIAN ANGELS STRIKE

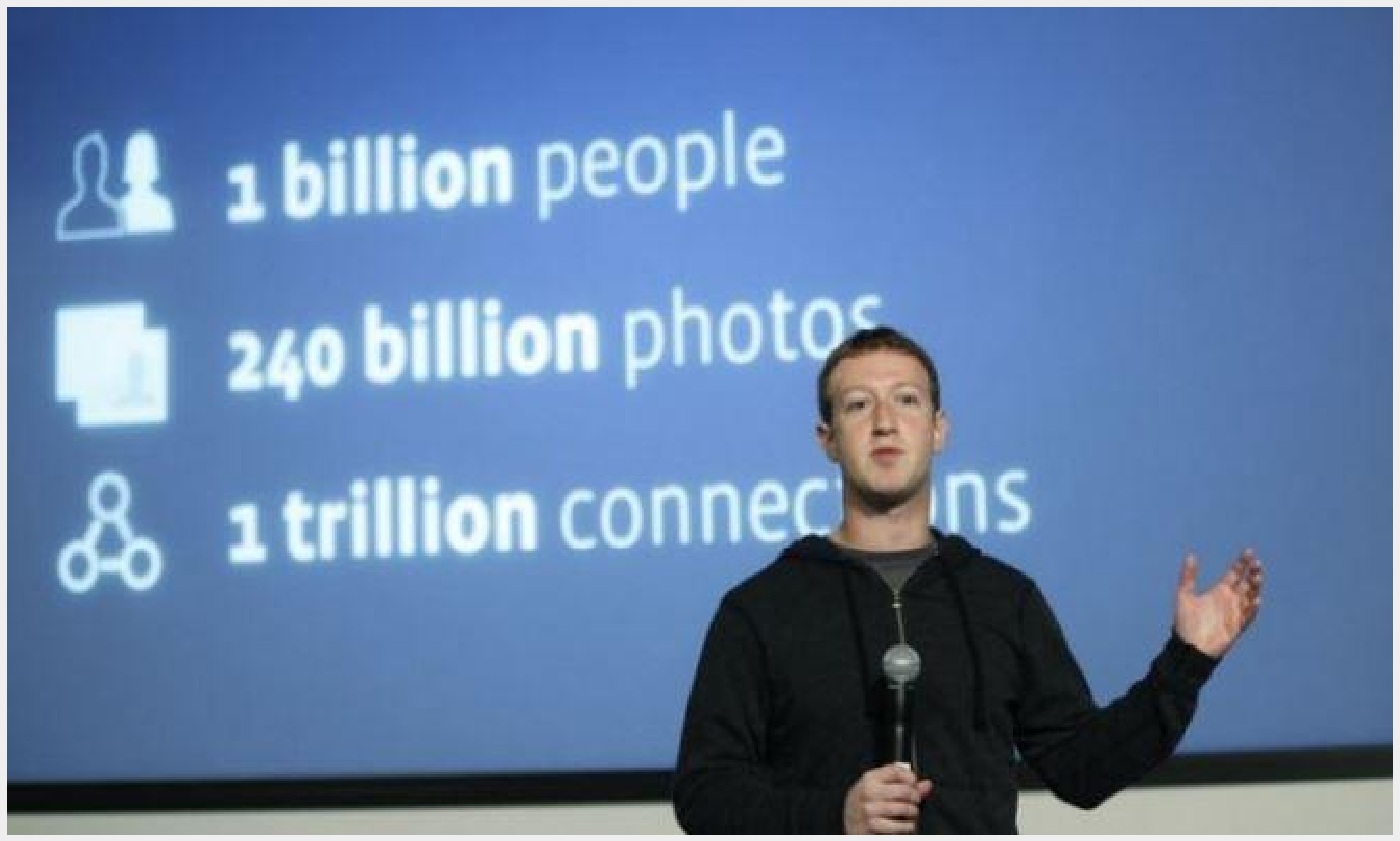
A talk by **Ashar Javed**

@

Hack In The Box, 14 - 17 October 2013

Kuala Lumpur, Malaysia (HITBSecConf2013)

GRAPH IS BIG



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

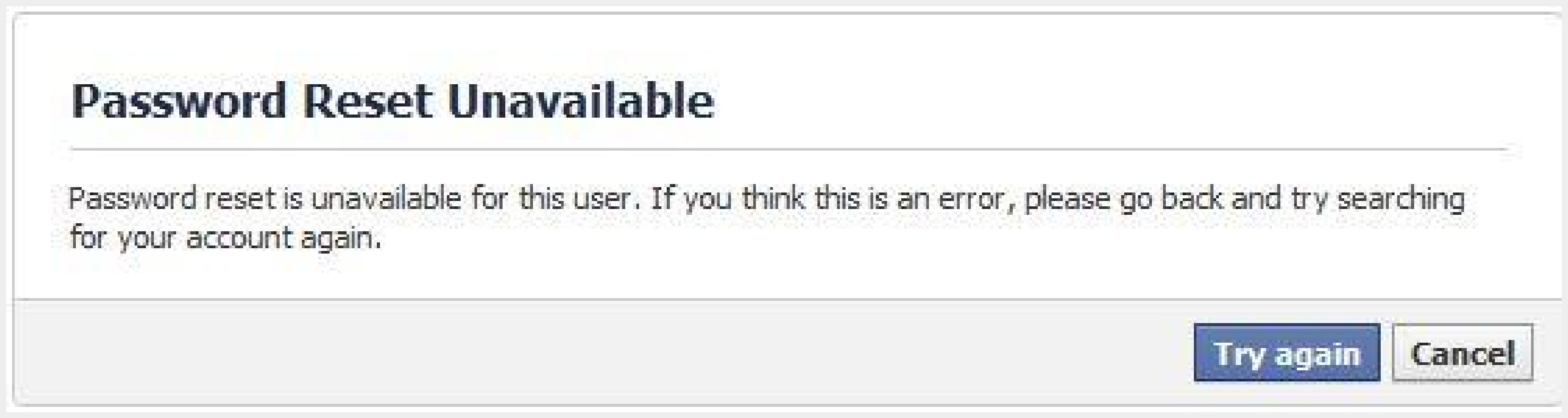
WHO AM I?

- A RESEARCHER IN R UHR- U NIVERSITY B OCHUM, 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

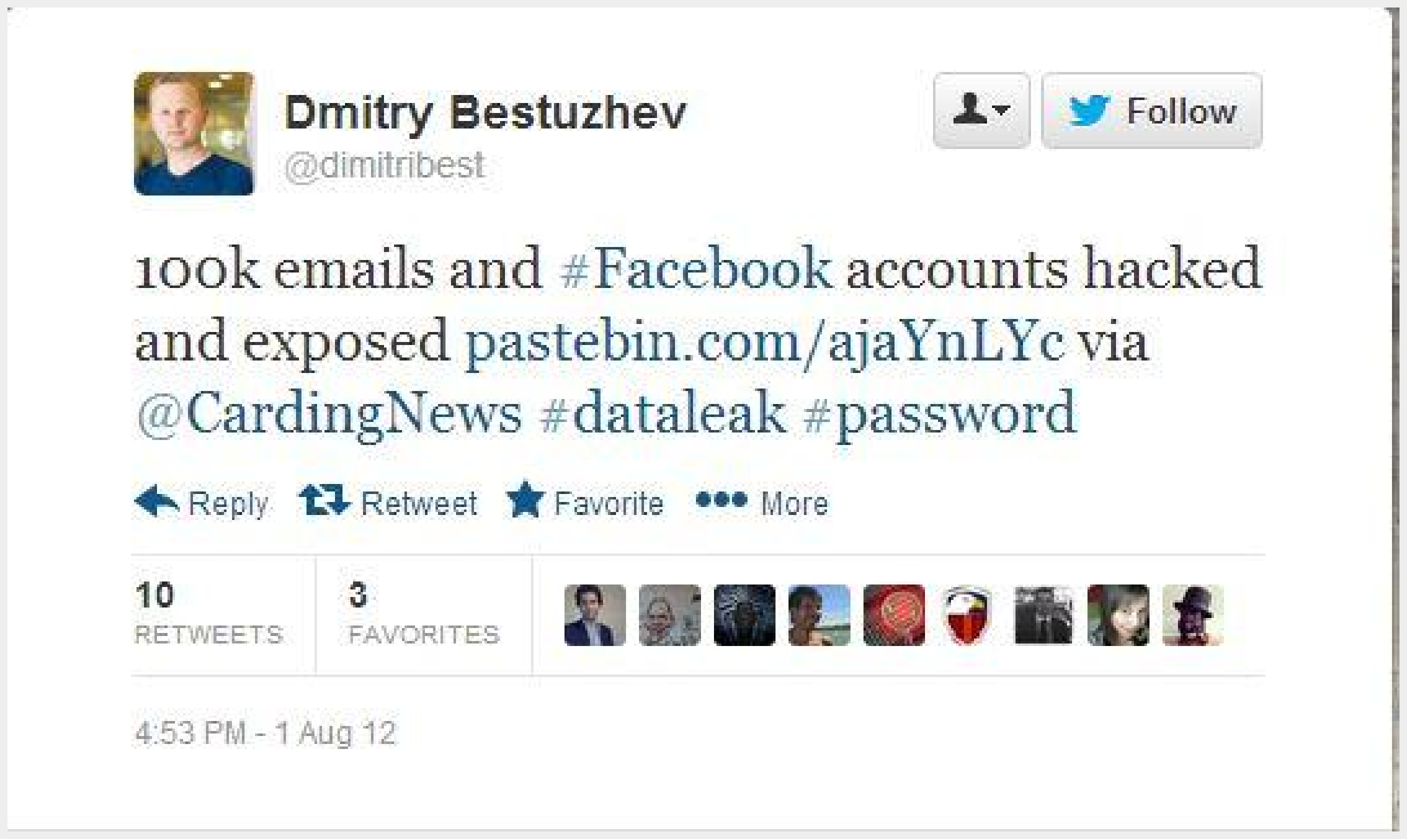
...



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.

A SHORT STORY



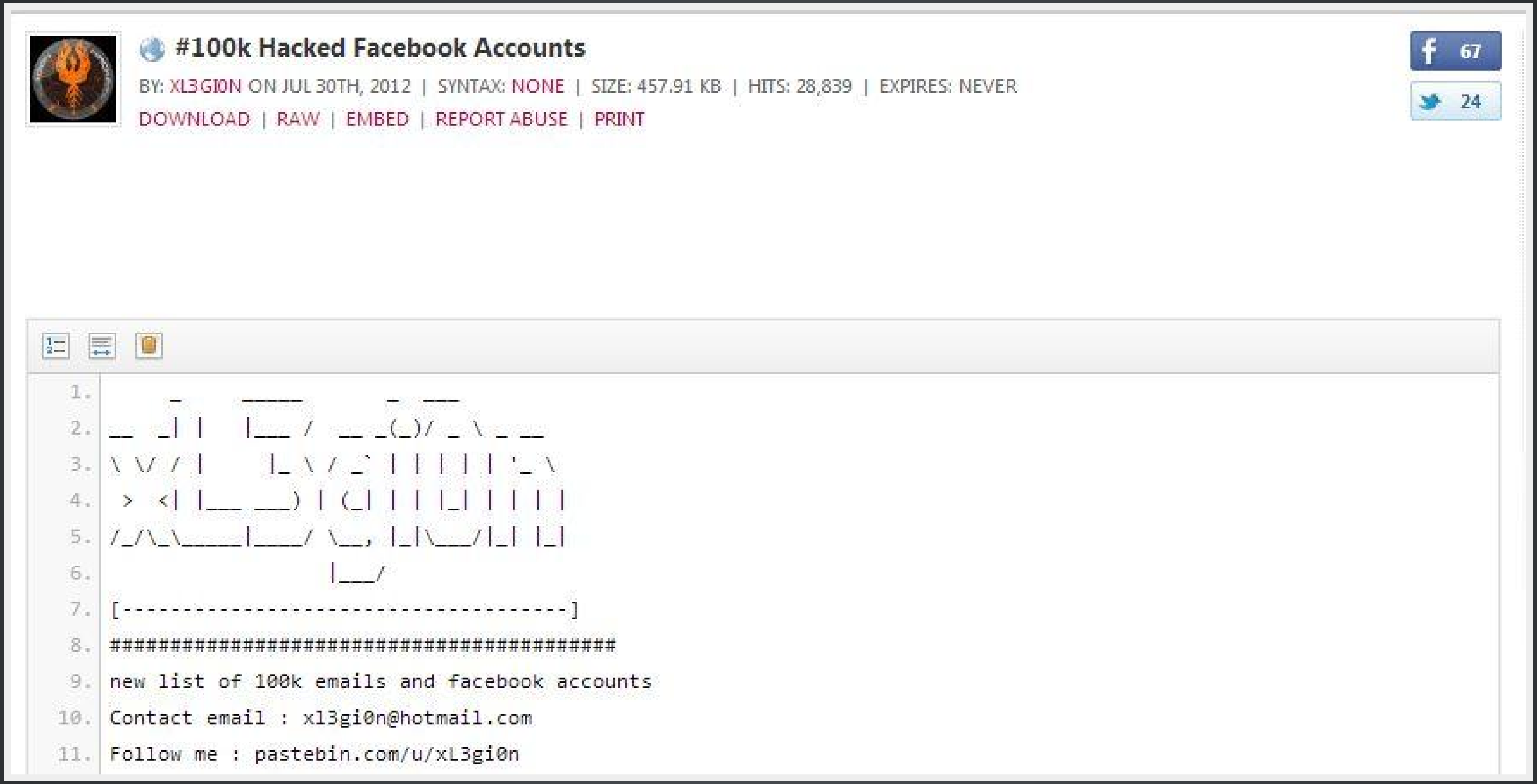
Dmitry Bestuzhev
@dimitribest

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

4:53 PM - 1 Aug 12

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

A PASTE@PASTEBIN



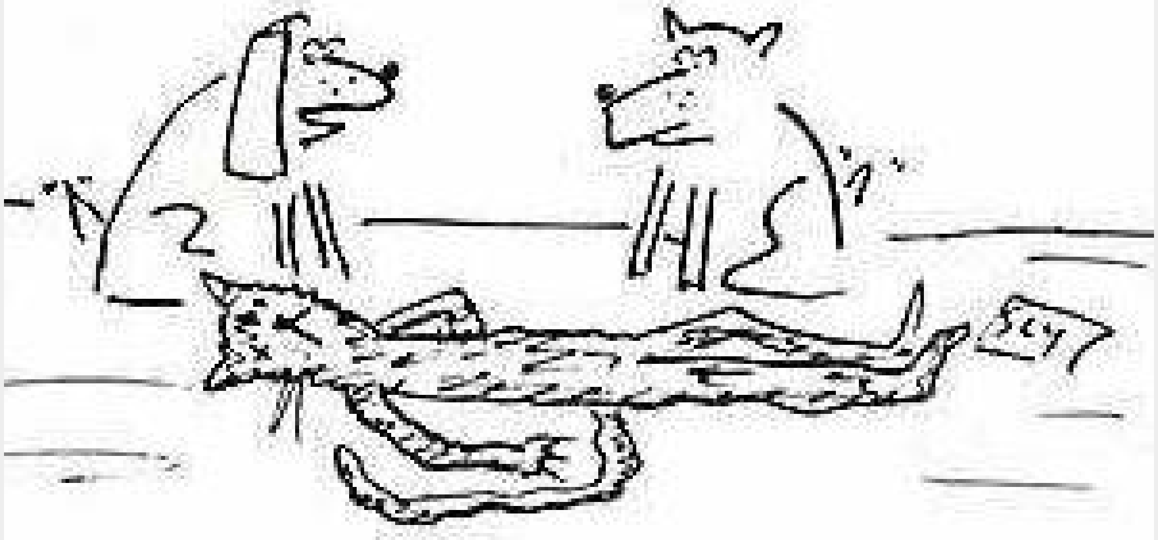
#100k Hacked Facebook Accounts

BY: XL3GI0N ON JUL 30TH, 2012 | SYNTAX: NONE | SIZE: 457.91 KB | HITS: 28,839 | EXPIRES: NEVER

```
       _     _____       _  ___
__  __| |   |___ /  __ _(_)/ _ \ _ __
\ \/ / |     |_ \ / _` | | | | | '_ \
 >  <| |___ ___) | (_| | | |_| | | | |
/_/\_\_____|____/ \__, |_|\___/|_| |_|
                  |___/
[-------------------------------------]
##########################################
new list of 100k emails and facebook accounts
Contact email : xl3gi0n@hotmail.com
Follow me : pastebin.com/u/xL3gi0n
```

http://pastebin.com/ajaYnLYc

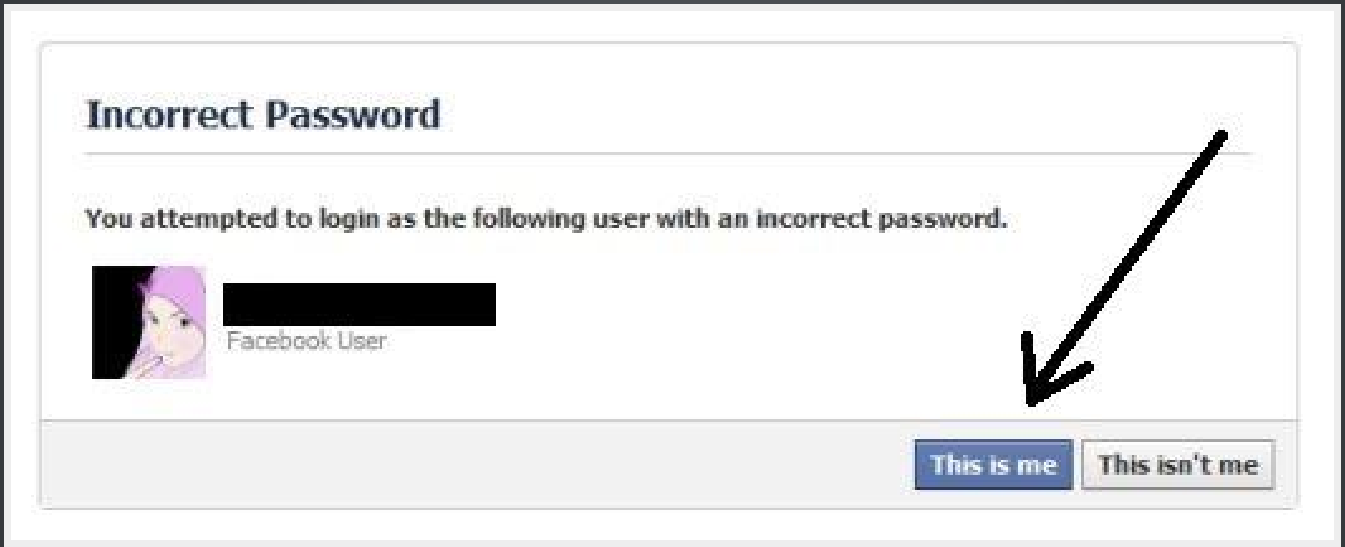
WHO TO BLAME?



"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



Incorrect Password

You attempted to login as the following user with an incorrect password.

[redacted]

Facebook User

AN INNOCENT QUESTION ...

Why is Facebook asking on somebody's account?

This is me
This isn't me

&

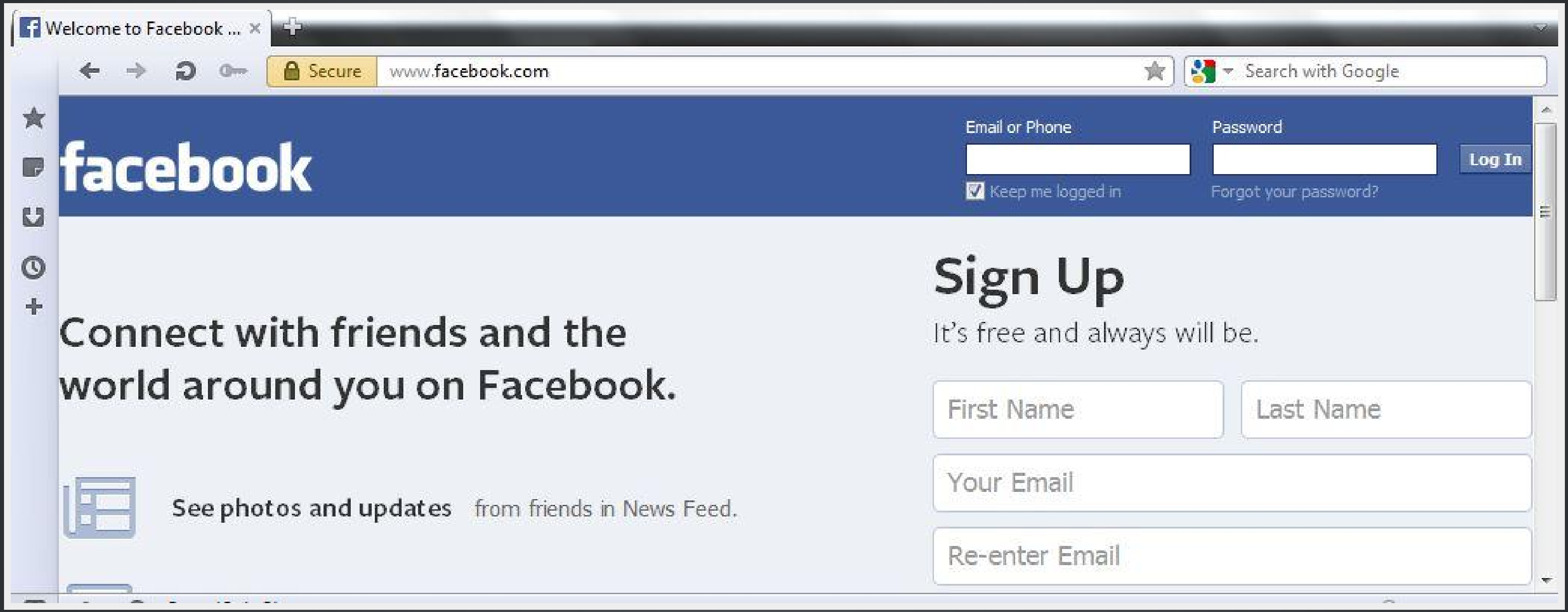
What would be your answer, **if you are an attacker** :-)

LEGITIMATE PASSWORD RECOVERY FLOW

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

STEP (1)

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



Connect with friends and the world around you on Facebook.

See photos and updates from friends in News Feed.

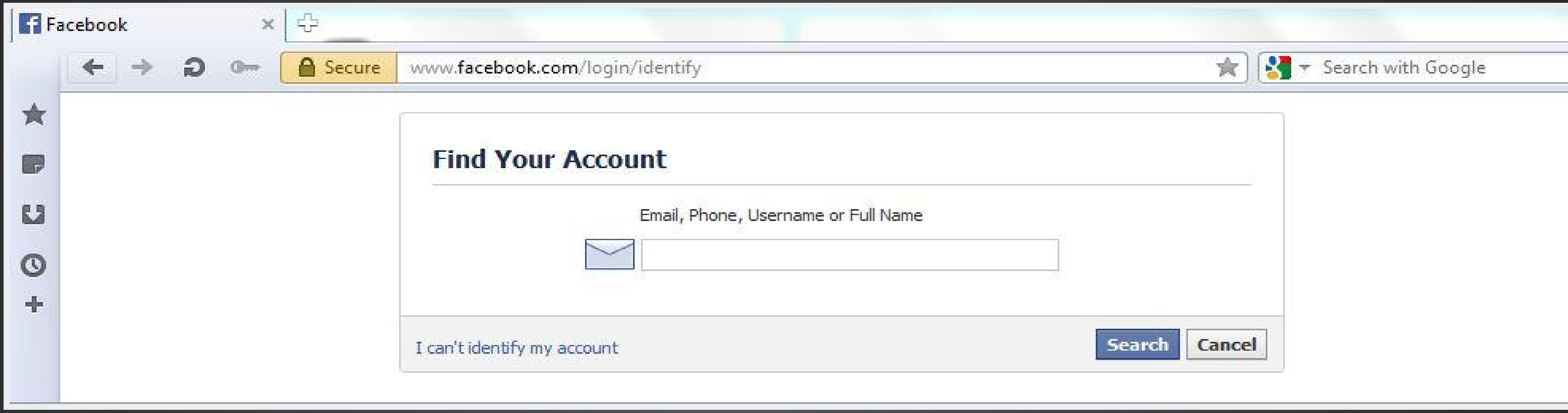
Sign Up

It's free and always will be.

Click "**Forgot Your Password?**"

STEP (2)

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



Find Your Account

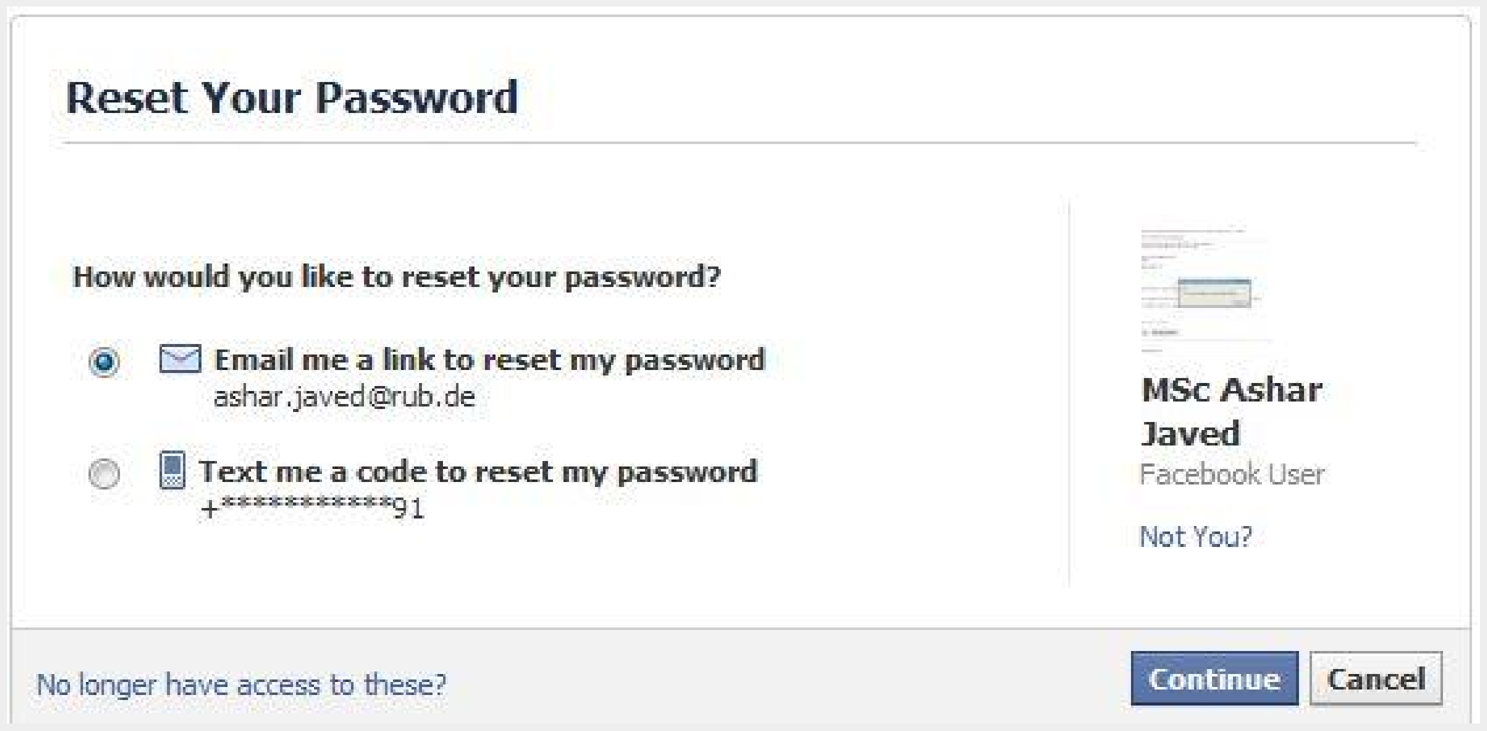
Email, Phone, Username or Full Name

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?

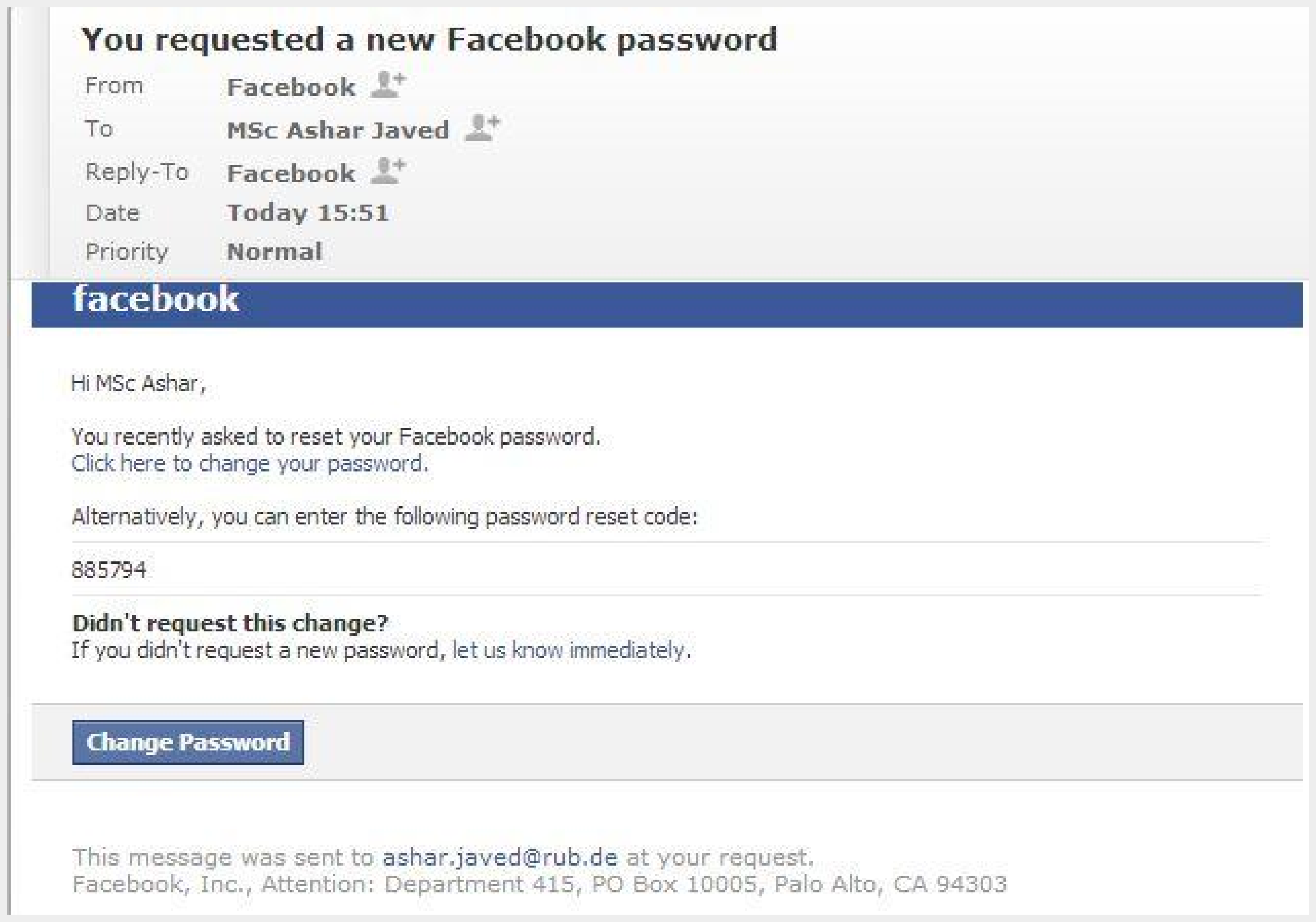
● Email me a link to reset my password
ashar.javed@rub.de

○ Text me a code to reset my password
+************91

MSc Ashar Javed
Facebook User

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:

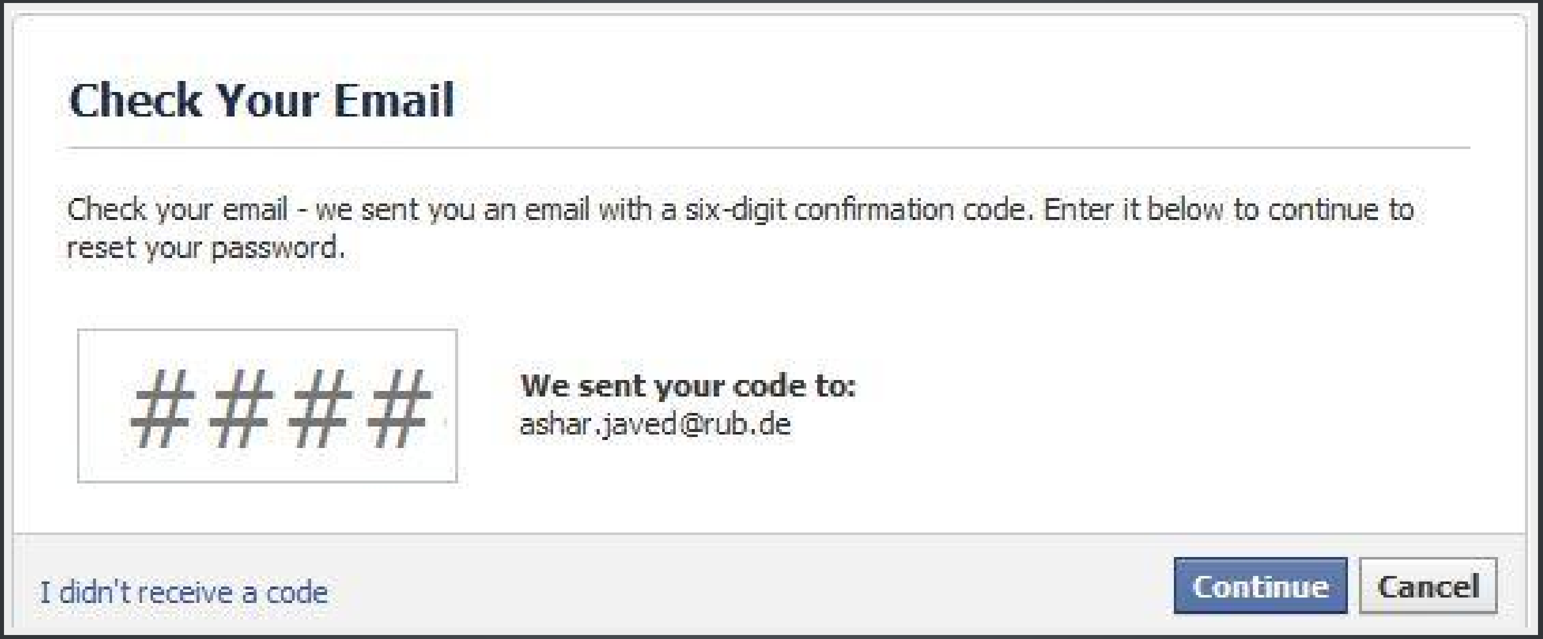
885794

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

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.

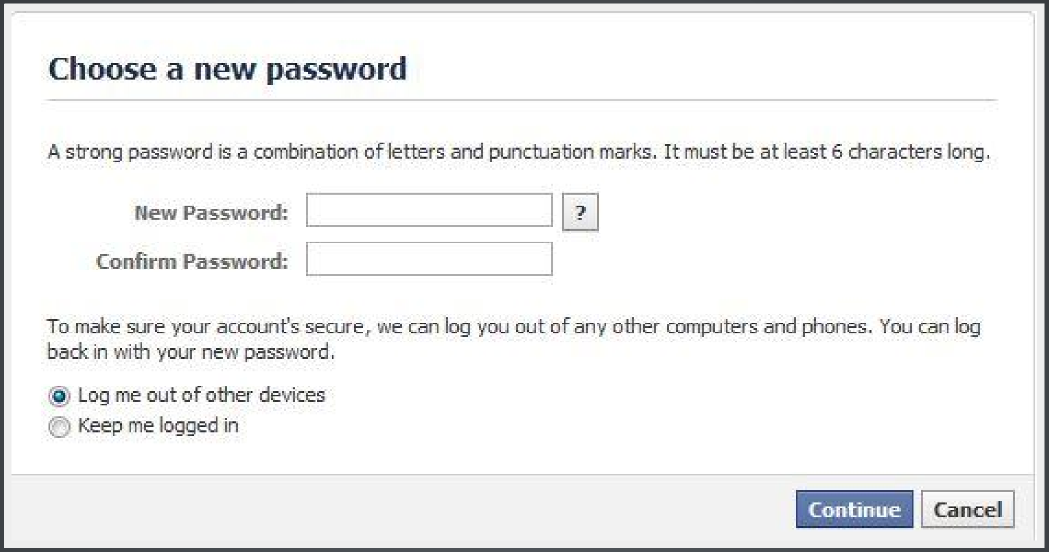
####

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

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

STEP (5)

Set "**New Password**"



Choose a new password

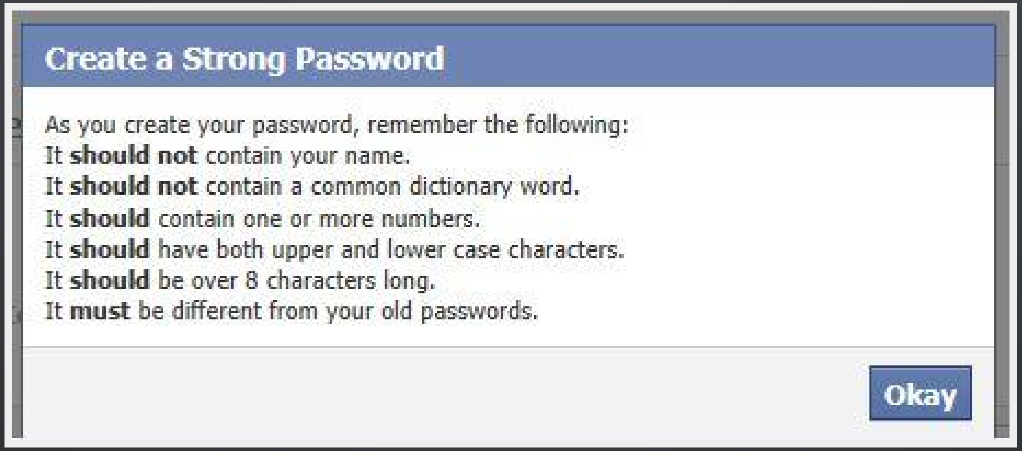
A strong password is a combination of letters and punctuation marks. It must be at least 6 characters long.

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

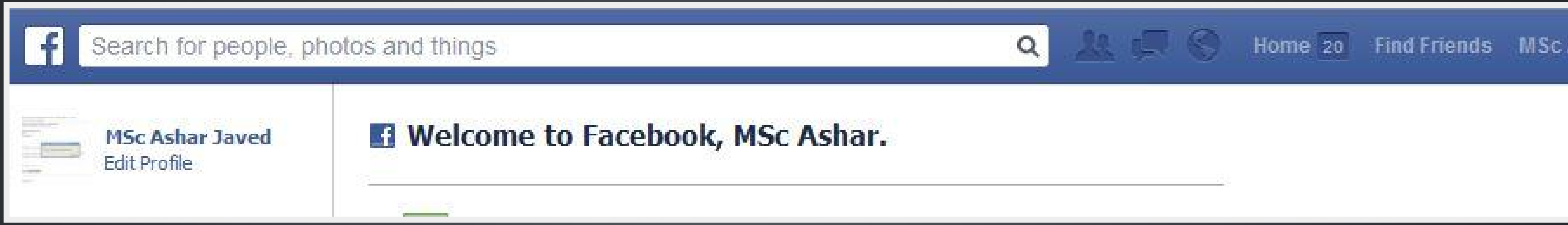


Create a Strong Password

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)

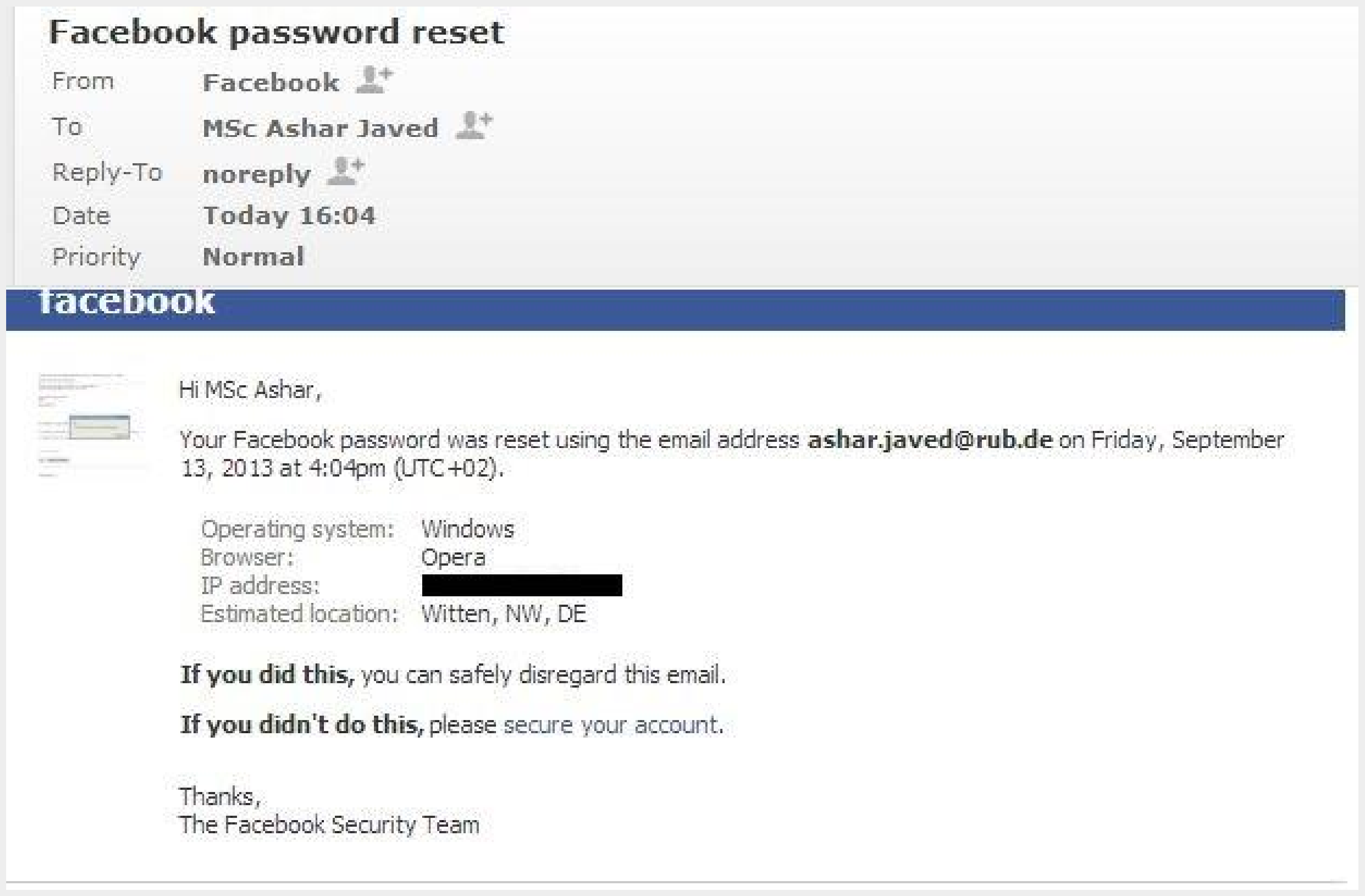
Welcome to Facebook, MSc. Ashar



Search for people, photos and things

Welcome to Facebook, MSc Ashar.

INFORMATIVE EMAIL FROM FACEBOOK



Facebook password reset

From	**Facebook**
To	**MSc Ashar Javed**
Reply-To	**noreply**
Date	**Today 16:04**
Priority	**Normal**

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

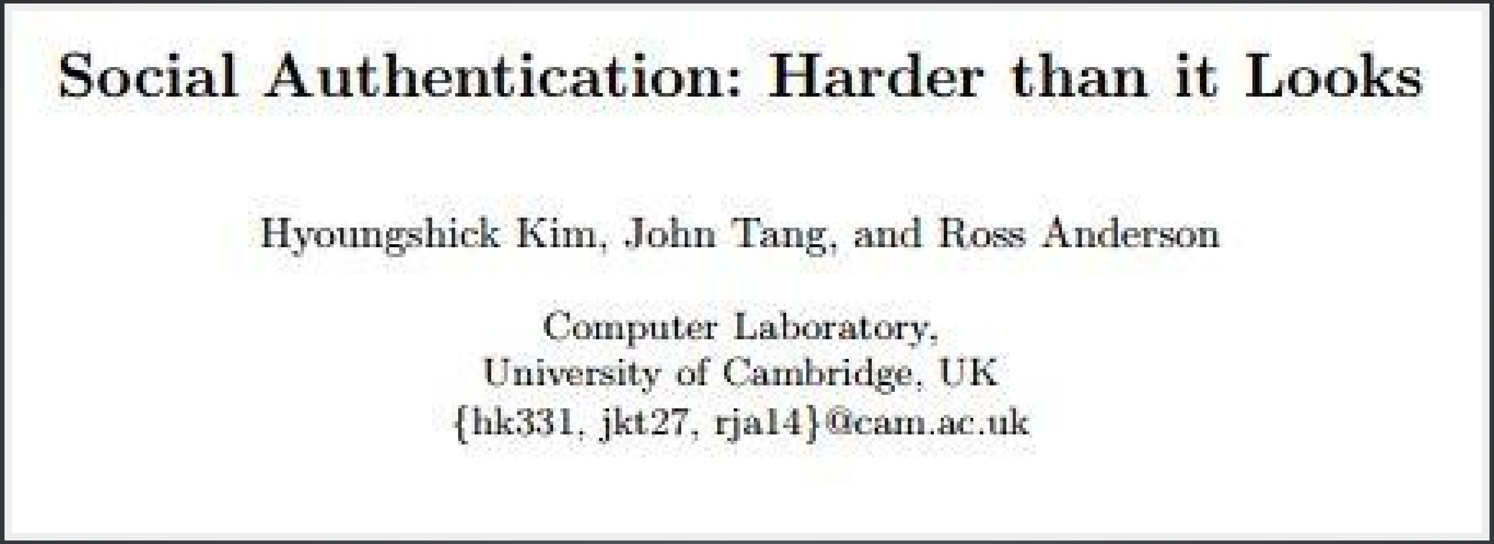
TRUSTED FRIENDS (TF)

"TF IS BASED ON SOCIAL AUTHENTICATION"

&

" Bringing Social to Security " is GOOD

BUT ...



Social Authentication: Harder than it Looks

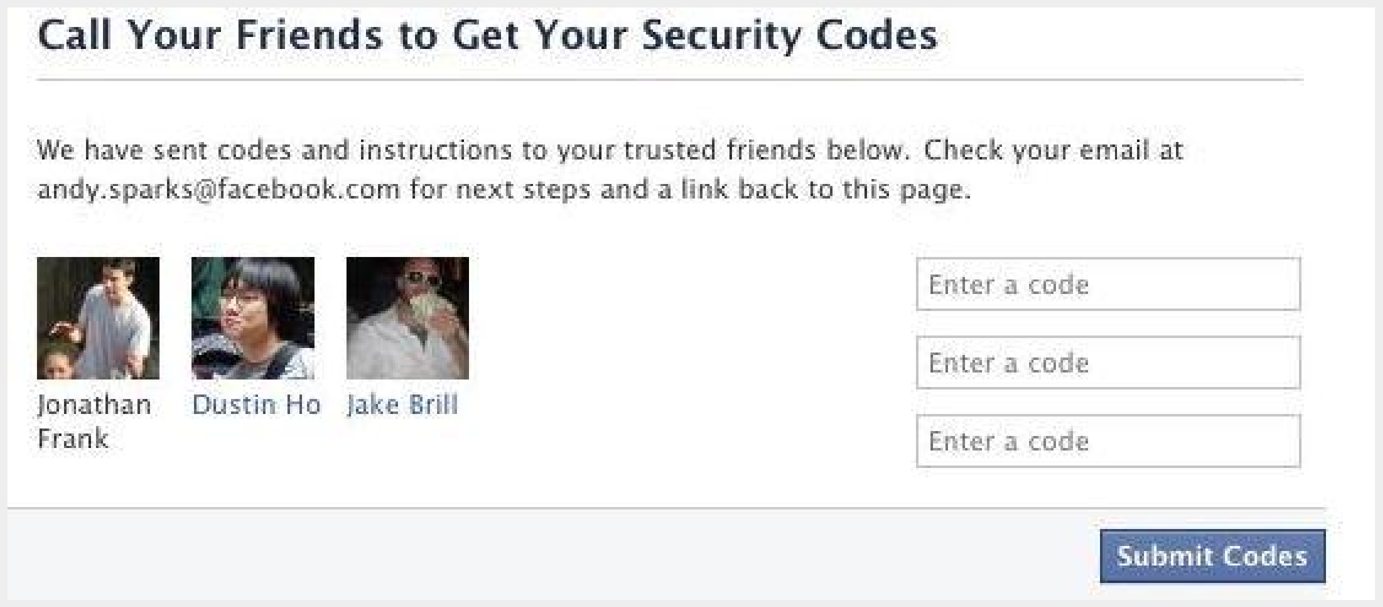
Hyoungshick Kim, John Tang, and Ross Anderson

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 (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.

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"

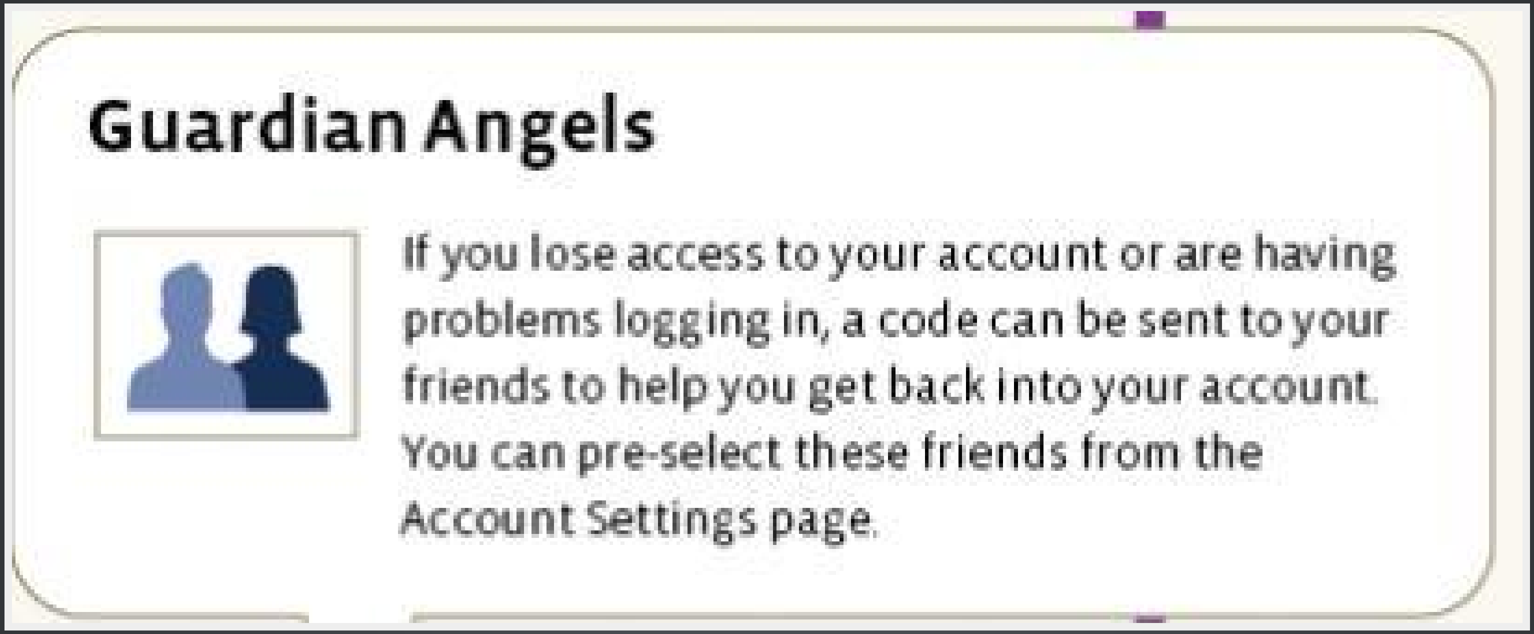
https://www.facebook.com/notes/facebook-security/national-cybersecurity-awareness-month-updates/10150335022240766

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=~ohkT

GUARDIAN ANGELS

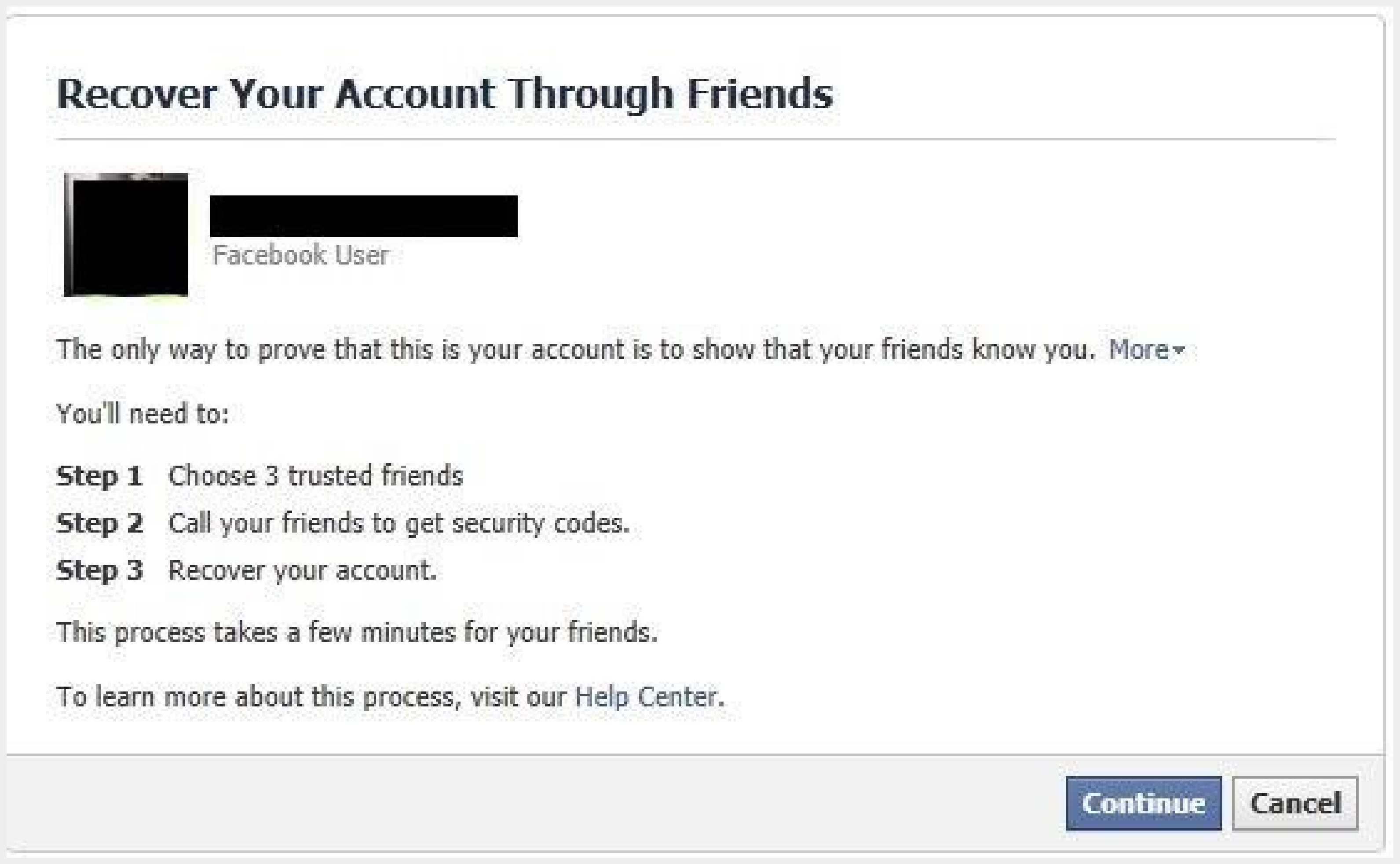


Guardian Angels

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.

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

HOW TRUSTED FRIENDS FEATURE WORKS?



Recover Your Account Through Friends

[redacted]

[redacted]

Facebook User

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

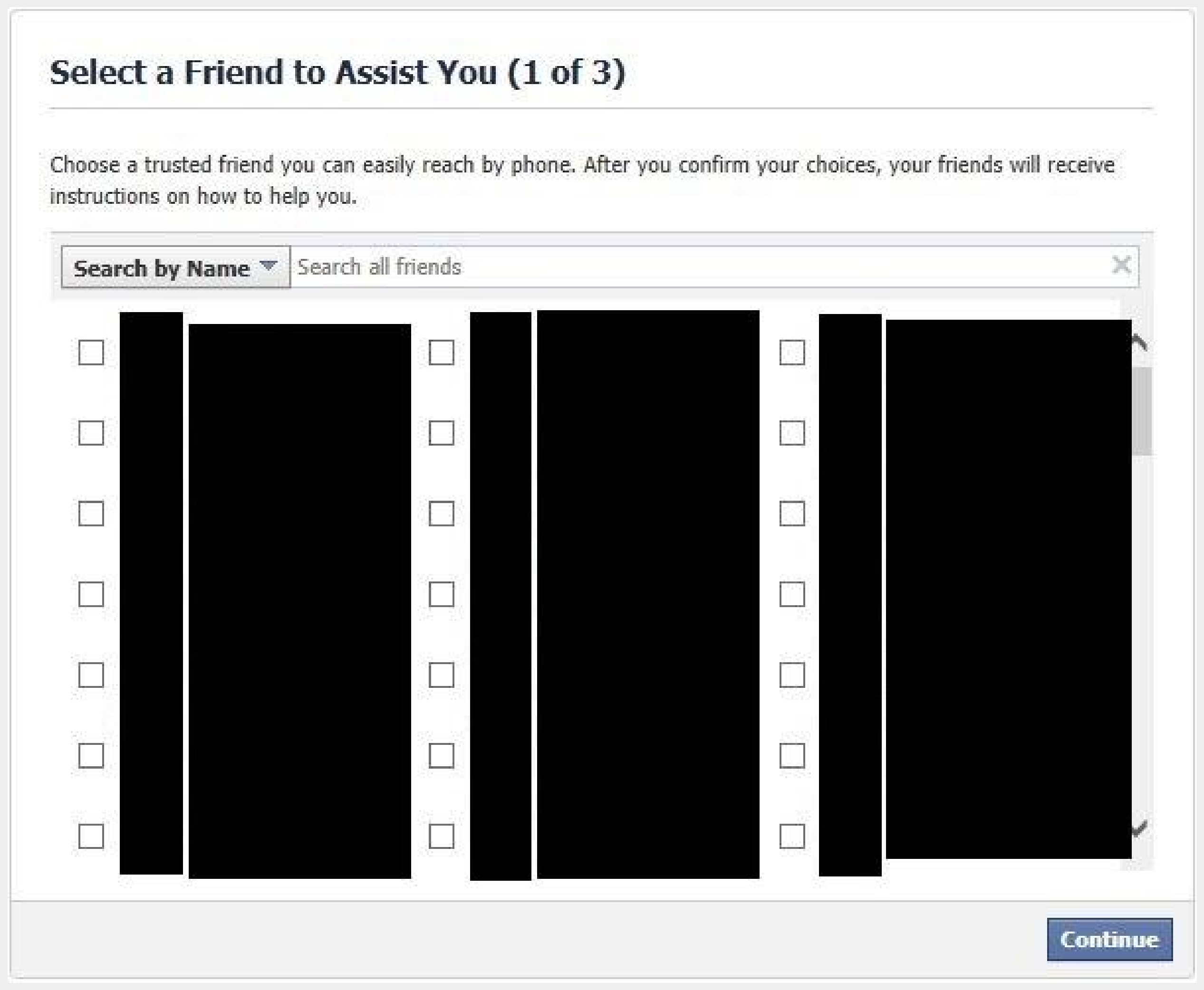
Step 2 Call your friends to get security codes.

Step 3 Recover your account.

This process takes a few minutes for your friends.

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

LIST # 1

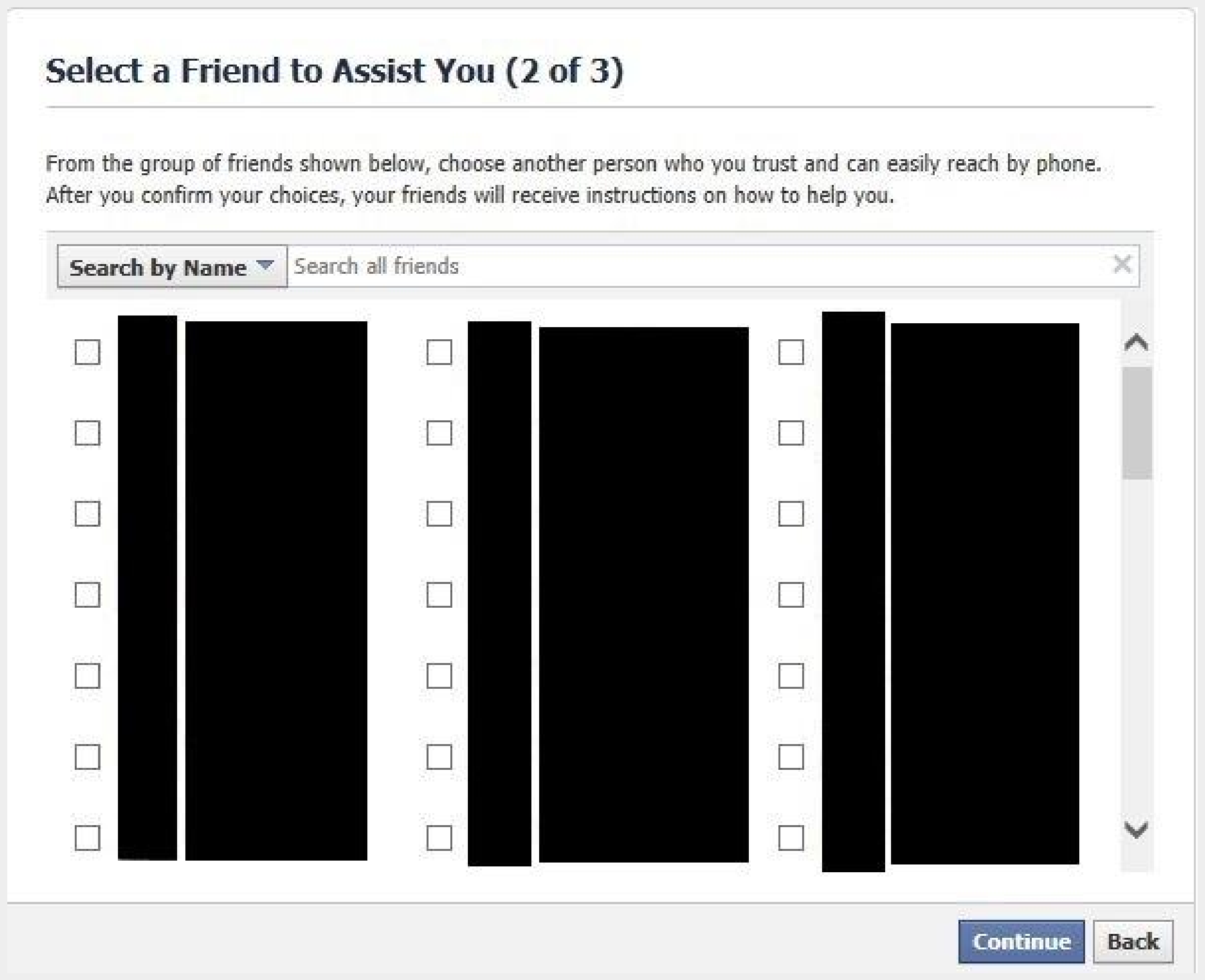


Select a Friend to Assist You (1 of 3)

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.

□ [redacted] [redacted] □ [redacted] [redacted] □ [redacted] [redacted]
□ □ □
□ □ □
□ □ □
□ □ □
□ □ □
□ □ □

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.

□
□
□
□
□
□
□

[redacted] [redacted]

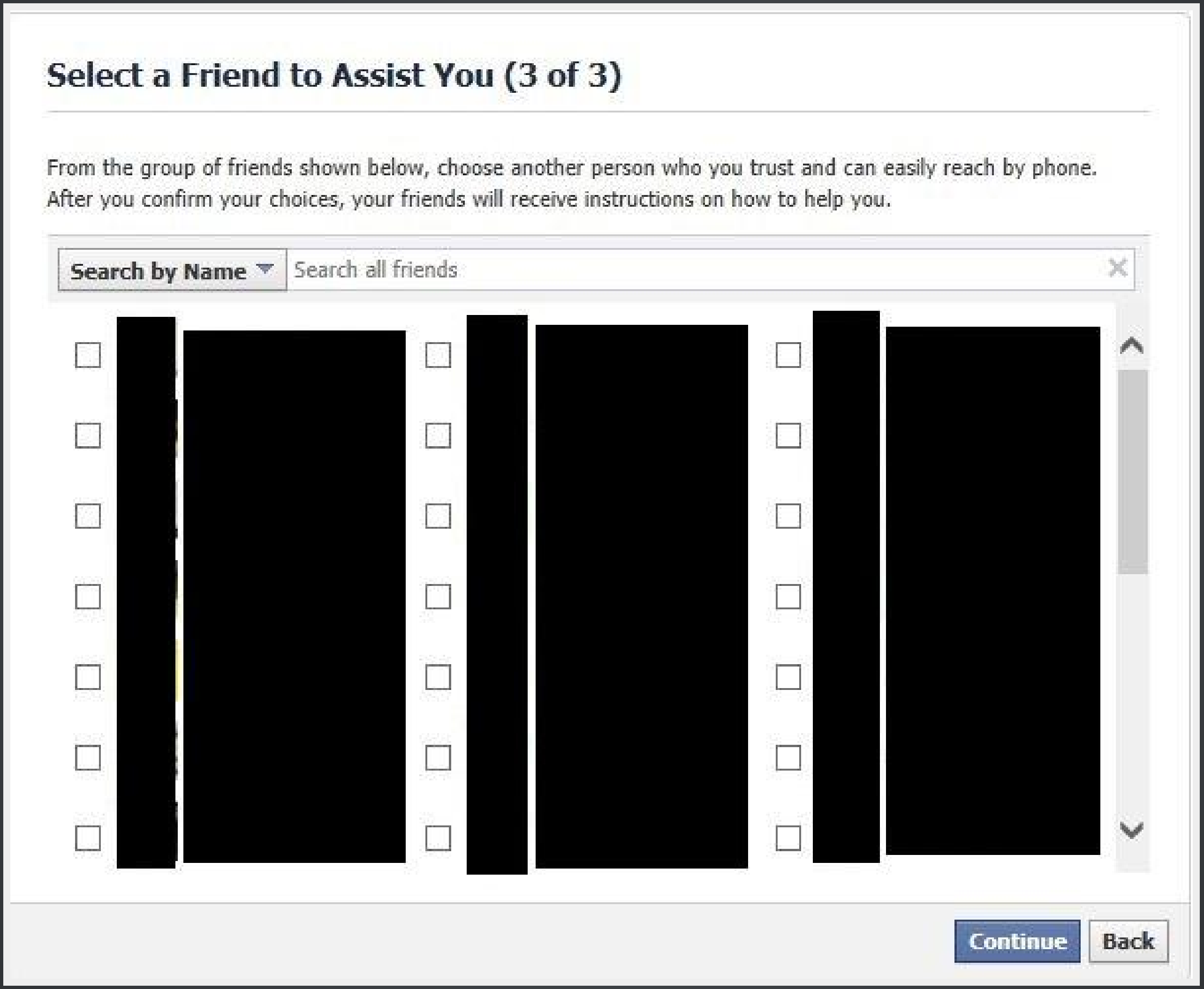
□
□
□
□
□
□
□

[redacted] [redacted]

□
□
□
□
□
□
□

[redacted] [redacted]

LIST # 3

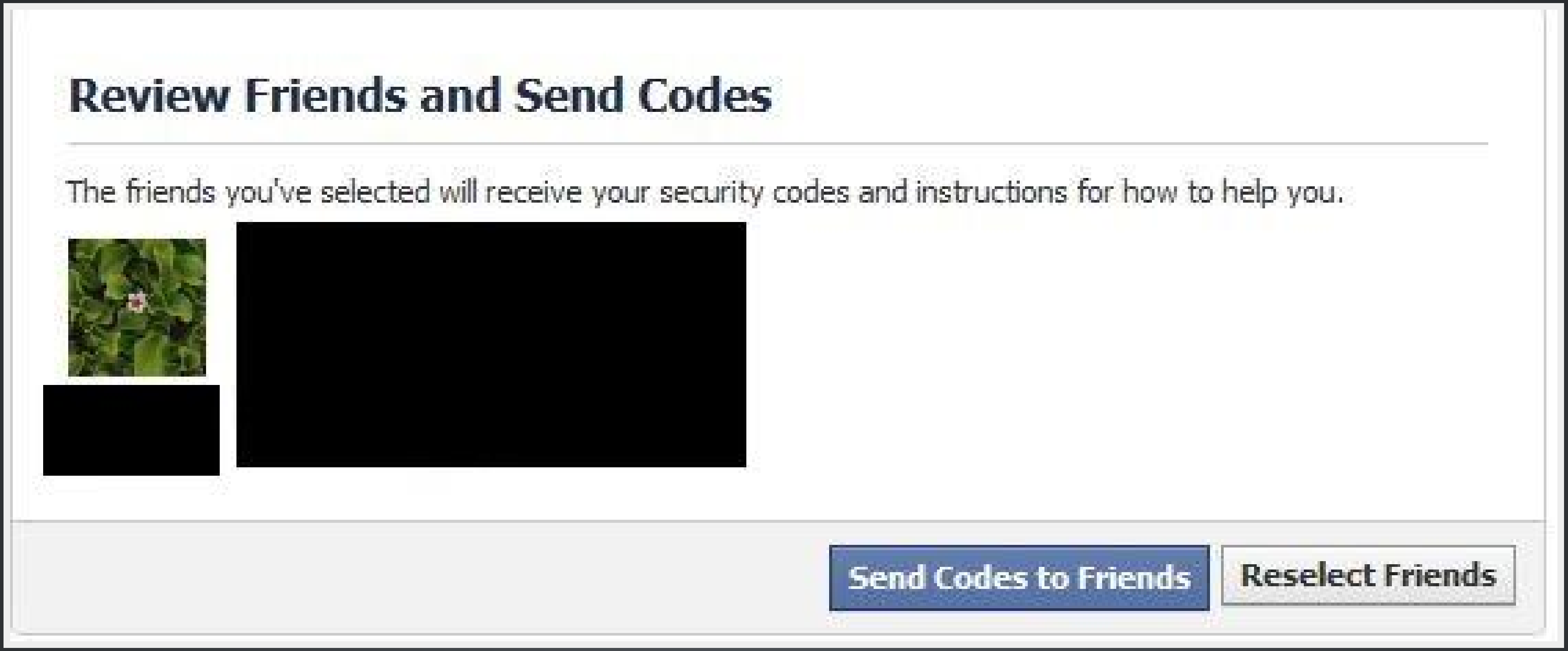


Select a Friend to Assist You (3 of 3)

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.

□ [redacted] [redacted]	□ [redacted] [redacted]	□ [redacted] [redacted]
□	□	□
□	□	□
□	□	□
□	□	□
□	□	□
□	□	□

REVIEW FRIENDS



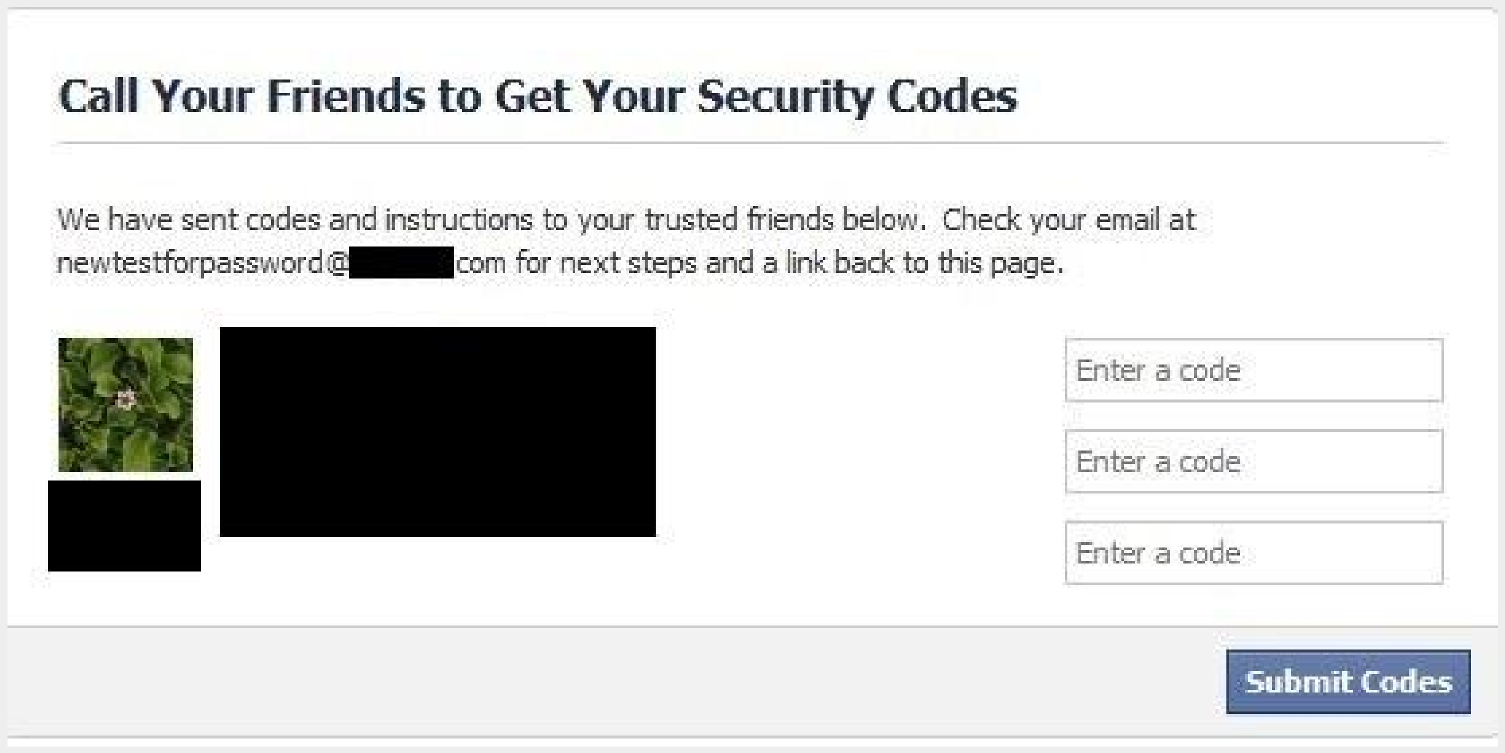
Review Friends and Send Codes

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

[redacted]

[redacted]

ENTER CODES & GAIN ACCESS TO YOUR ACCOUNT



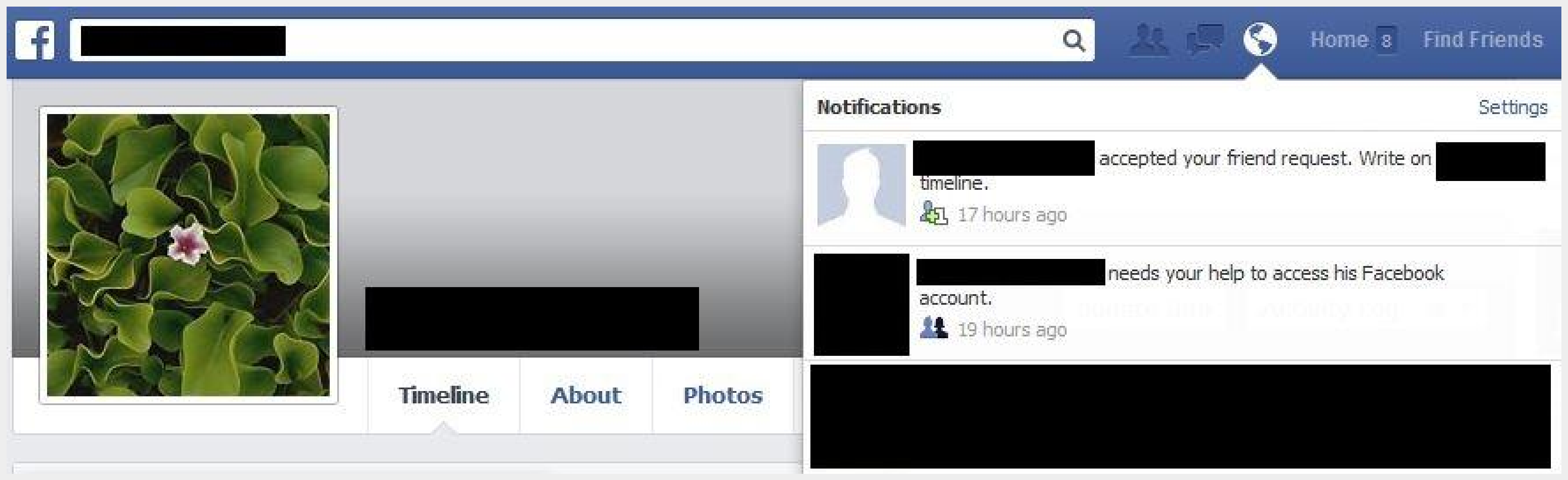
Call Your Friends to Get Your Security Codes

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.

[redacted]

[redacted]

SCREEN-SHOT OF FAKE PROFILE



Notifications

Settings

[redacted] accepted your friend request. Write on [redacted] timeline.

17 hours ago

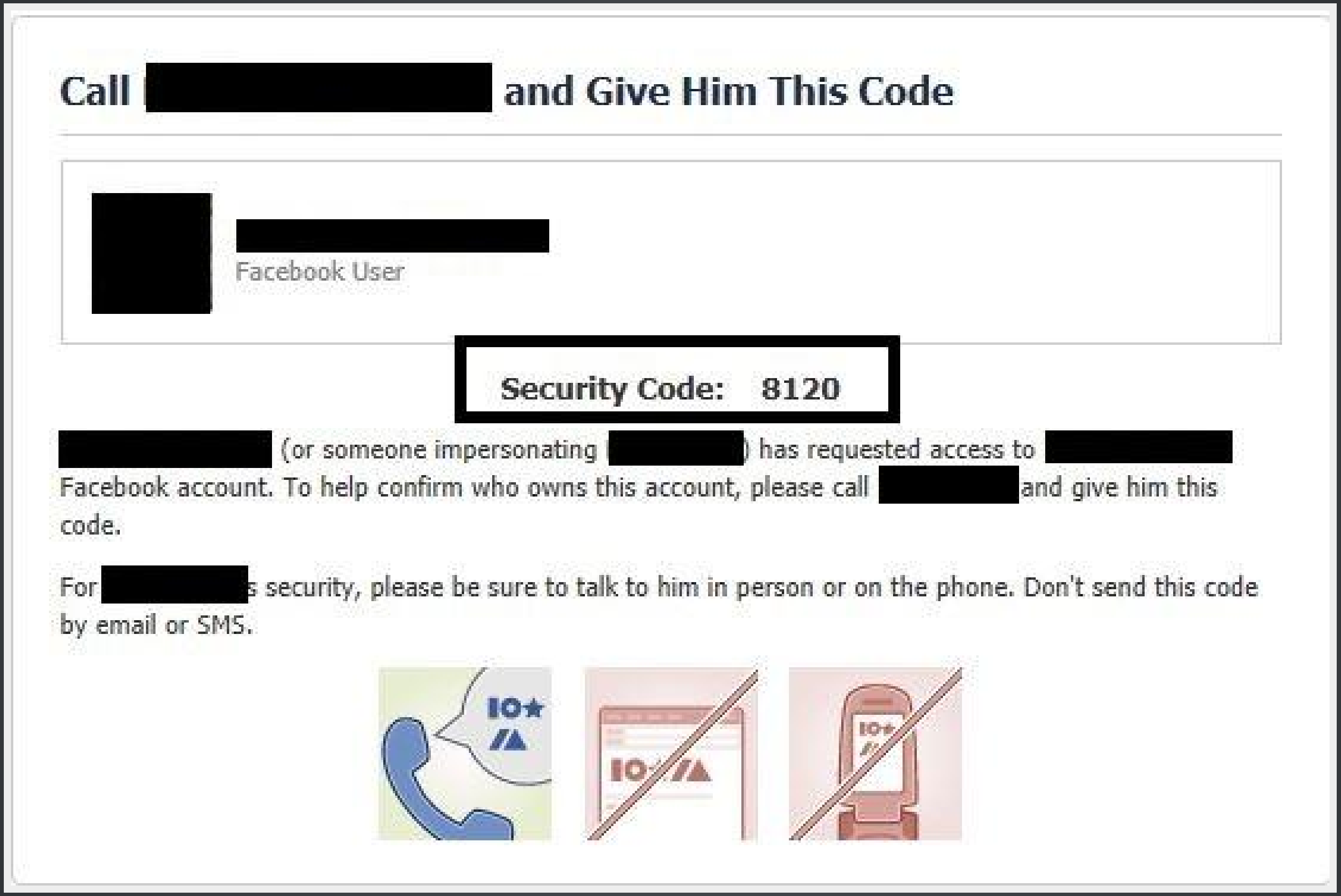
[redacted]

[redacted] needs your help to access his Facebook account.

19 hours ago

[redacted]

4 DIGIT CODE



Call [redacted] and Give Him This Code

[redacted]

[redacted]

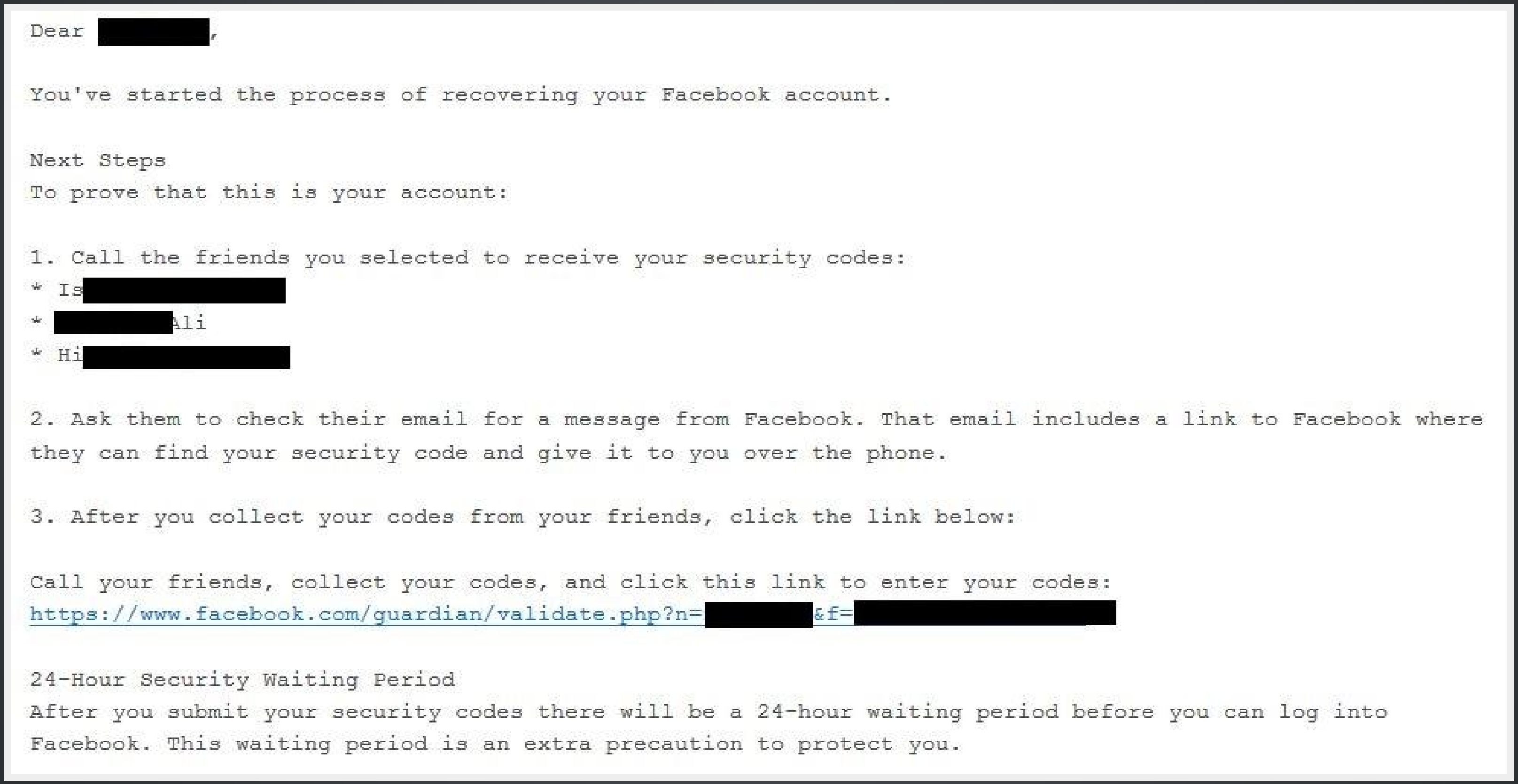
Facebook User

Security Code: 8120

[redacted] (or someone impersonating [redacted]) has requested access to [redacted] 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.

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:

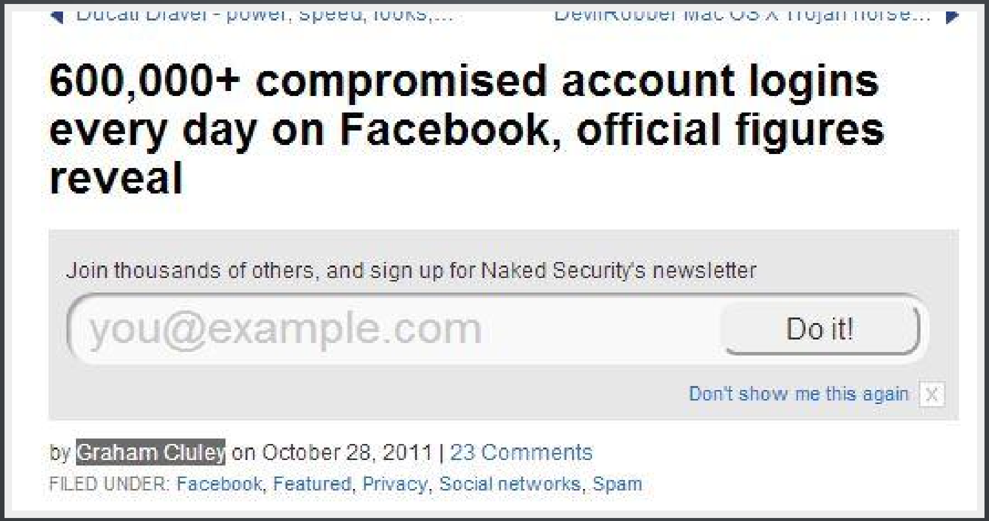
Call your friends, collect your codes, and click this link to enter your codes:
https://www.facebook.com/guardian/validate.php?n=[redacted]&f=[redacted]

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



◀ Ducati Diavel - power, speed, looks,... DevilRobber Mac OS X Trojan horse... ▶

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

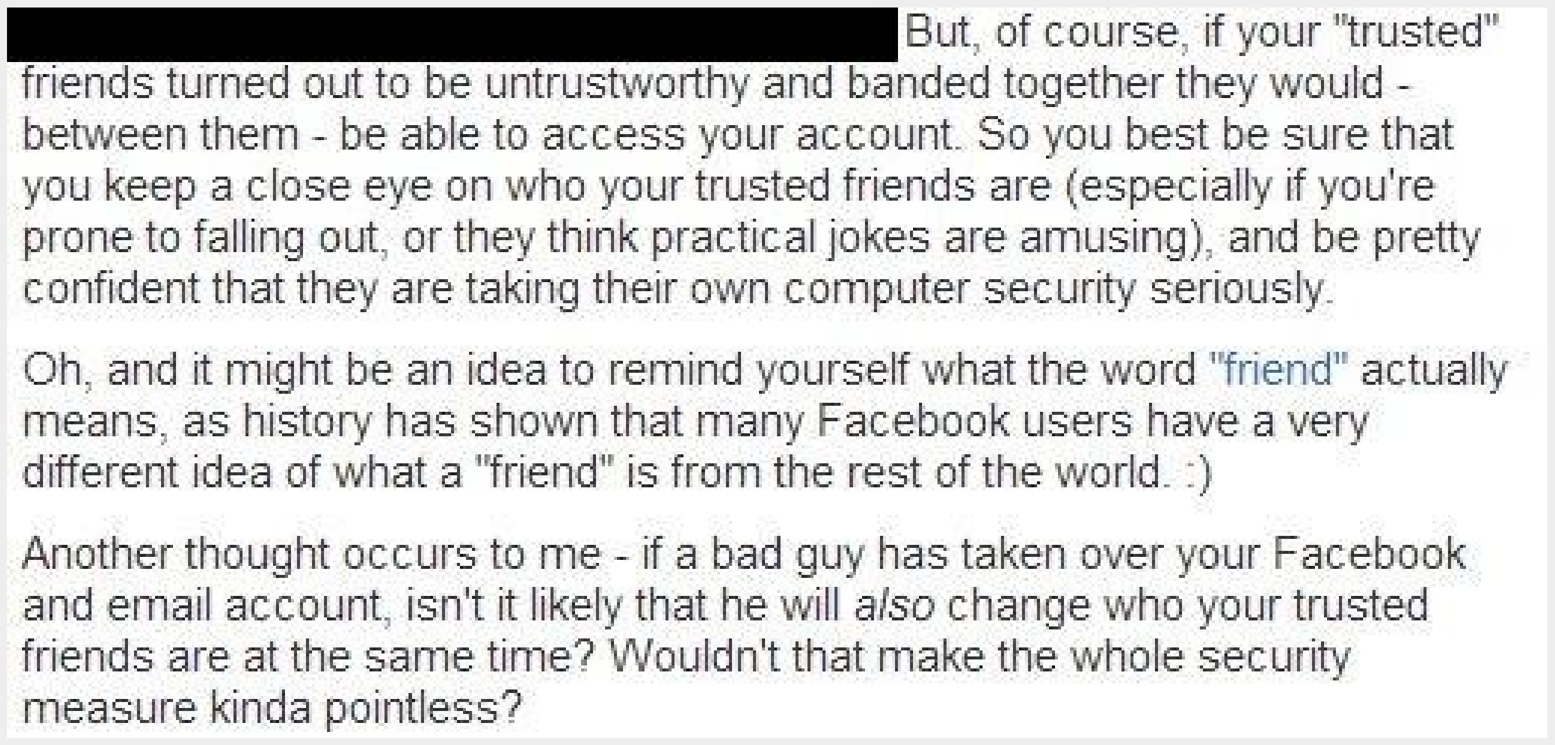
Join thousands of others, and sign up for Naked Security's newsletter

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



[redacted] 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. :)

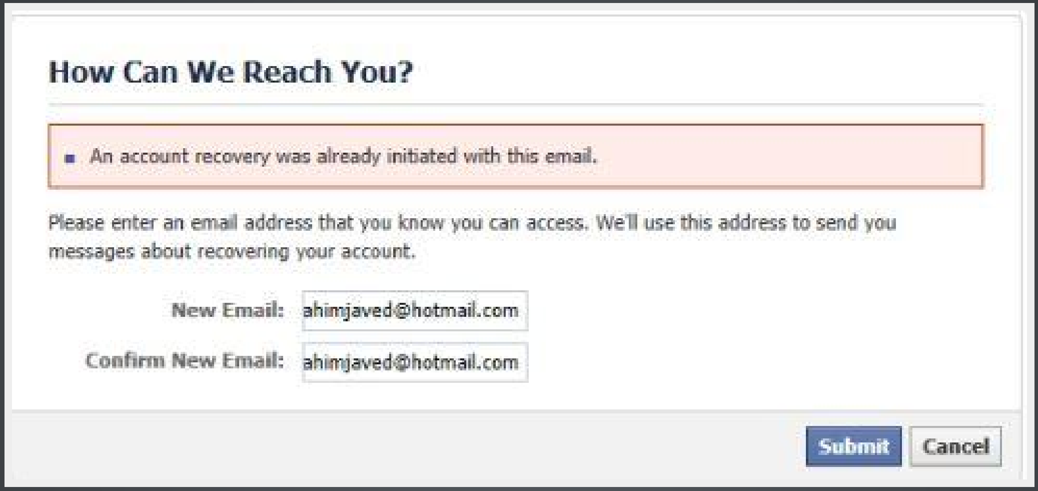
Another thought occurs to me - if a bad guy has taken over your Facebook and email account, isn't it likely that he will *also* change who your trusted friends are at the same time? Wouldn't that make the whole security measure kinda pointless?

QUESTION YOU MIGHT THINKING ...

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

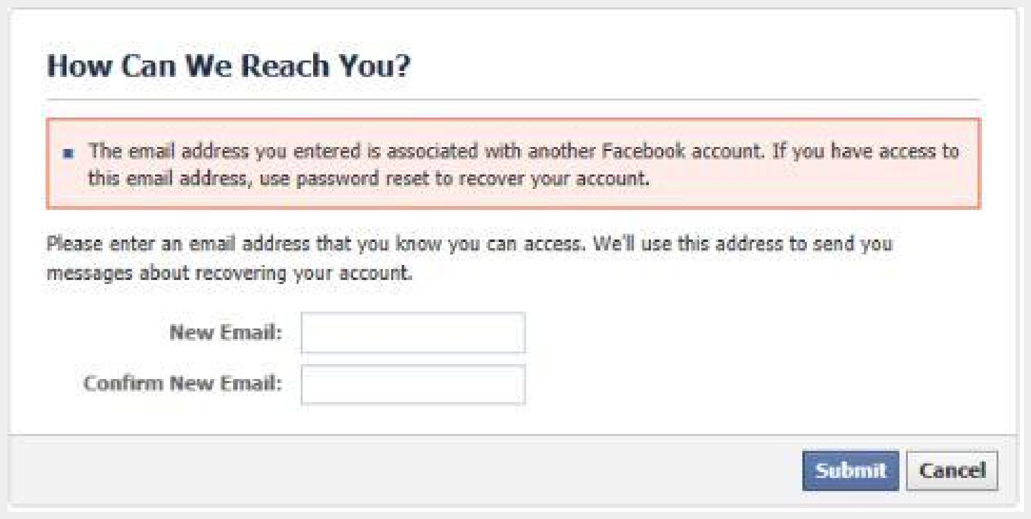


How Can We Reach You?

- 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:	ahimjaved@hotmail.com
Confirm New Email:	ahimjaved@hotmail.com



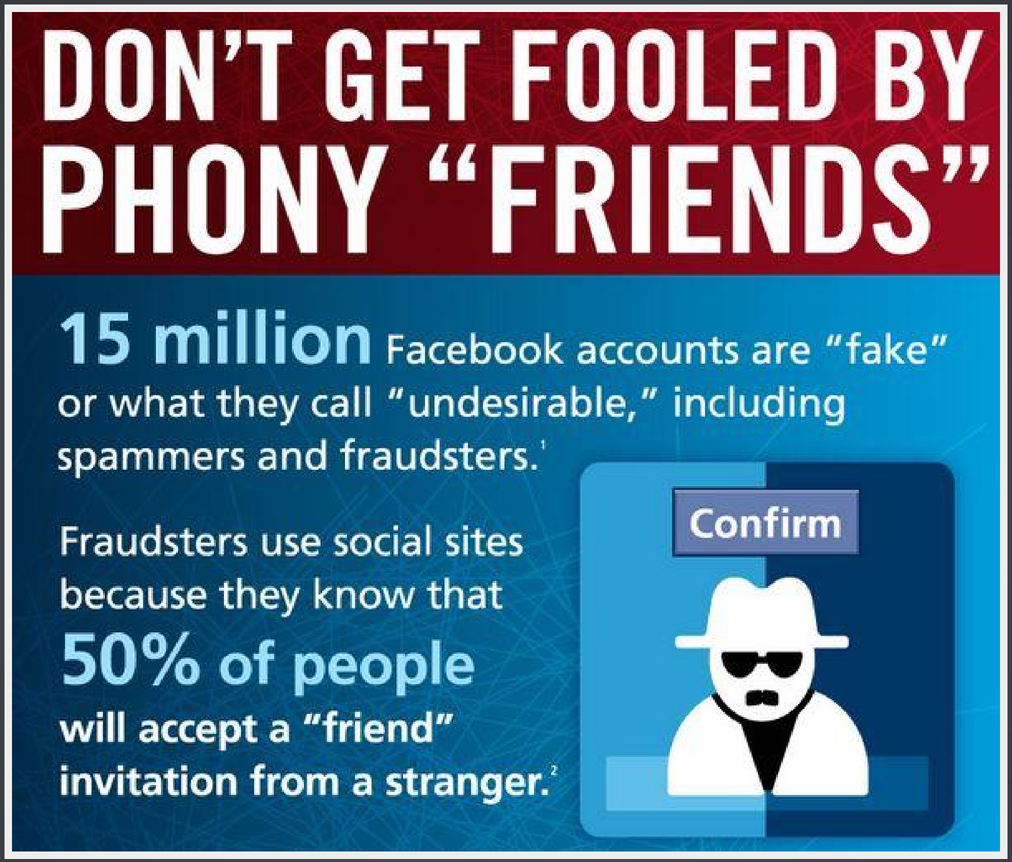
How Can We Reach You?

- 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:	

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

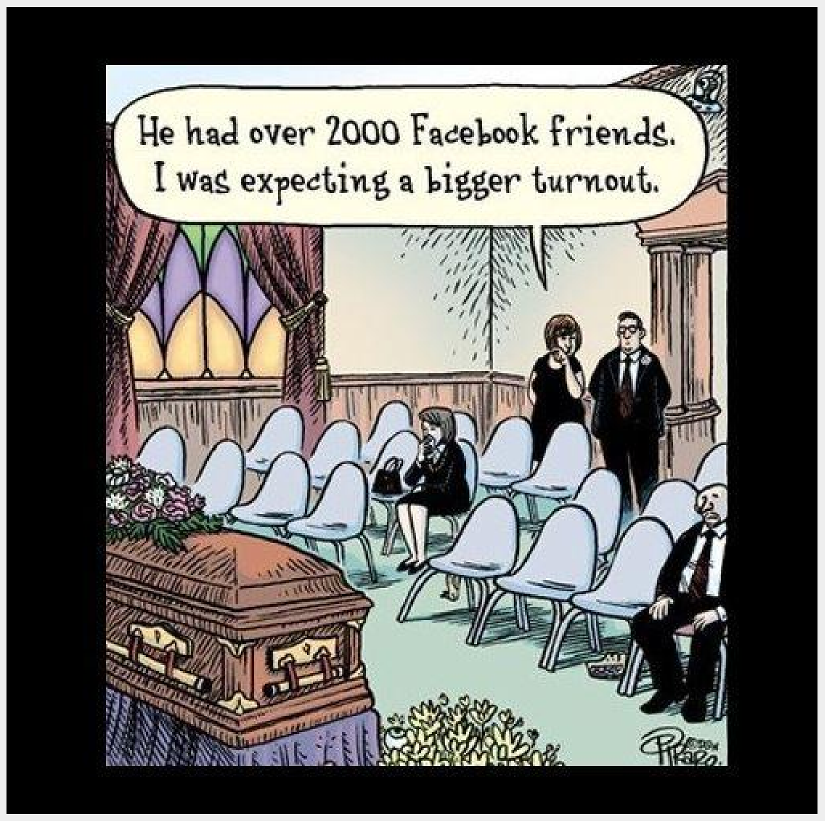
DATA SCIENCE OF THE FACEBOOK WORLD

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


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

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)

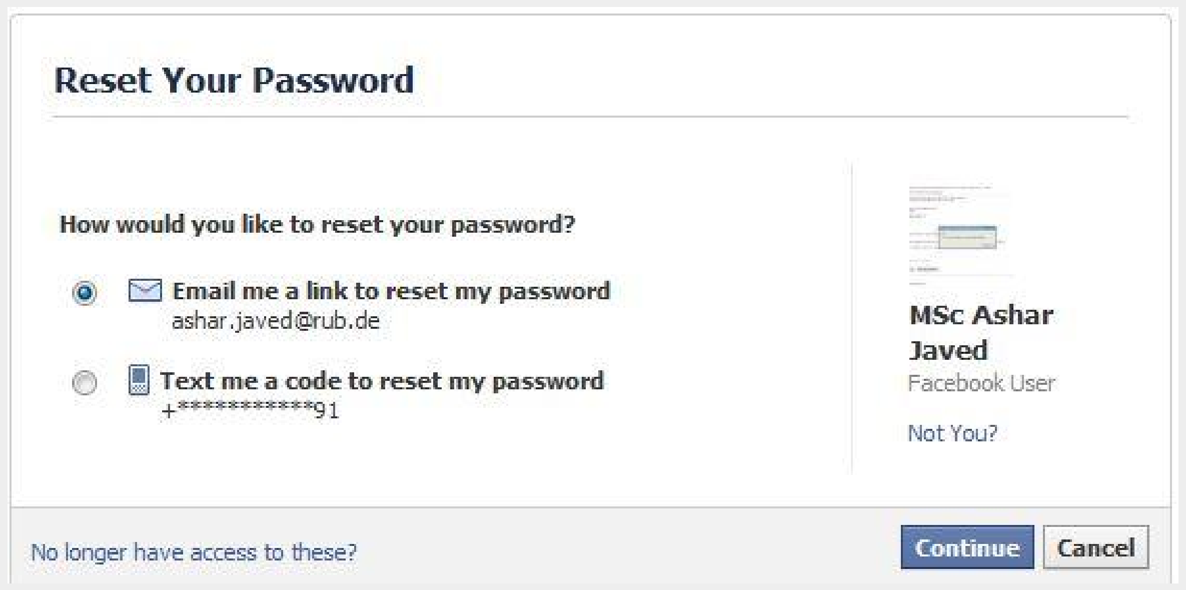
In order to start **TFA**, we need victim's Facebook username and FYI, it is **PUBLIC INFORMATION** & part of Facebook URL.

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.,



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
+************91

MSc Ashar Javed
Facebook User

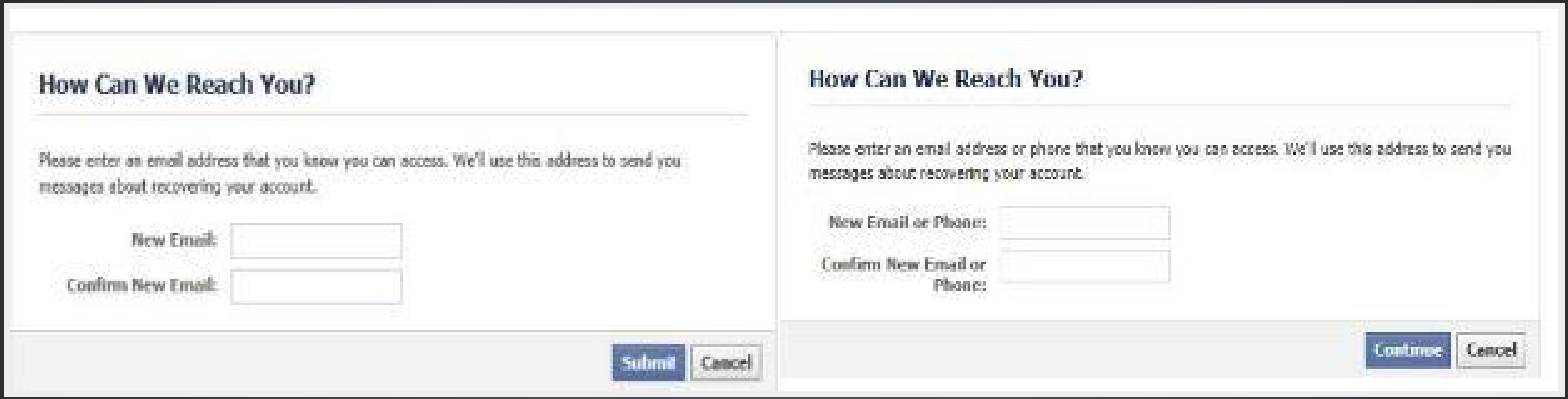
Not You?

No longer have access to these?

"No longer have access to these?"

NO LONGER HAVE ACCESS TO THESE?

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



How Can We Reach You?

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:

How Can We Reach You?

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

New Email or Phone:

Confirm New Email or Phone:

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...

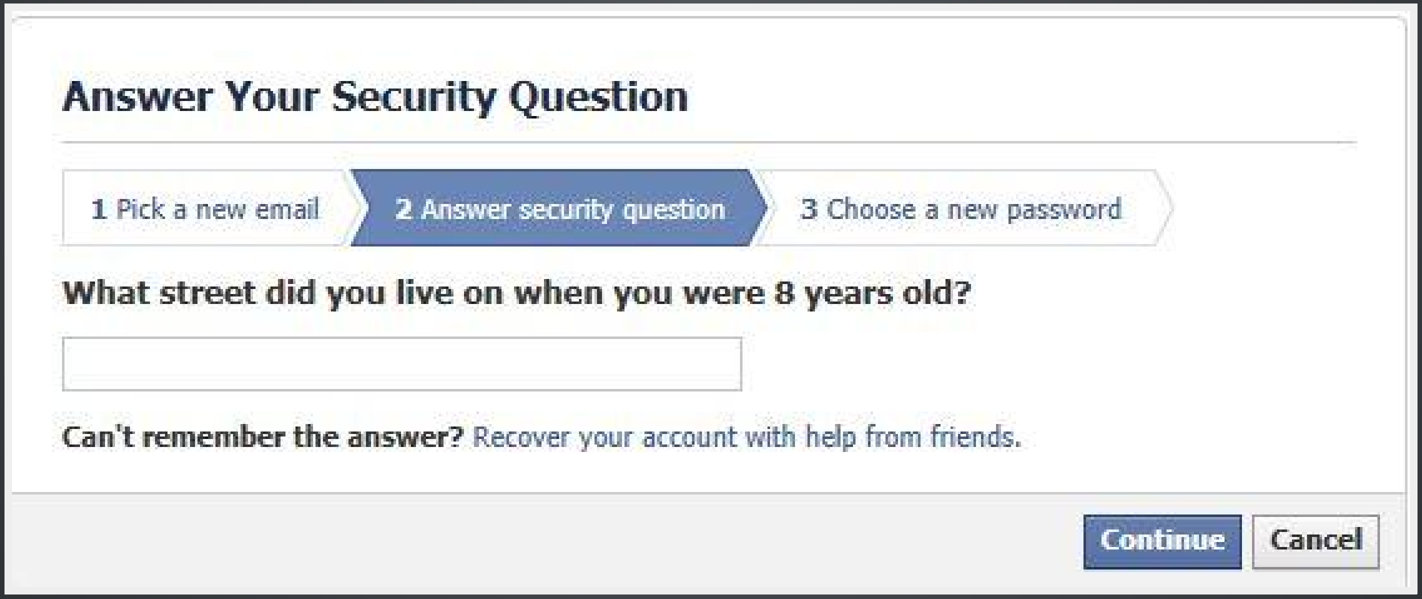
How can Facebook bind this **new email address** or phone number to the legitimate user's address or phone?

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

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

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

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.,

1. **Answer Security Question**
2. **Choose Three Friends of Attacker's Choice**

TFA’S VARIATIONS/FORMS

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

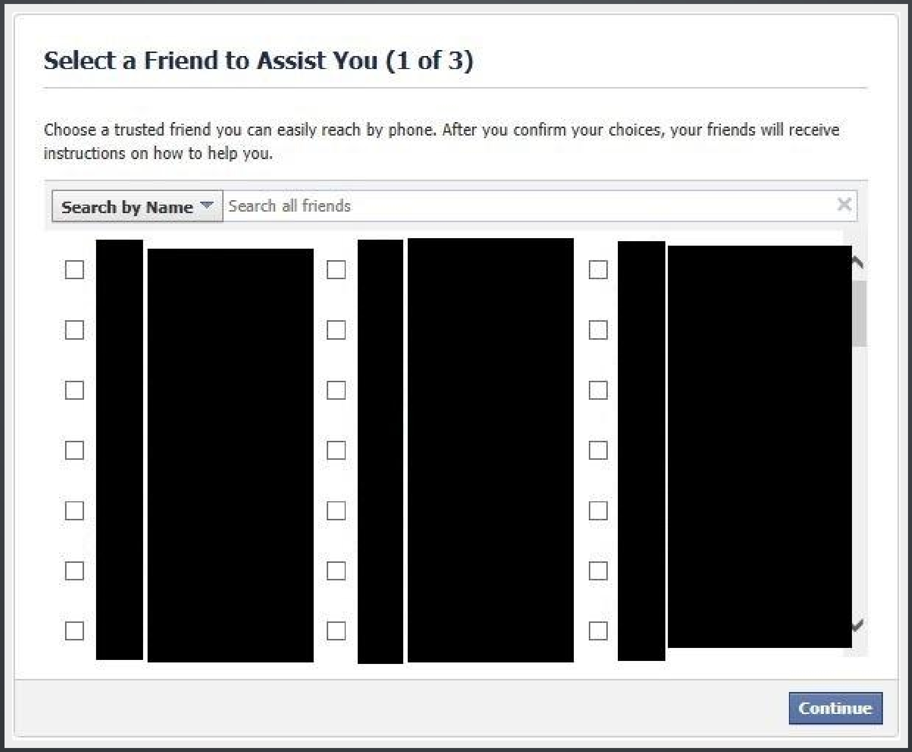
ATTACKER'S CHOICES

- 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.



Select a Friend to Assist You (1 of 3)

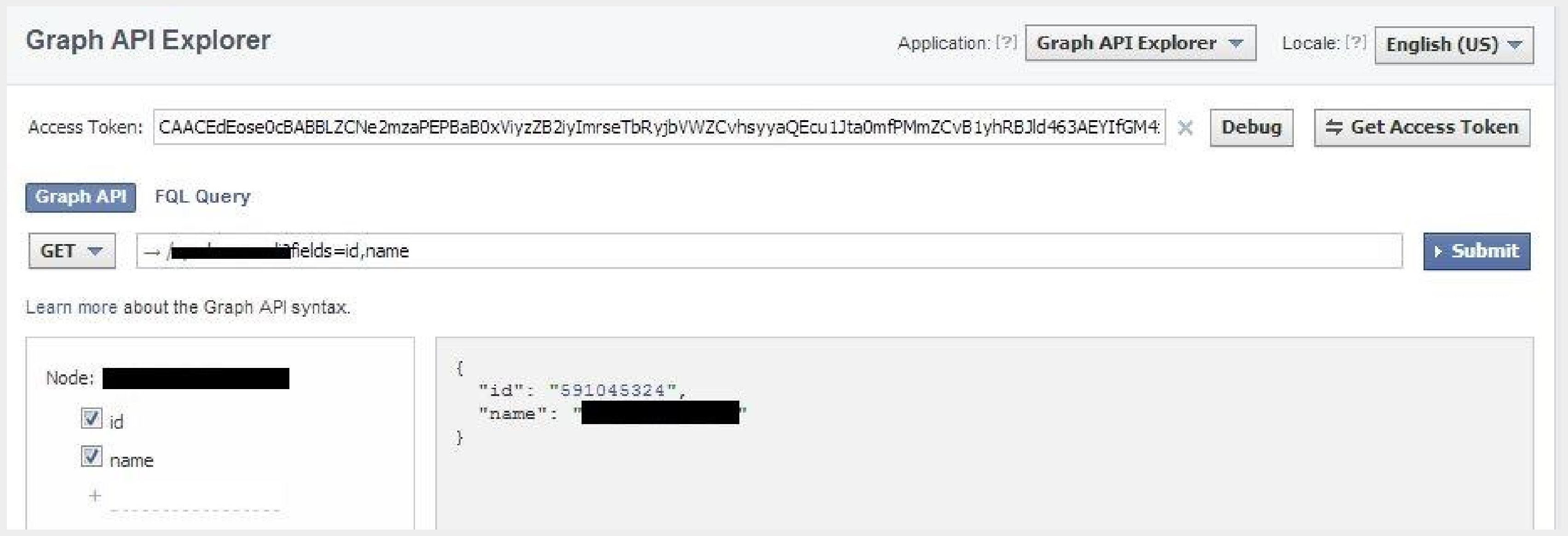
Choose a trusted friend you can easily reach by phone. After you confirm your choices, your friends will receive instructions on how to help you.

□ [redacted] [redacted] □ [redacted] [redacted] □ [redacted] [redacted]
□ □ □
□ □ □
□ □ □
□ □ □
□ □ □
□ □ □

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



Access Token: CAACEdEose0cBABBLZCNe2mzaPEPBaB0xViyzZB2iyImrseTbRyjbVWZCvhsyyaQEcu1Jta0mfPMmZCvB1yhRBJld463AEYIfGM4:

GET → /[redacted]?fields=id,name

Node: [redacted]

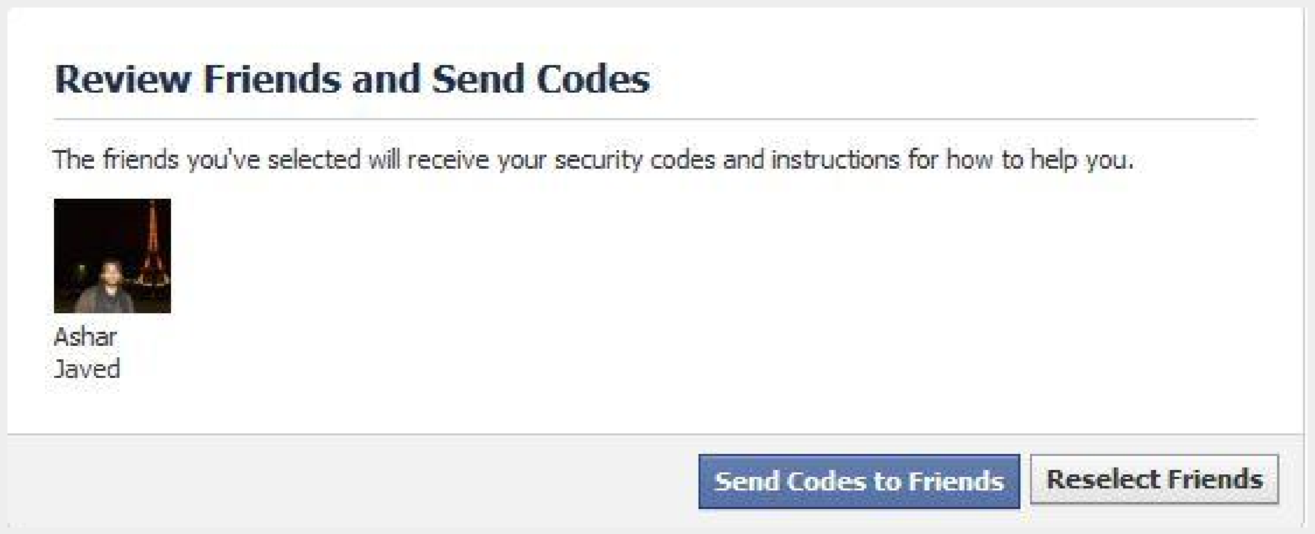
☑ id

☑ name

```
{
  "id": "591045324",
  "name": "[redacted]"
}
```

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

EVIL IDEA



Review Friends and Send Codes

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

Ashar
Javed

URL looks like:

https://www.facebook.com/guardian/confirm.php?

guardians[0]=511543064&guardians[1]=511543064&guardians[2]=511543064

&**cuid**=AYhhCnxPb9g8xVAUGmuPh4e33s2NcCRj8Qng7wKGN7fxe9hXTQtVUKr0Rm-

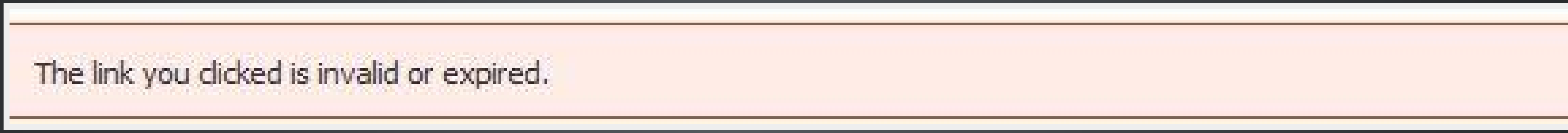
0LBeTOCX_Es83lN0_BGe8Yi2GG7iGRbZwIL5rNXktD1mSsnW-

ZFD2fZB1Z7lLuyYdQ4GWPbf9bzhik9zXBpNeOsvUv-

MpzCcAQT2jxLtEa25YGlg_qg&**cp**=testpurposexss@gmail.com

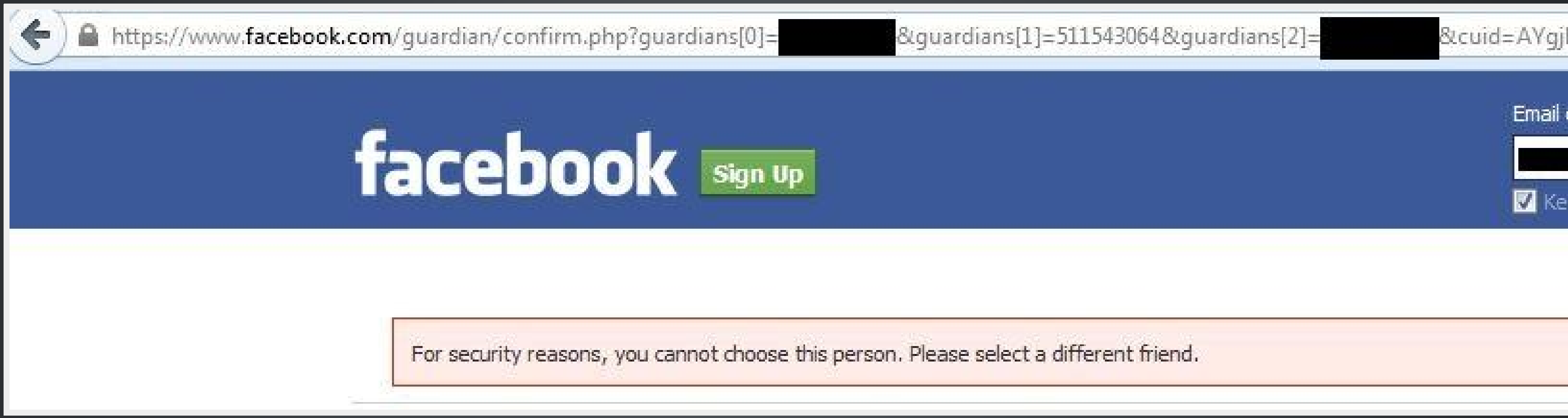
EVIL IDEA DOESN'T WORK

Facebook correctly says:



The link you clicked is invalid or expired.

INTERESTING MESSAGE FROM FACEBOOK



https://www.facebook.com/guardian/confirm.php?guardians[0]=[redacted]&guardians[1]=511543064&guardians[2]=[redacted]&cuid=AYgj

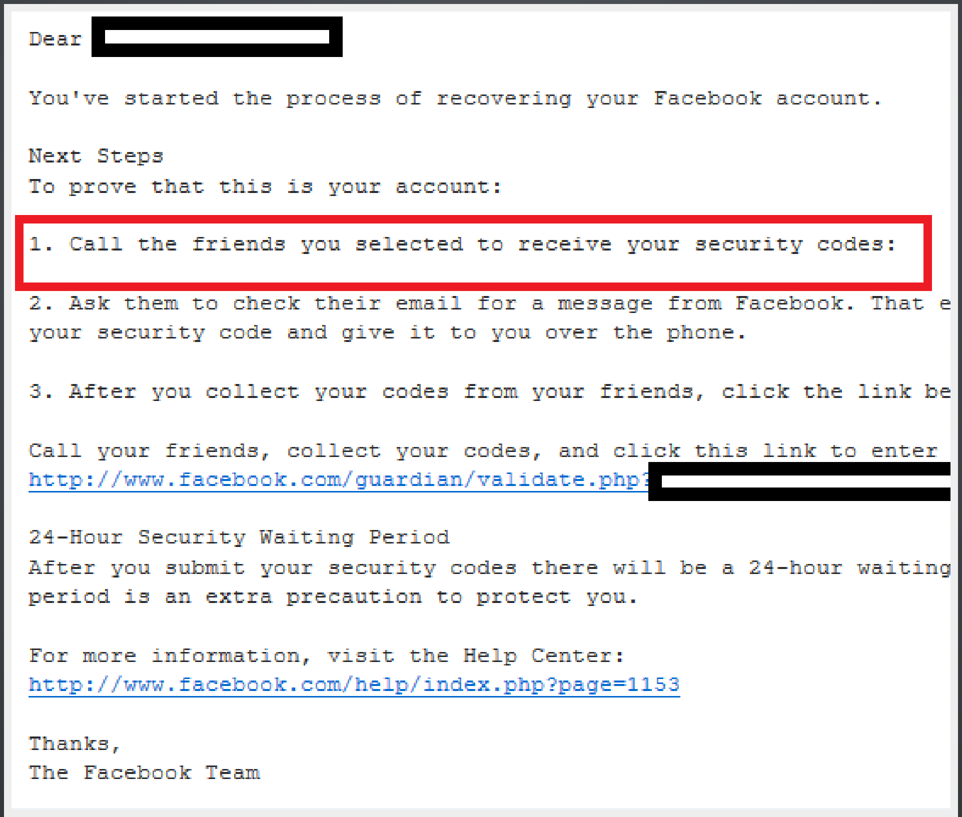
[redacted]

For security reasons, you cannot choose this person. Please select a different friend.

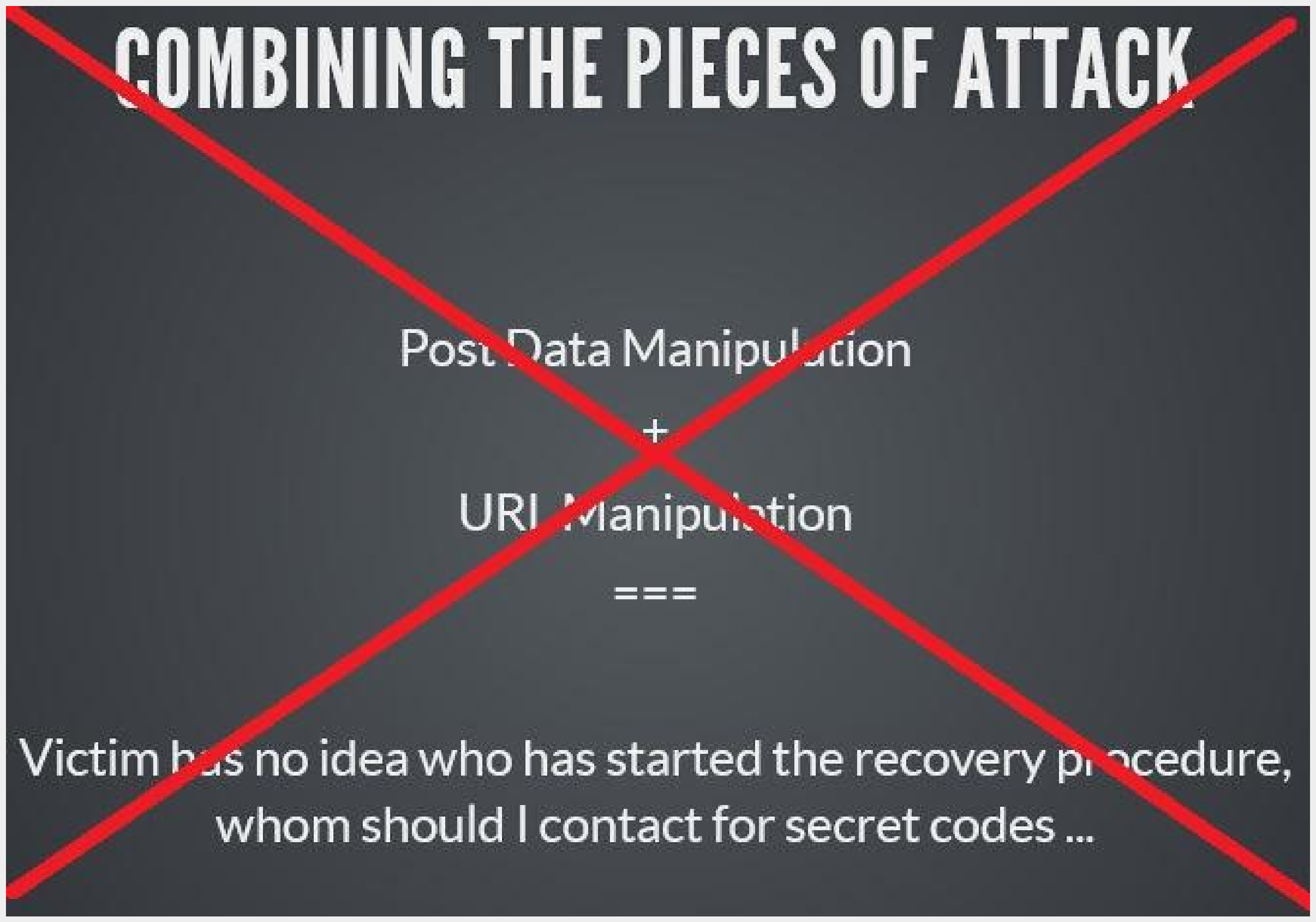
WHAT DOES IT MEAN?

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
```



COMBINING THE PIECES OF ATTACK

Post Data Manipulation

+

URL Manipulation

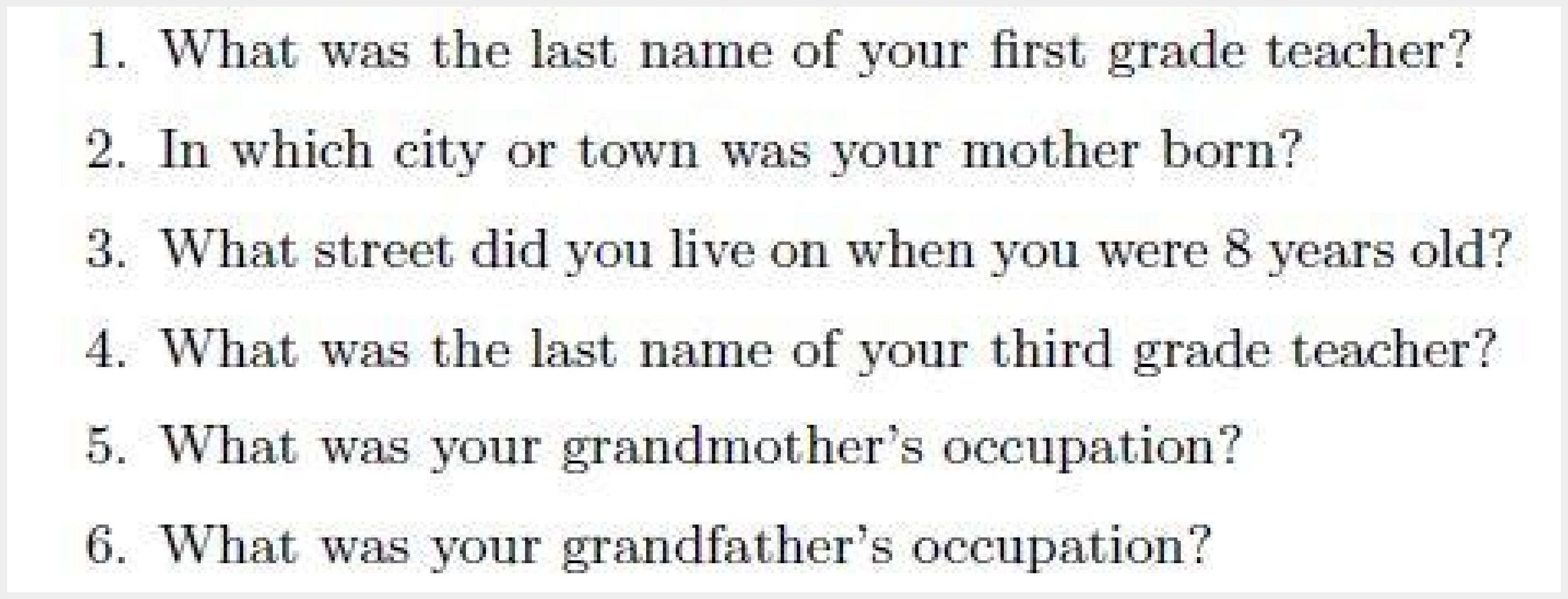
===

Victim has no idea who has started the recovery procedure, whom should I contact for secret codes ...

CHAIN TRUSTED FRIENDS ATTACK (CTFA)

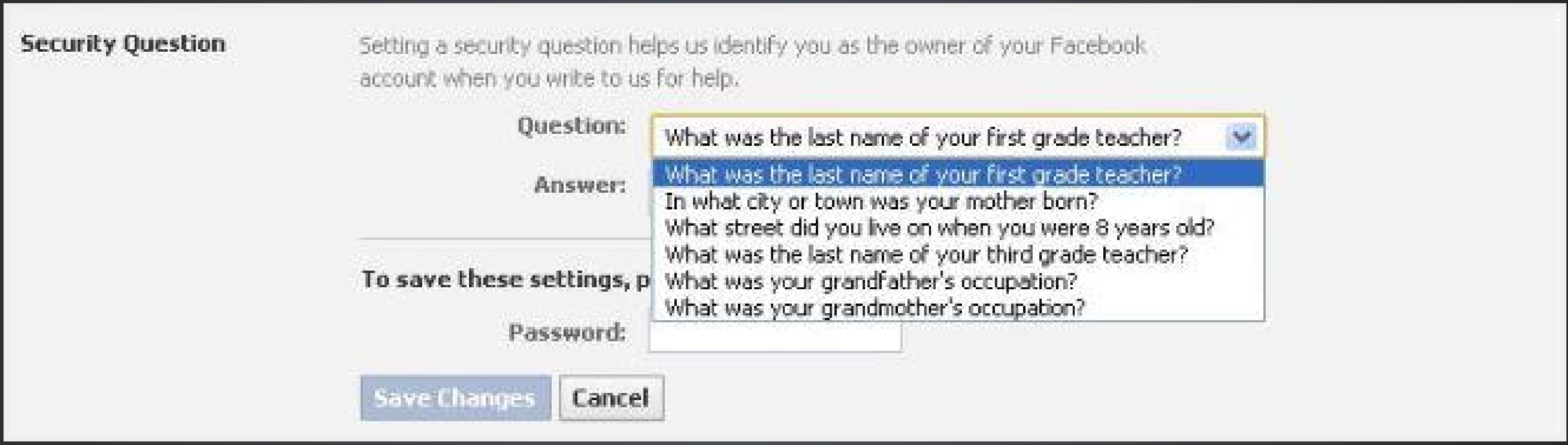
In CTFA, attacker can make a chain of compromised accounts and with the help of chain he may compromised account(s) that are even not in his friends list.

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!



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: What was the last name of your first grade teacher?

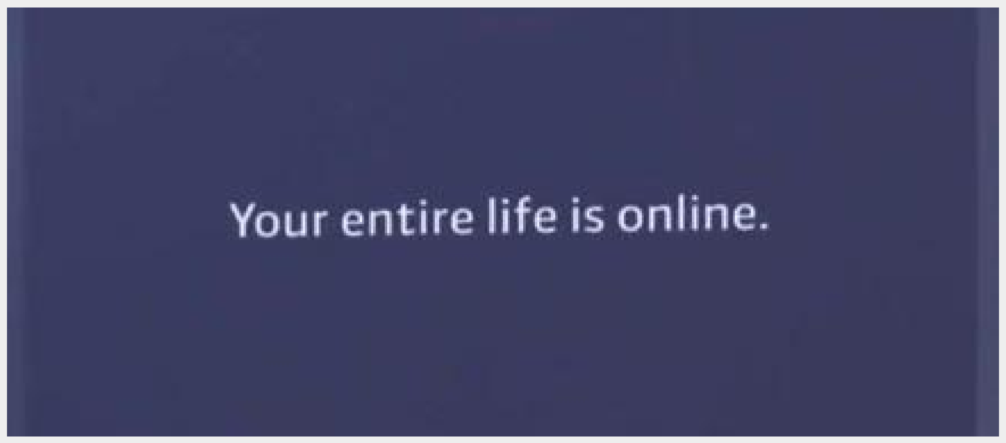
- What was the last name of your first grade teacher?
- In what city or town was your mother born?
- What street did you live on when you were 8 years old?
- What was the last name of your third grade teacher?
- What was your grandfather's occupation?
- What was your grandmother's occupation?

Answer:

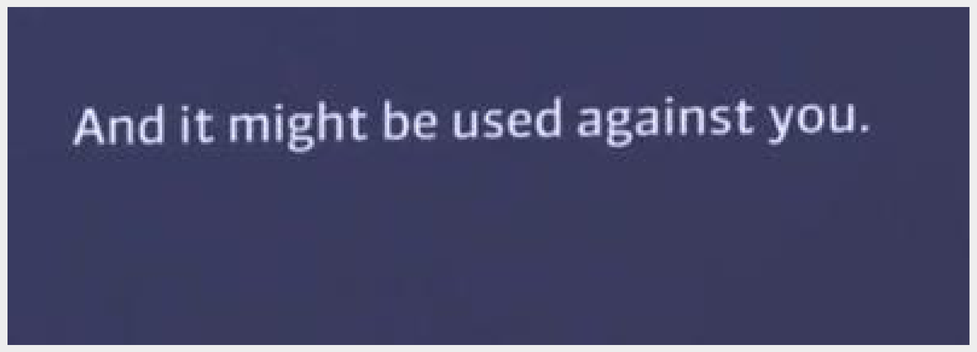
To save these settings, p

Password:

EXCERTS FROM 'MIND READER' VIDEO



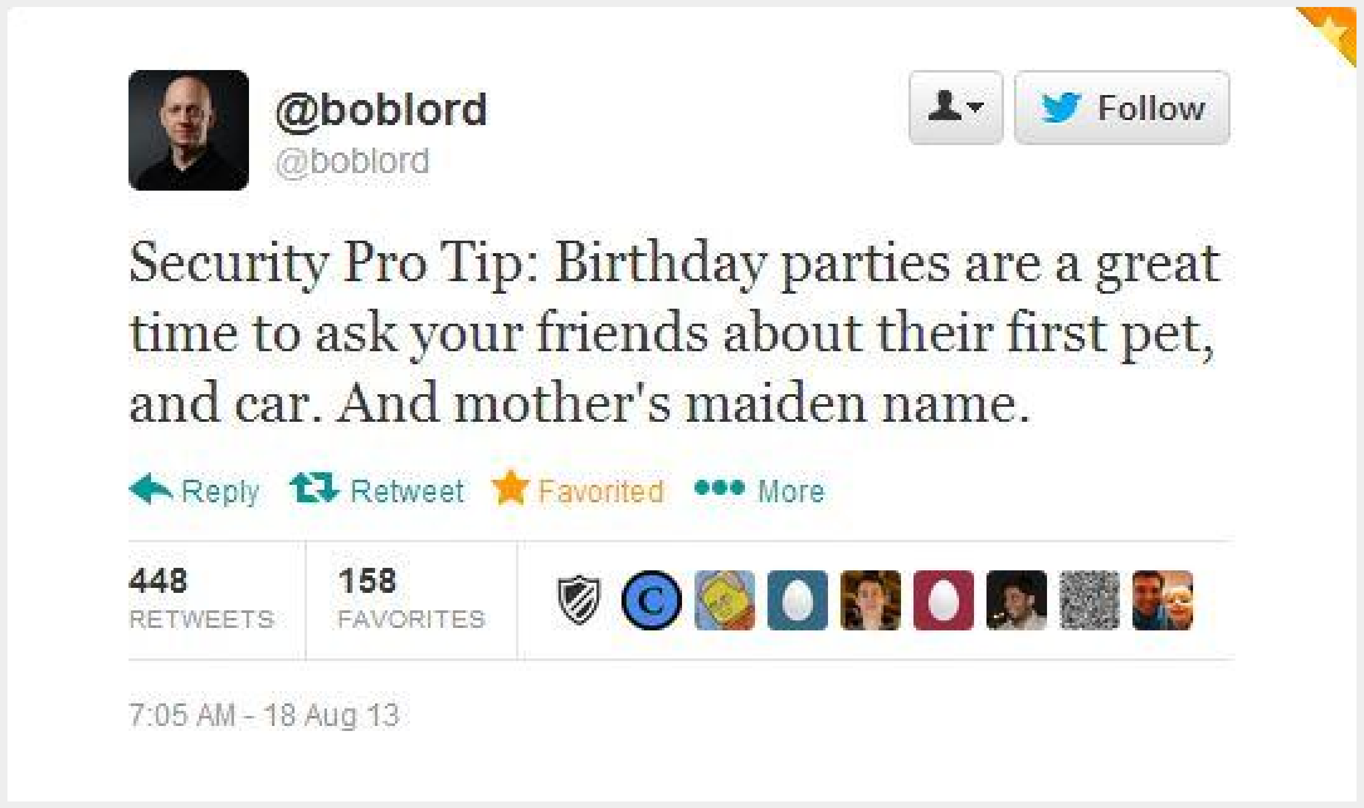
Your entire life is online.



And it might be used against you.

https://www.youtube.com/watch?v=F7pYHN9iC9I

HOW TO GET THE ANSWERS OF THESE QUESTIONS?



@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.

7:05 AM - 18 Aug 13

ACCORDING TO 'ME'

Following ways work like charm:

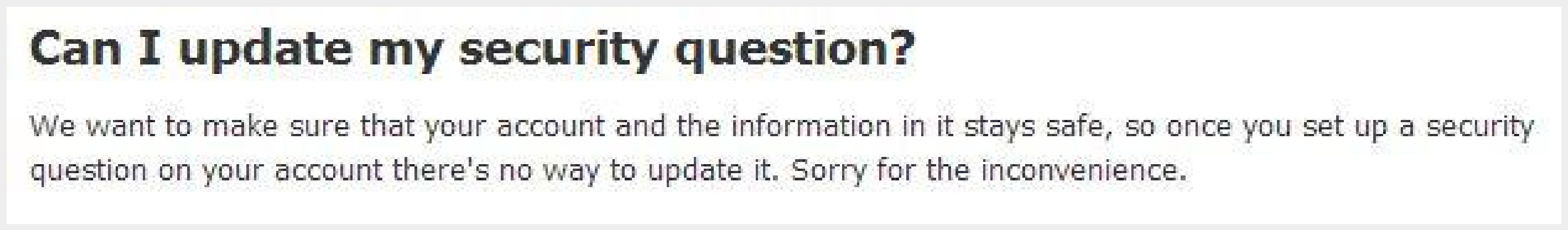
-- In case of social network, answer can be found on public profile.

-- 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



Can I update my security question?

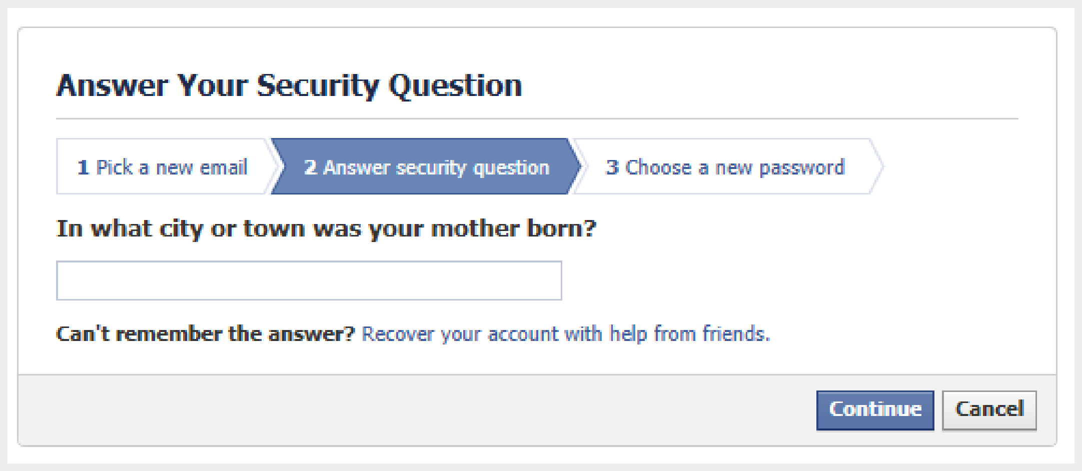
We want to make sure that your account and the information in it stays safe, so once you set up a security question on your account there's no way to update it. Sorry for the inconvenience.

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.

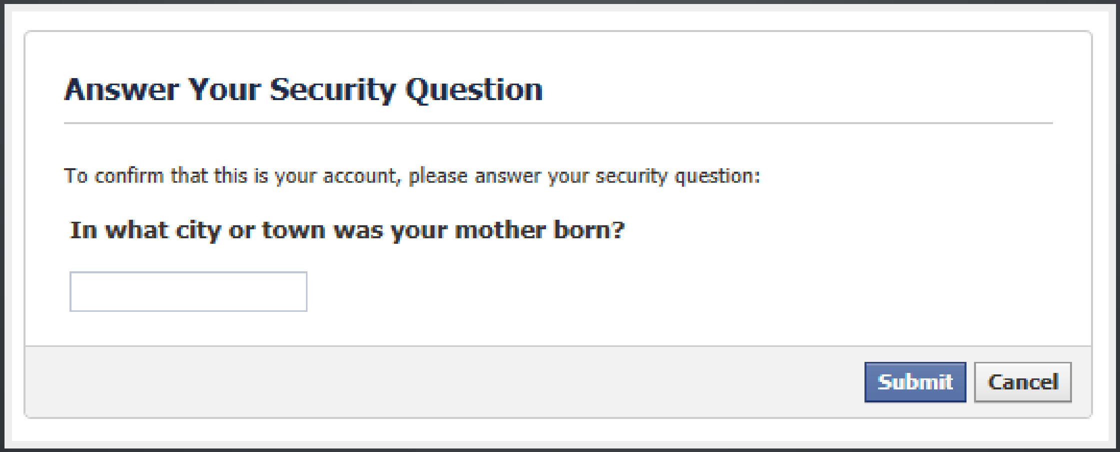
INCONSISTENCY IN SECURITY QUESTIONS' USER INTERFACE



Answer Your Security Question

In what city or town was your mother born?

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

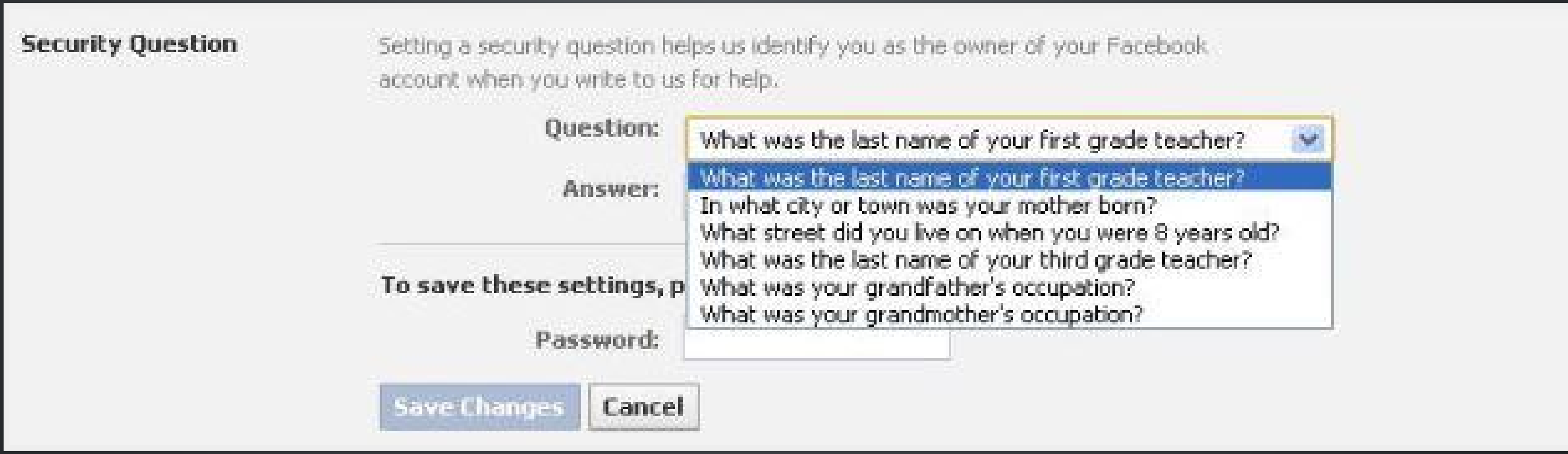


Answer Your Security Question

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

In what city or town was your mother born?

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: What was the last name of your first grade teacher?

- What was the last name of your first grade teacher?
- In what city or town was your mother born?
- What street did you live on when you were 8 years old?
- What was the last name of your third grade teacher?
- What was your grandfather's occupation?
- What was your grandmother's occupation?

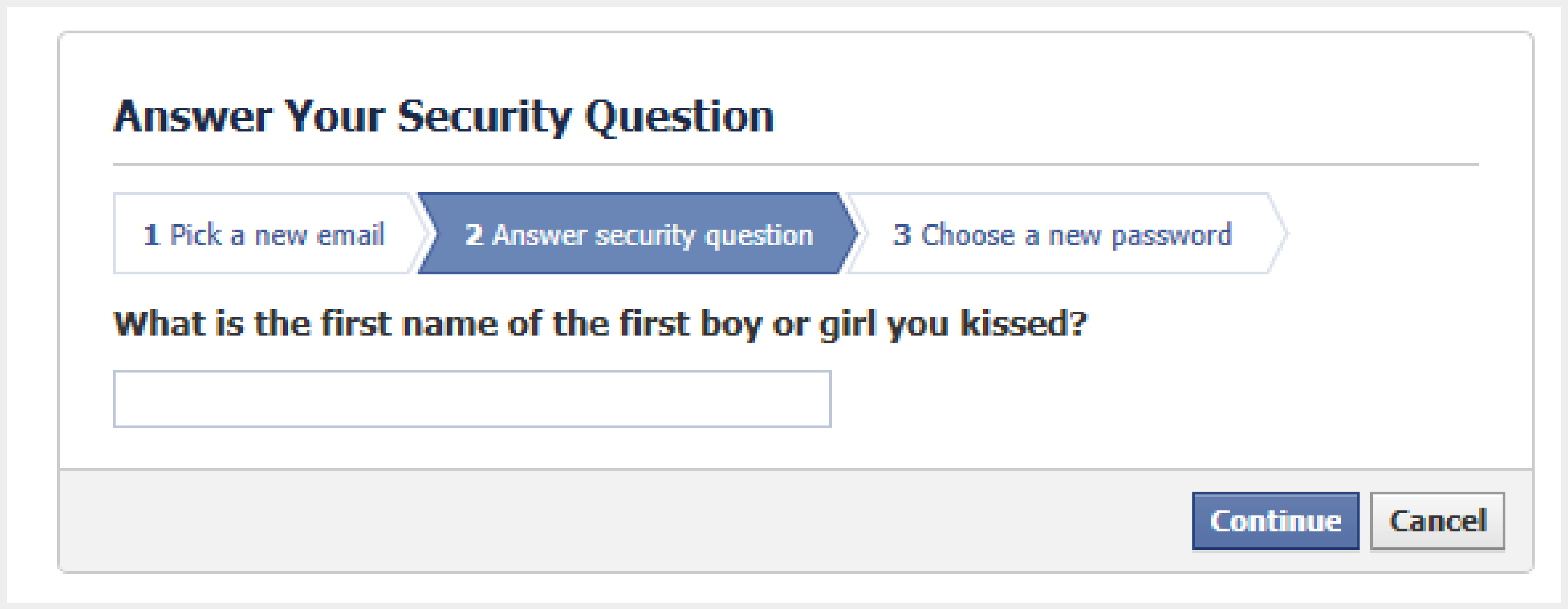
Answer:

To save these settings, p

Password:

MY REACTION :-)

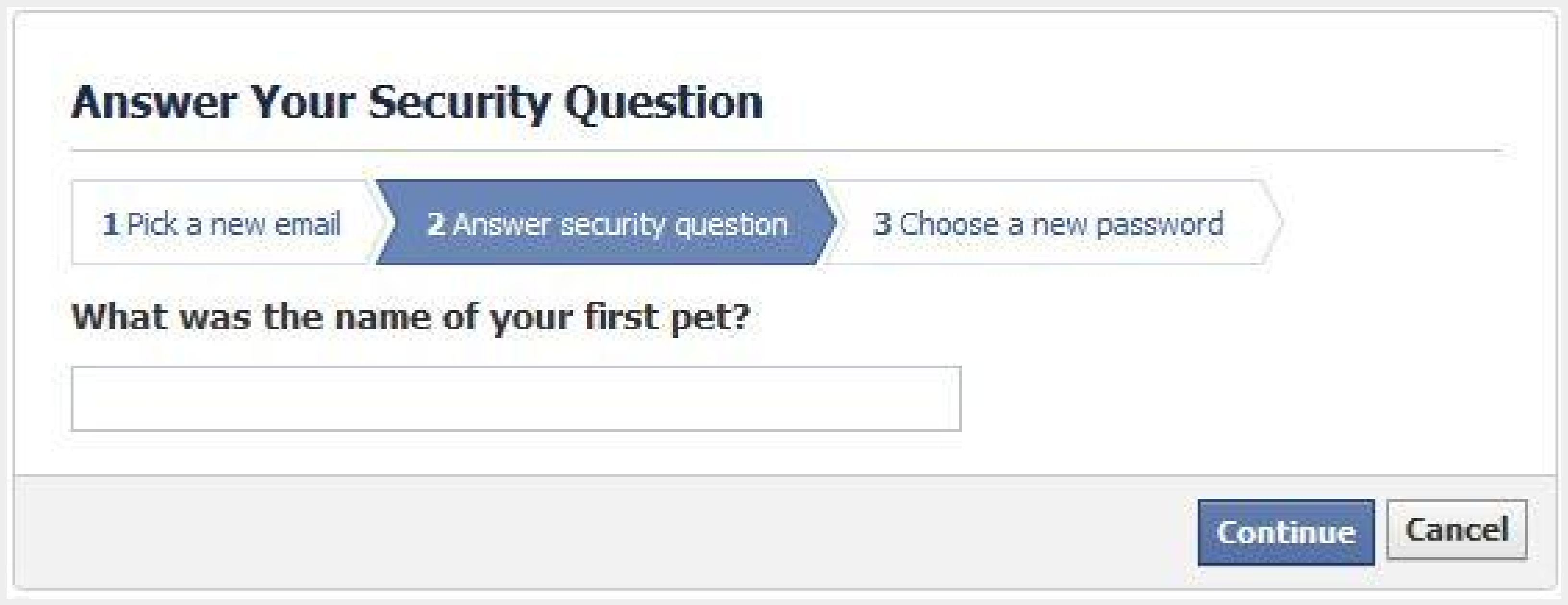
SECURITY QUESTION # 1



Answer Your Security Question

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

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?

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)

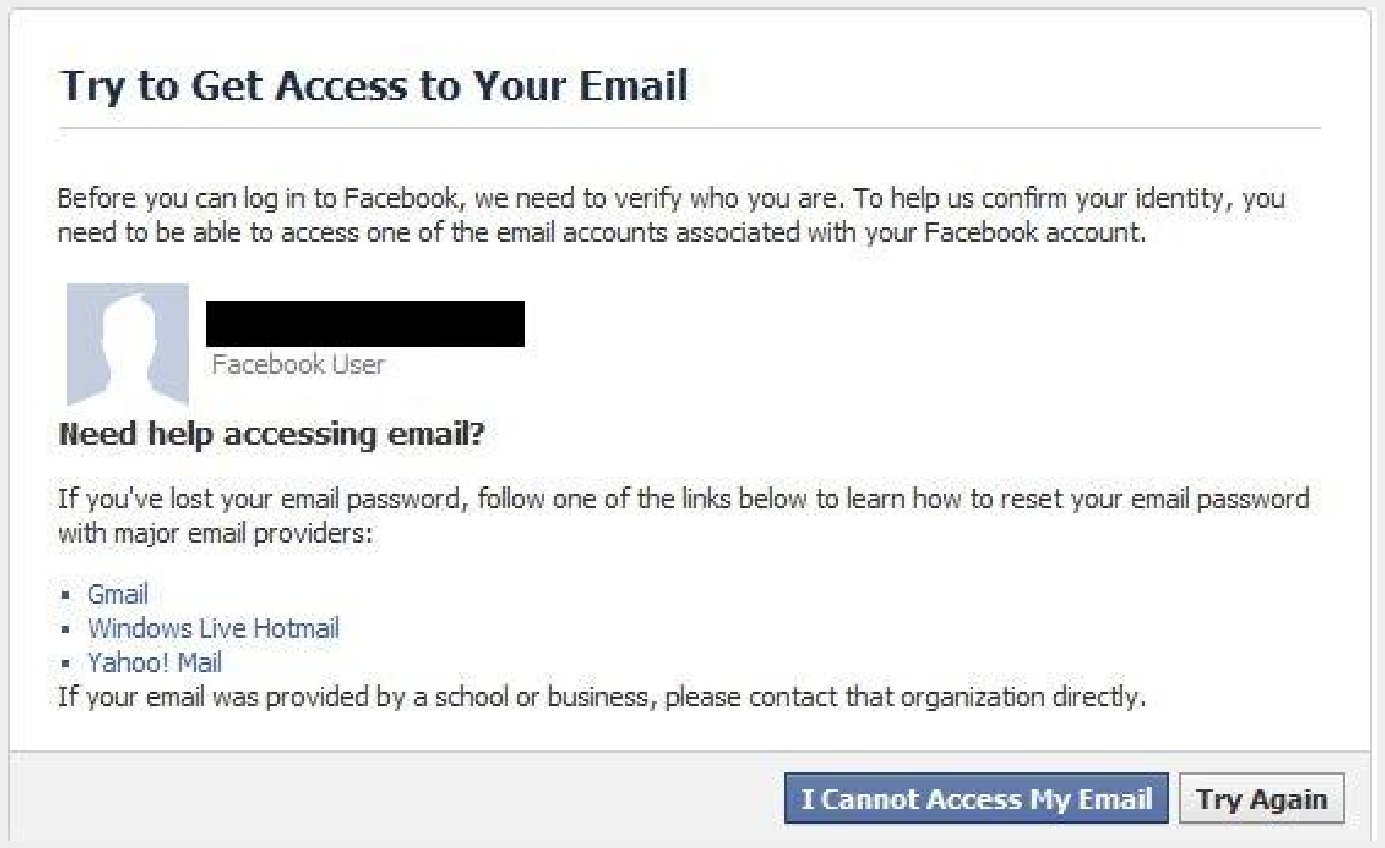
EMPIRICAL STUDY

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.

[redacted]
Facebook User

Need help accessing email?

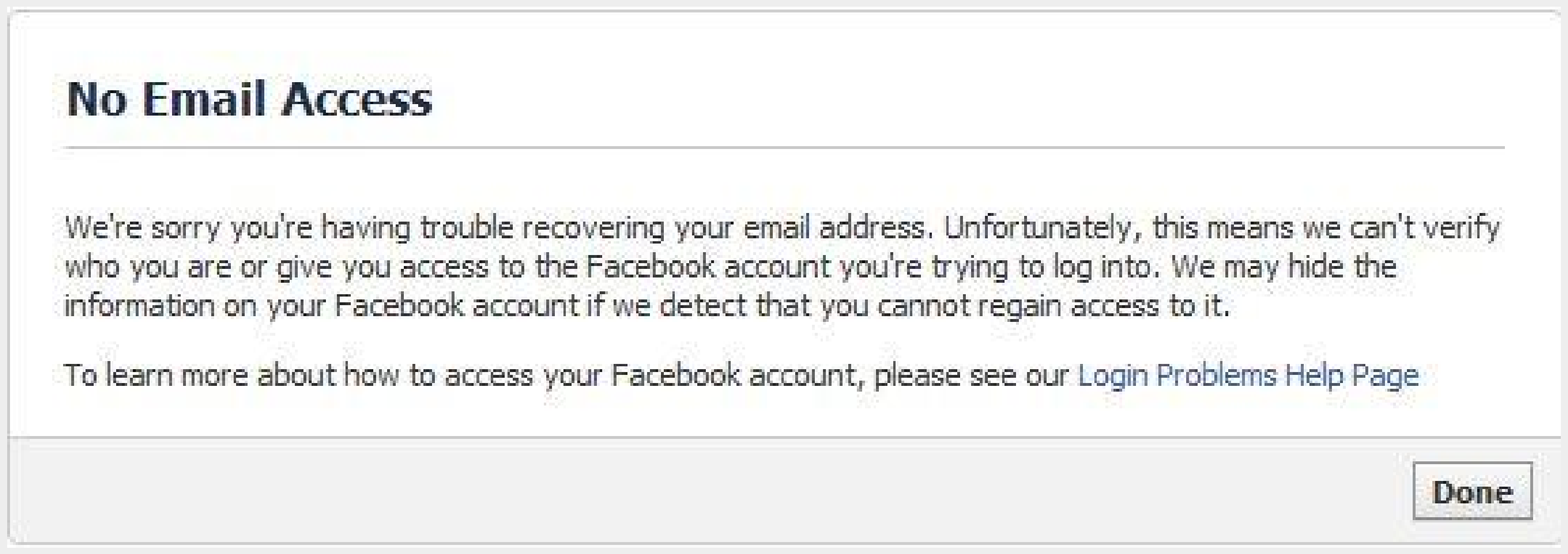
If you've lost your email password, follow one of the links below to learn how to reset your email password with major email providers:

- Gmail
- Windows Live Hotmail
- Yahoo! Mail

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

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

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

IN 69 CASES

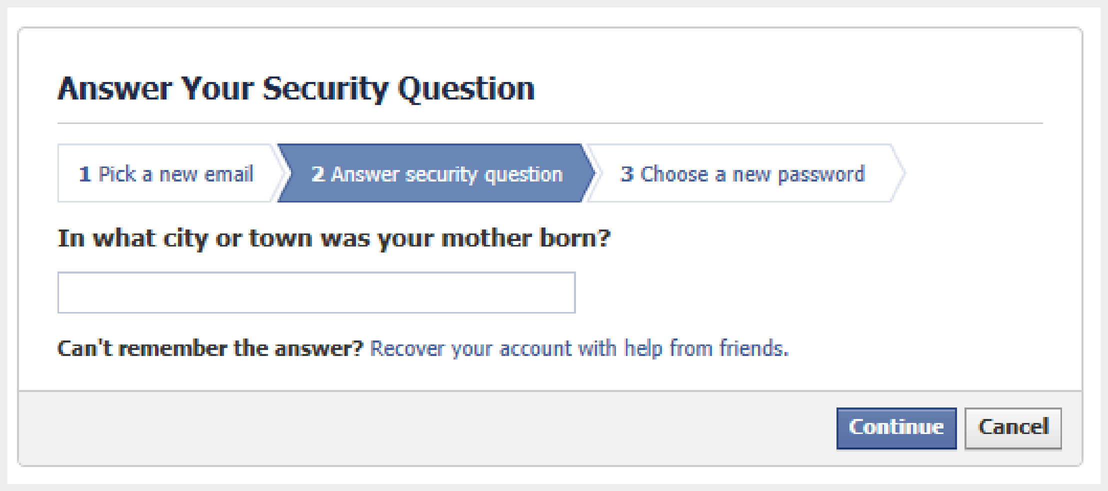
Facebook exposed the selected security question of the victim

OR

Option of Trusted friends' selection

OR

Choice among above two options



Answer Your Security Question

In what city or town was your mother born?

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

11 OUT OF 69 ACCOUNTS COMPROMISED

Out of 11 compromised accounts

8 by answering security question

AND

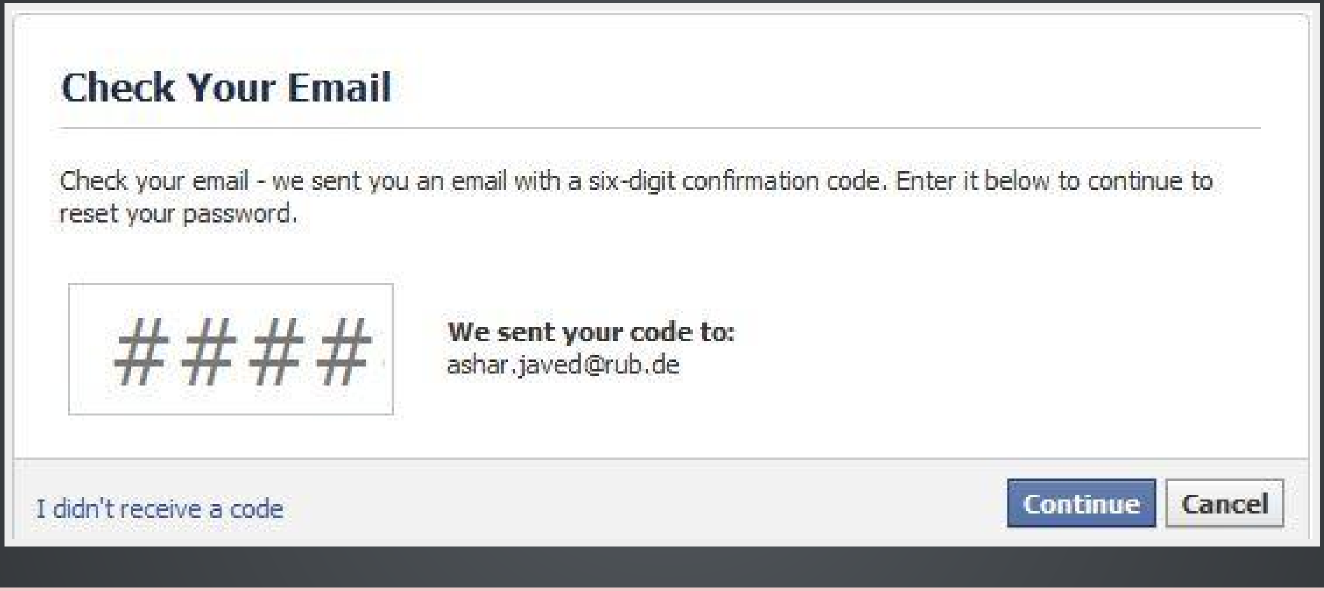
3 using trusted friends feature

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.

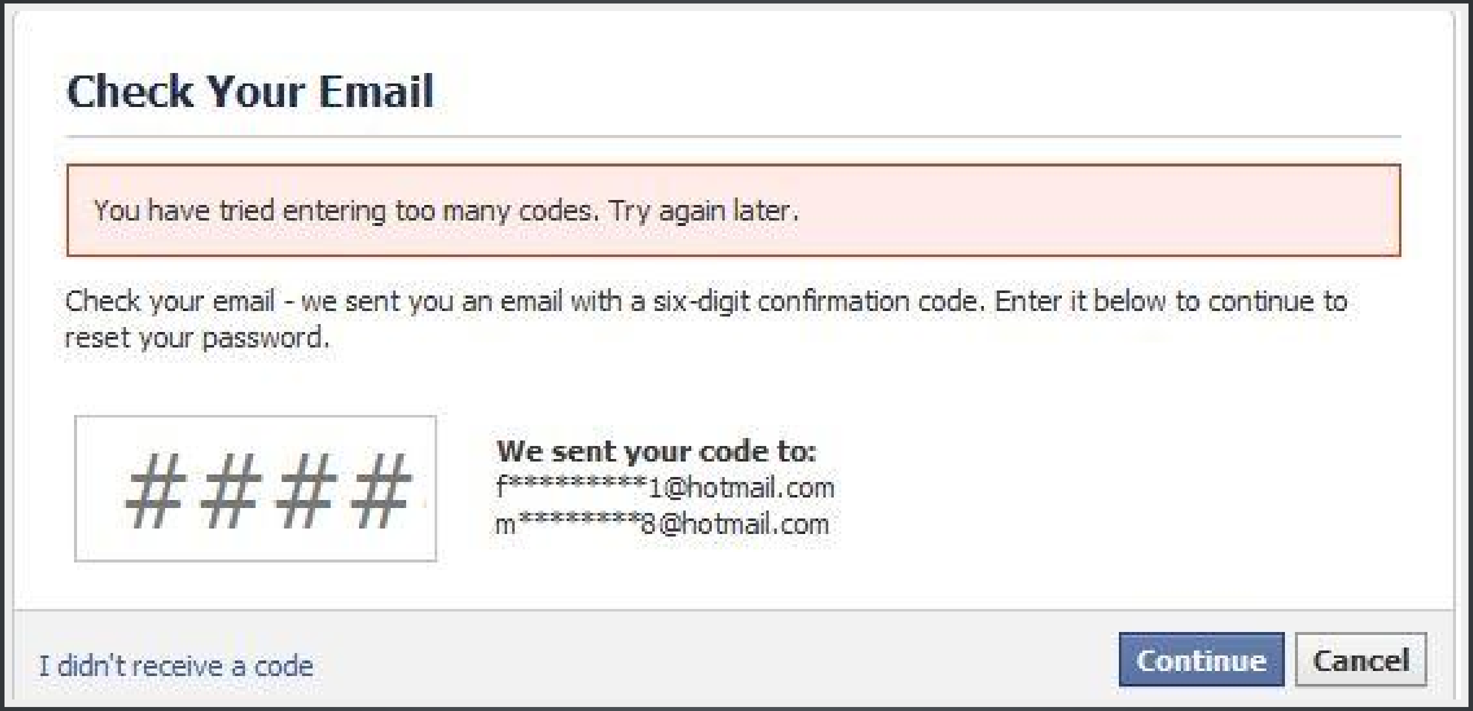
####

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

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:



Check Your Email

You have tried entering too many codes. Try again later.

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

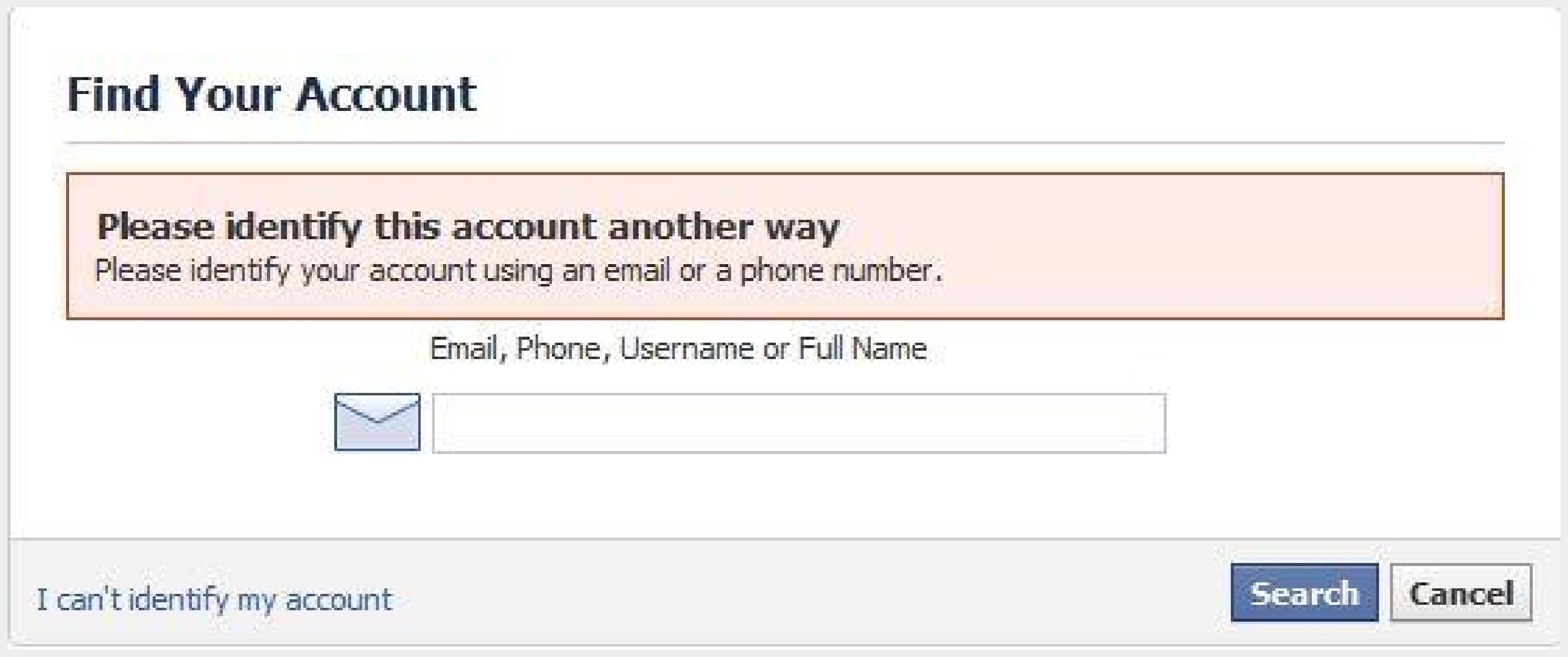
####

We sent your code to:
f**********1@hotmail.com
m*********8@hotmail.com

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

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

IDENTIFY ACCOUNT ANOTHER WAY



Find Your Account

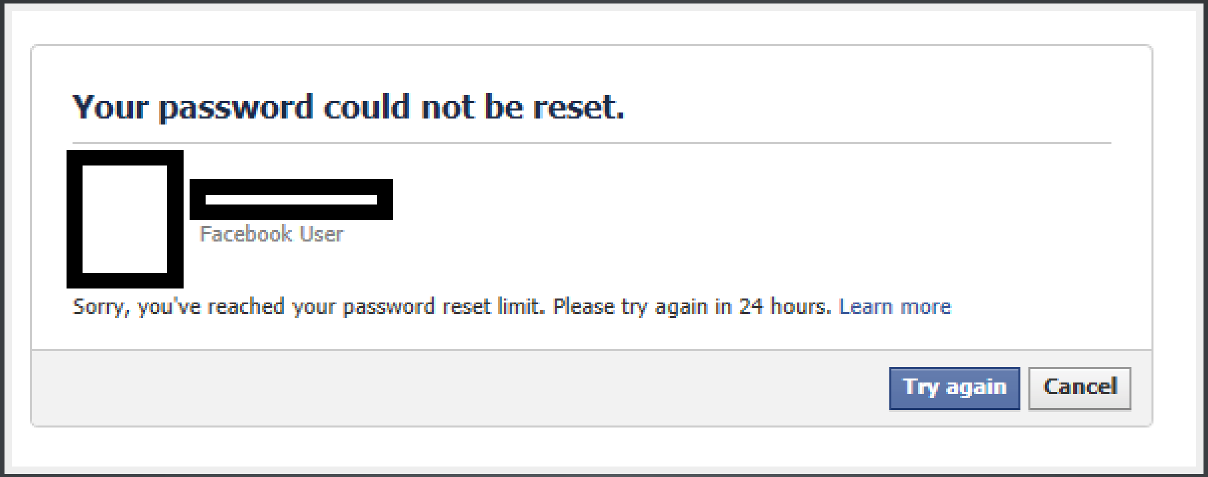
Please identify this account another way

Please identify your account using an email or a phone number.

Email, Phone, Username or Full Name

In this way, attacker can force victim to use email address or phone and if victim has lost his email address ....

WORST THING

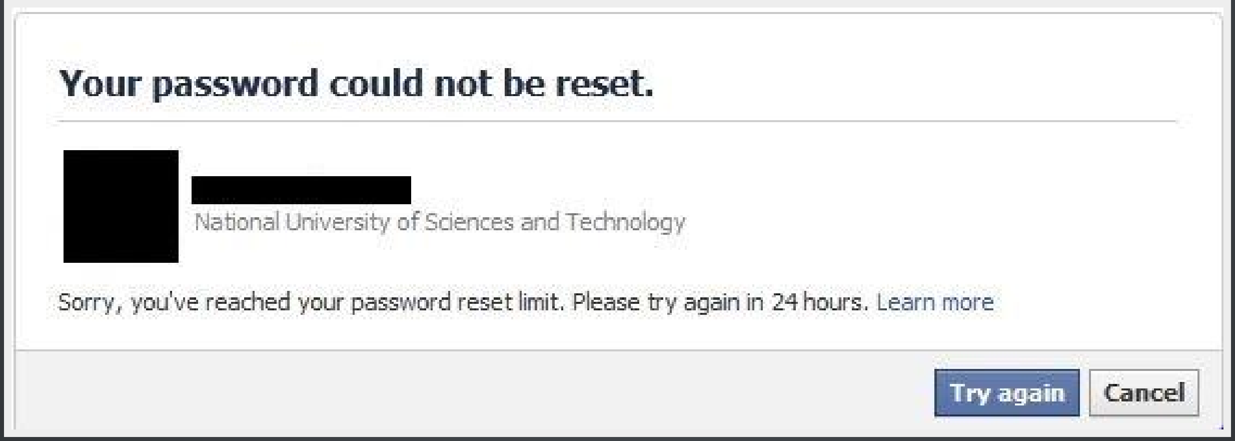


Your password could not be reset.

[redacted] [redacted]

Facebook User

Sorry, you've reached your password reset limit. Please try again in 24 hours. Learn more



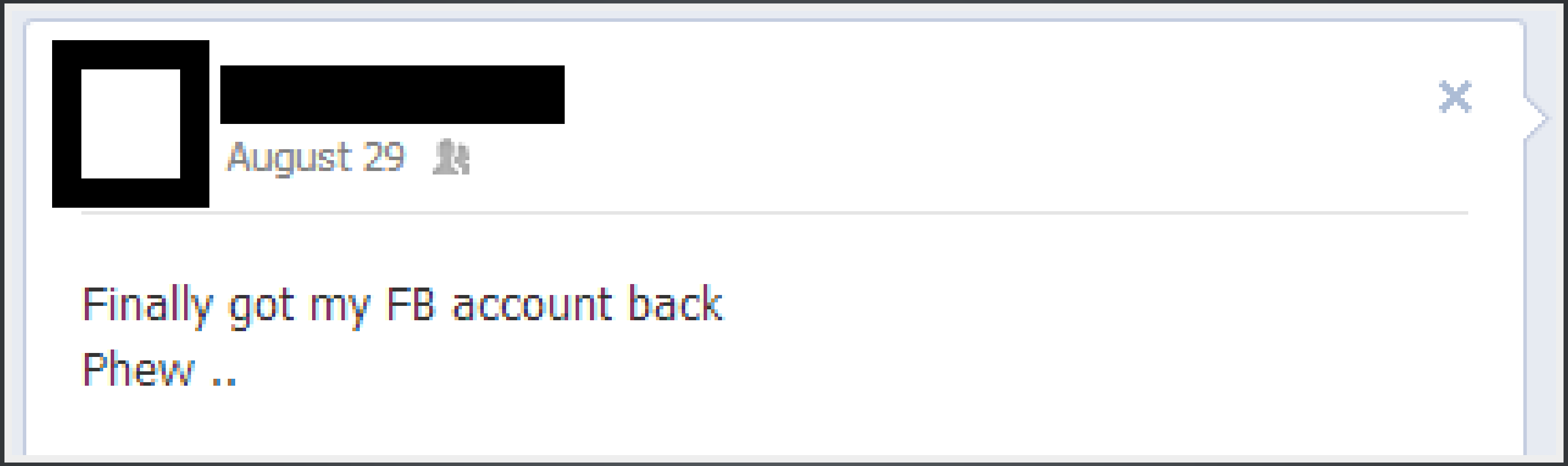
Your password could not be reset.

[redacted] [redacted]

National University of Sciences and Technology

Sorry, you've reached your password reset limit. Please try again in 24 hours. Learn more

MY FRIEND’S REACTION ON WORST THING



[redacted]

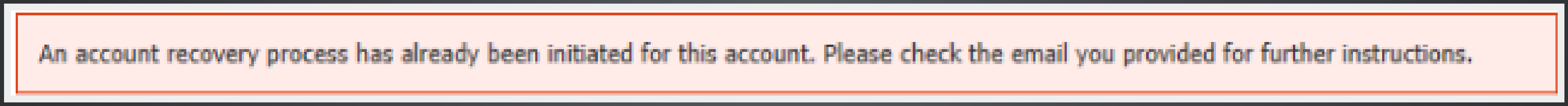
August 29

Finally got my FB account back
Phew ..

ANOTHER TYPE OF DOS ON FACEBOOK

TRUSTED FRIEND FEATURE DOS

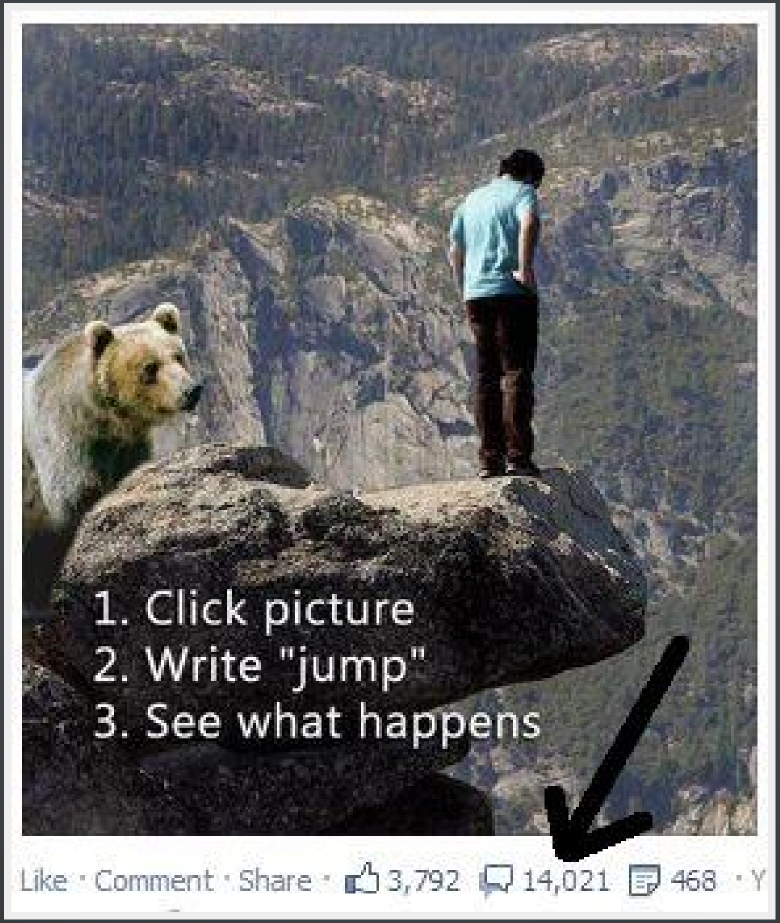
If an attacker has started the password recovery using **TF** and at the same time victim tries to use this feature ... he will receive the following message from Facebook



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...

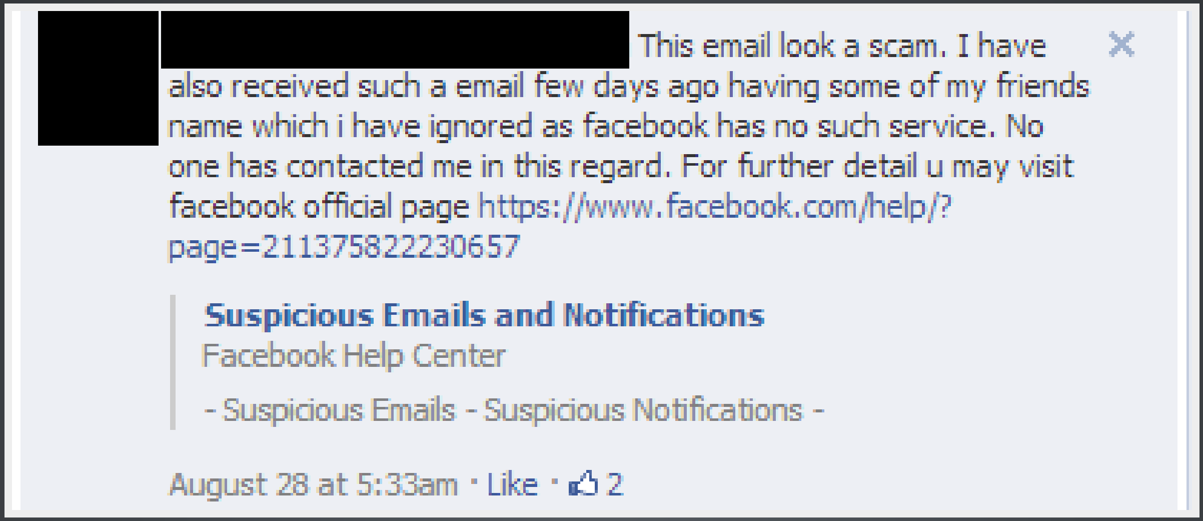


1. Click picture
2. Write "jump"
3. See what happens

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

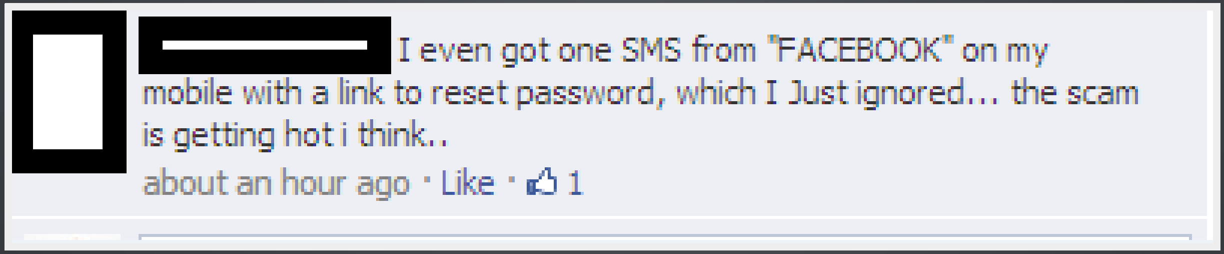


[redacted] [redacted] This email look a scam. I have also received such a email few days ago having some of my friends name which i have ignored as facebook has no such service. No one has contacted me in this regard. For further detail u may visit facebook official page https://www.facebook.com/help/?page=211375822230657

Suspicious Emails and Notifications
Facebook Help Center

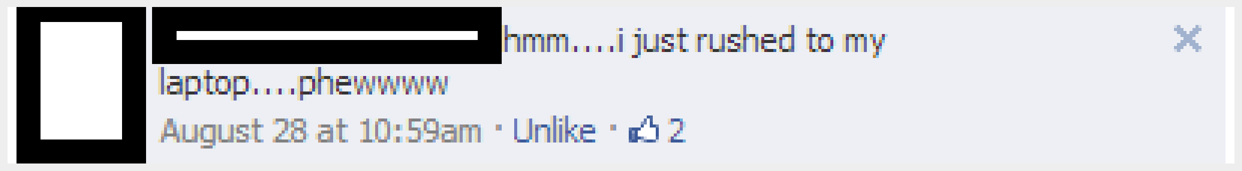
- Suspicious Emails - Suspicious Notifications -

August 28 at 5:33am · Like · 👍 2



[redacted] [redacted] 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..

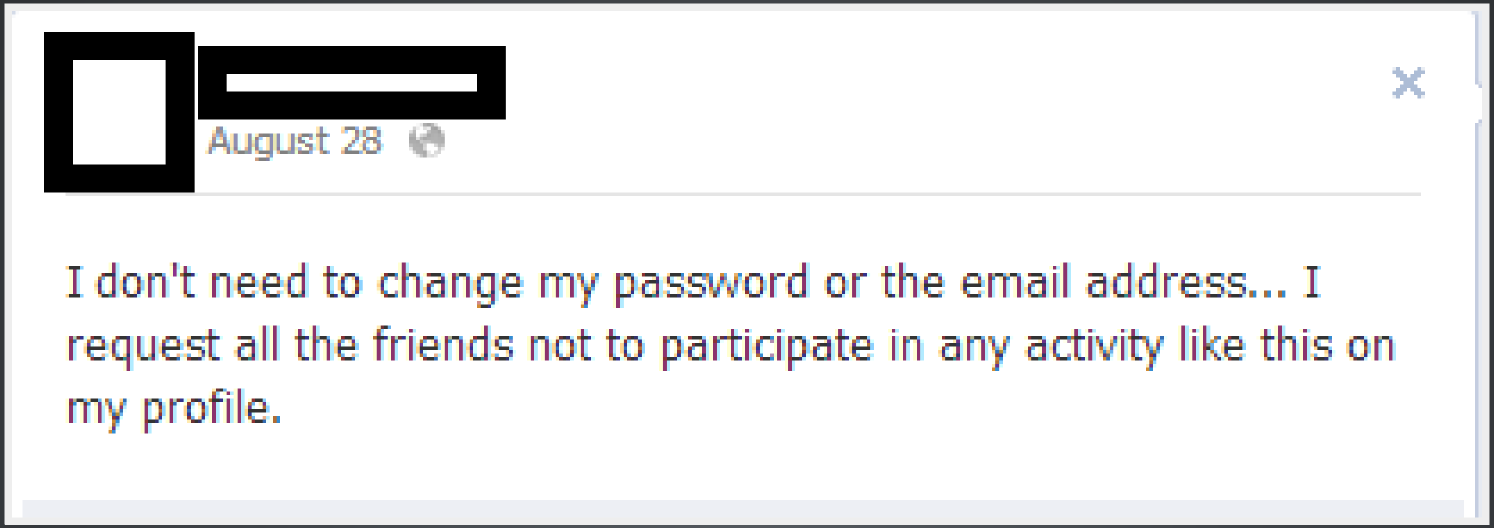
about an hour ago · Like · 👍 1



[redacted] [redacted] hmm....i just rushed to my laptop....phewwww

August 28 at 10:59am · Unlike · 👍 2

USERS' REACTION ON THIS EMAIL OR SMS

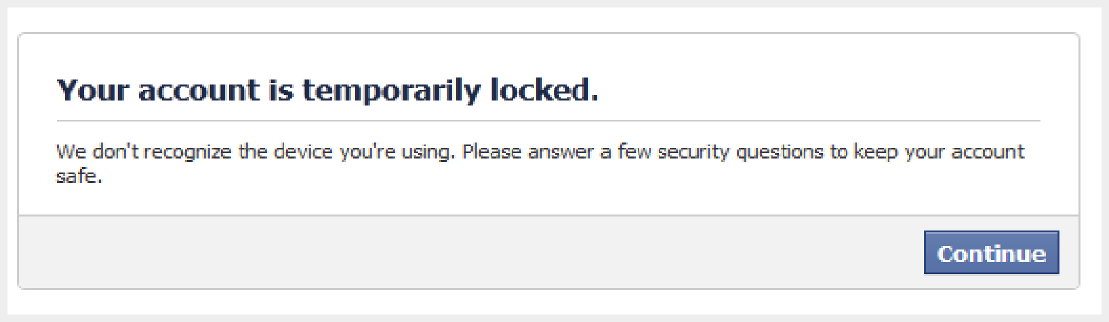


[redacted] [redacted]

August 28

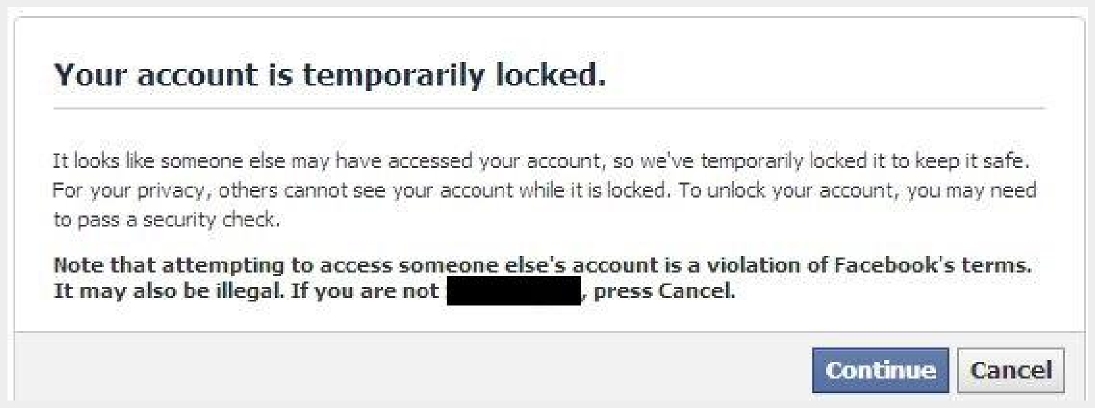
I don't need to change my password or the email address... I request all the friends not to participate in any activity like this on my profile.

2) TEMPORARILY LOCKED



Your account is temporarily locked.

We don't recognize the device you're using. Please answer a few security questions to keep your account safe.



Your account is temporarily locked.

It looks like someone else may have accessed your account, so we've temporarily locked it to keep it safe. For your privacy, others cannot see your account while it is locked. To unlock your account, you may need to pass a security check.

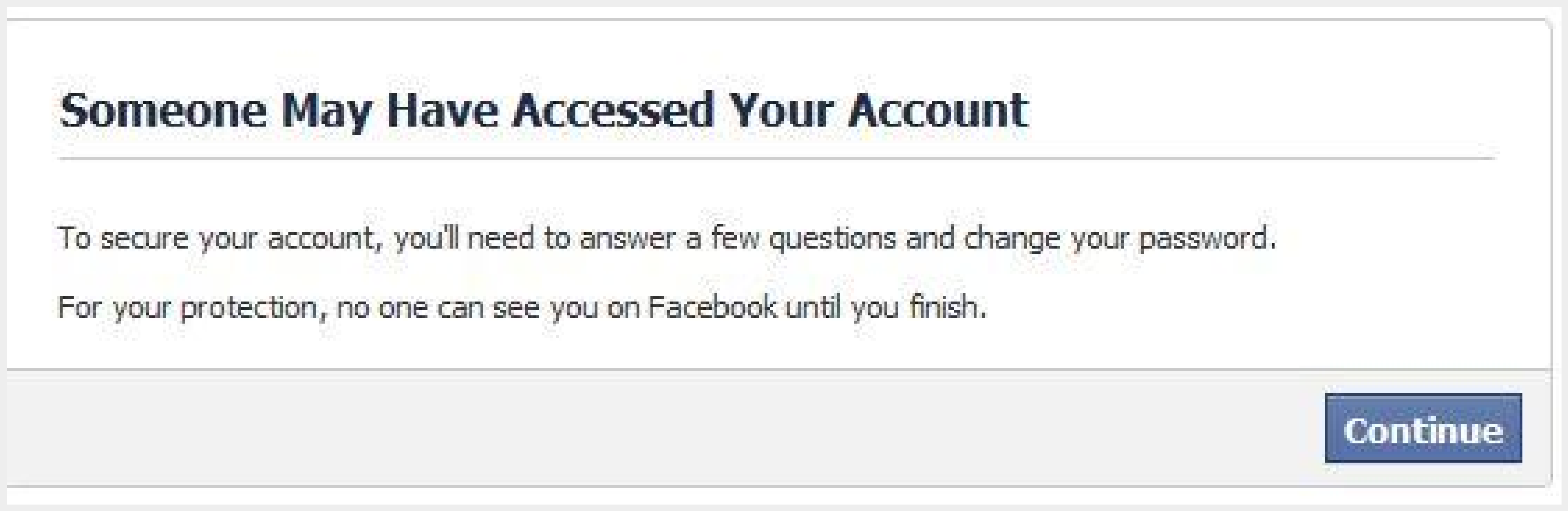
Note that attempting to access someone else's account is a violation of Facebook's terms. It may also be illegal. If you are not [redacted], press Cancel.

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)

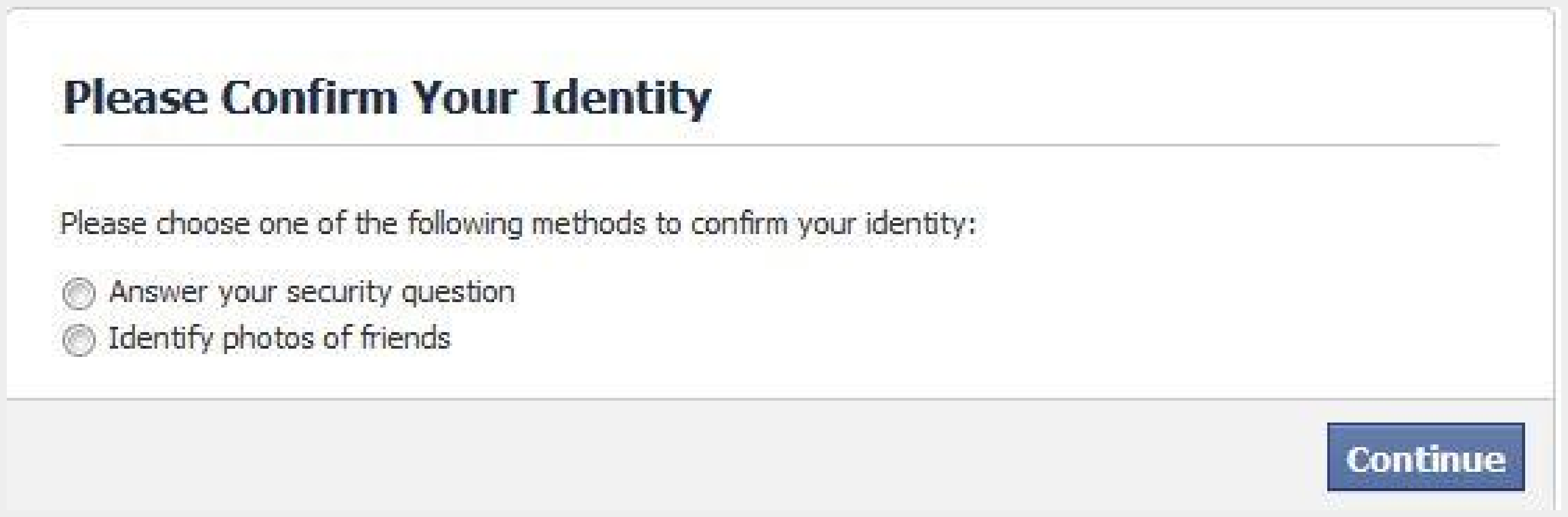


Someone May Have Accessed Your Account

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.

(2)



Please Confirm Your Identity

Please choose one of the following methods to confirm your identity:

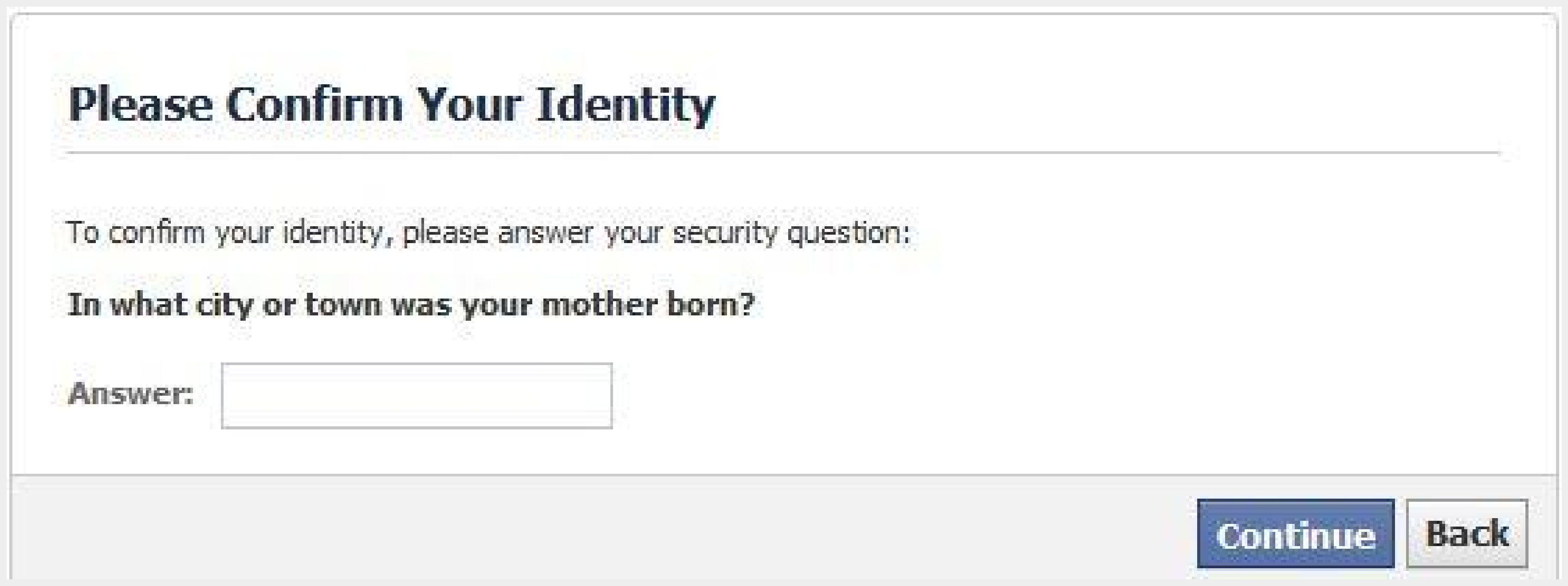
○ Answer your security question

○ Identify photos of friends

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

An ATTACKER

(3)



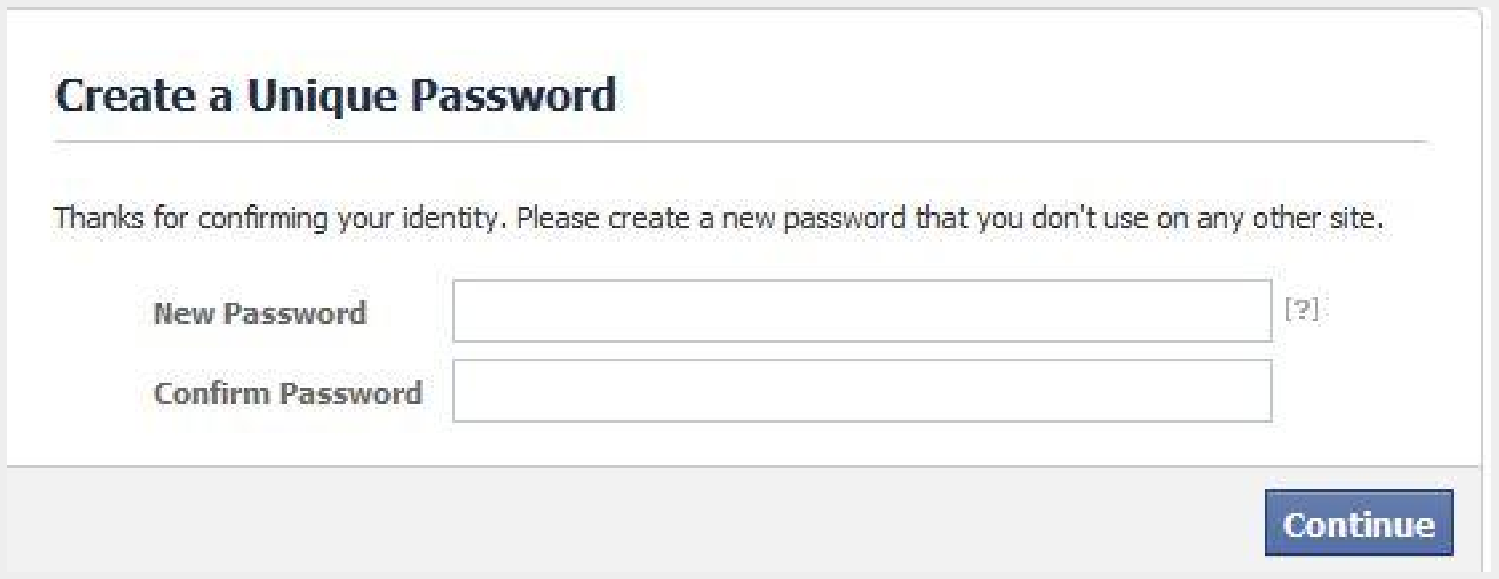
Please Confirm Your Identity

To confirm your identity, please answer your security question:

In what city or town was your mother born?

Answer:

(4)



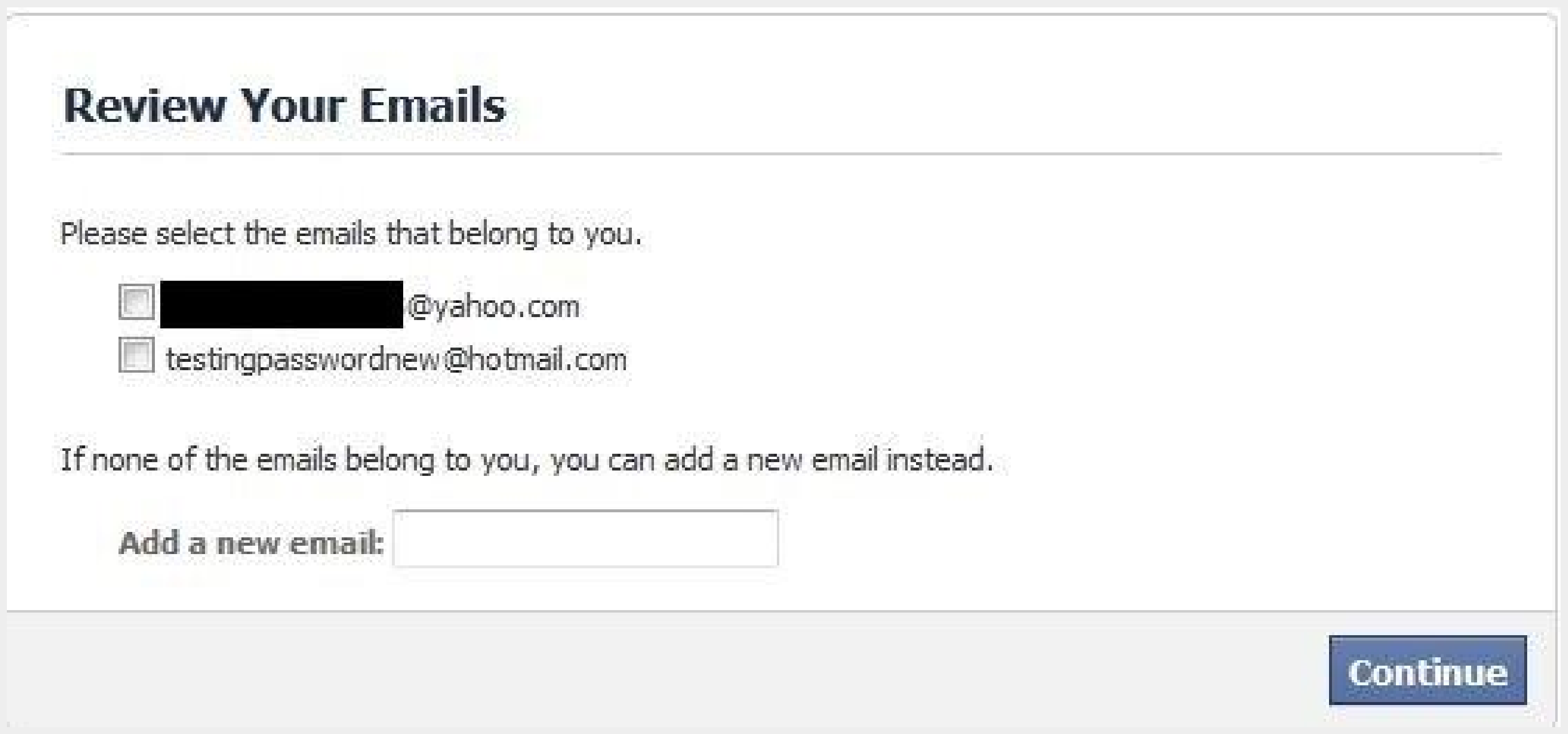
Create a Unique Password

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

New Password [?]

Confirm Password

(5)



Review Your Emails

Please select the emails that belong to you.

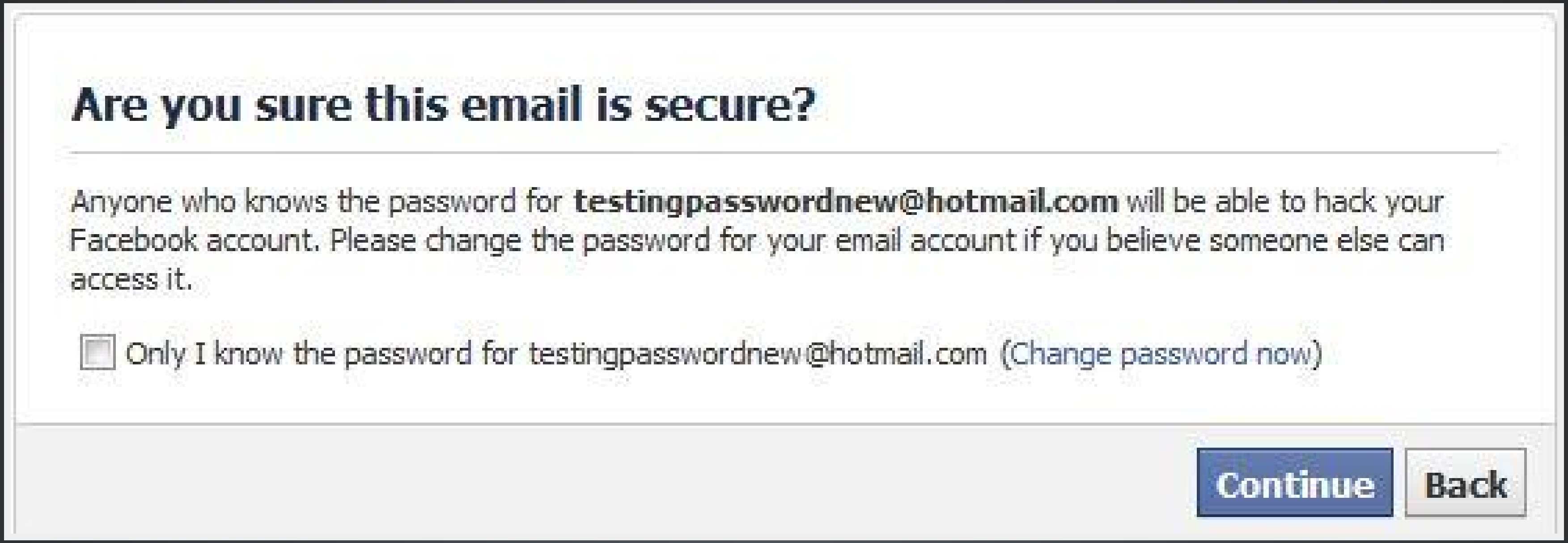
□ [redacted]@yahoo.com

□ testingpasswordnew@hotmail.com

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

Add a new email:

(6)

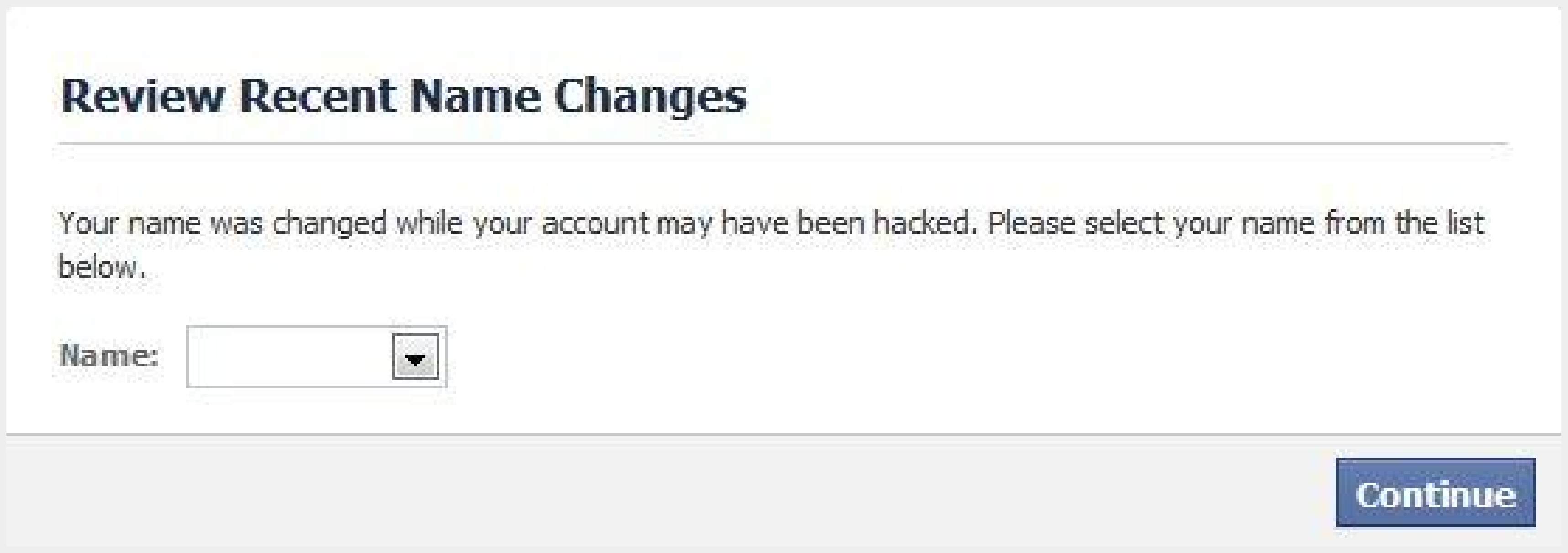


Are you sure this email is secure?

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)

(7)

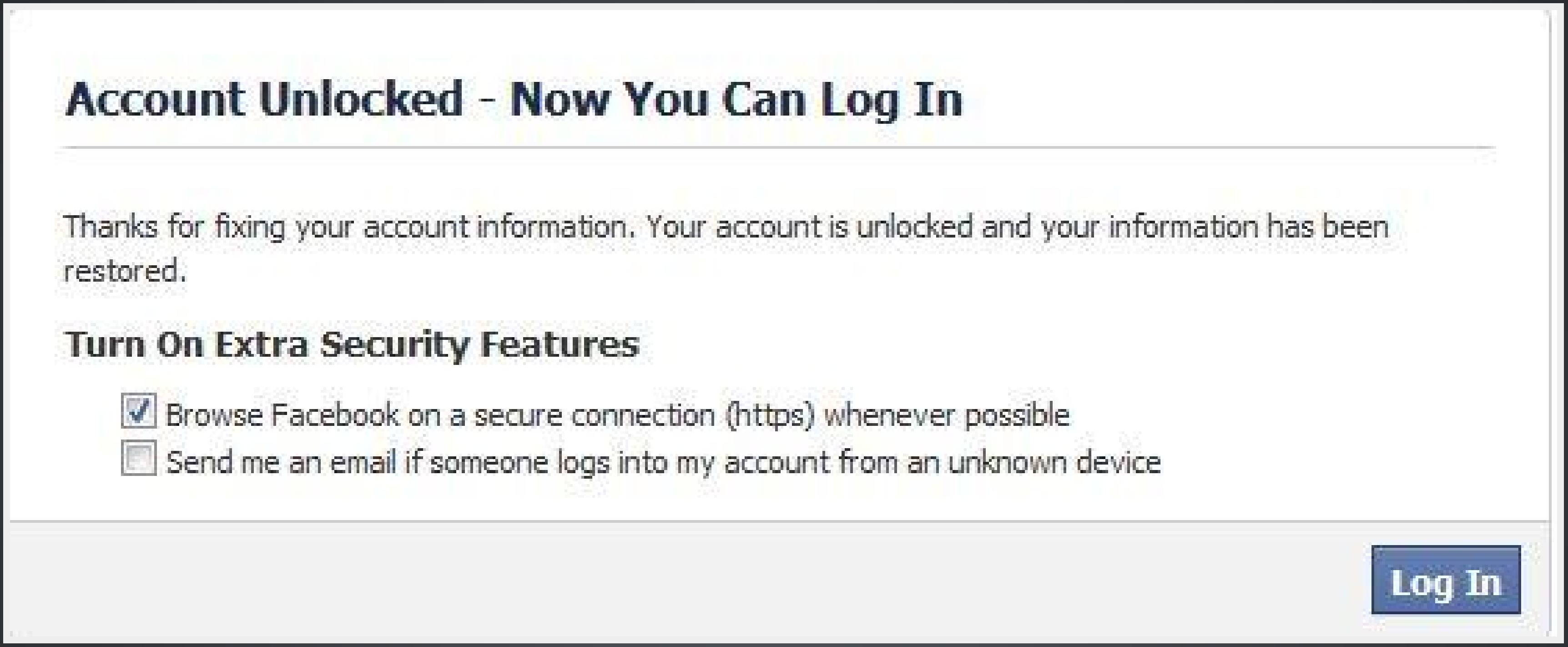


Review Recent Name Changes

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

Name:

(8)



Account Unlocked - Now You Can Log In

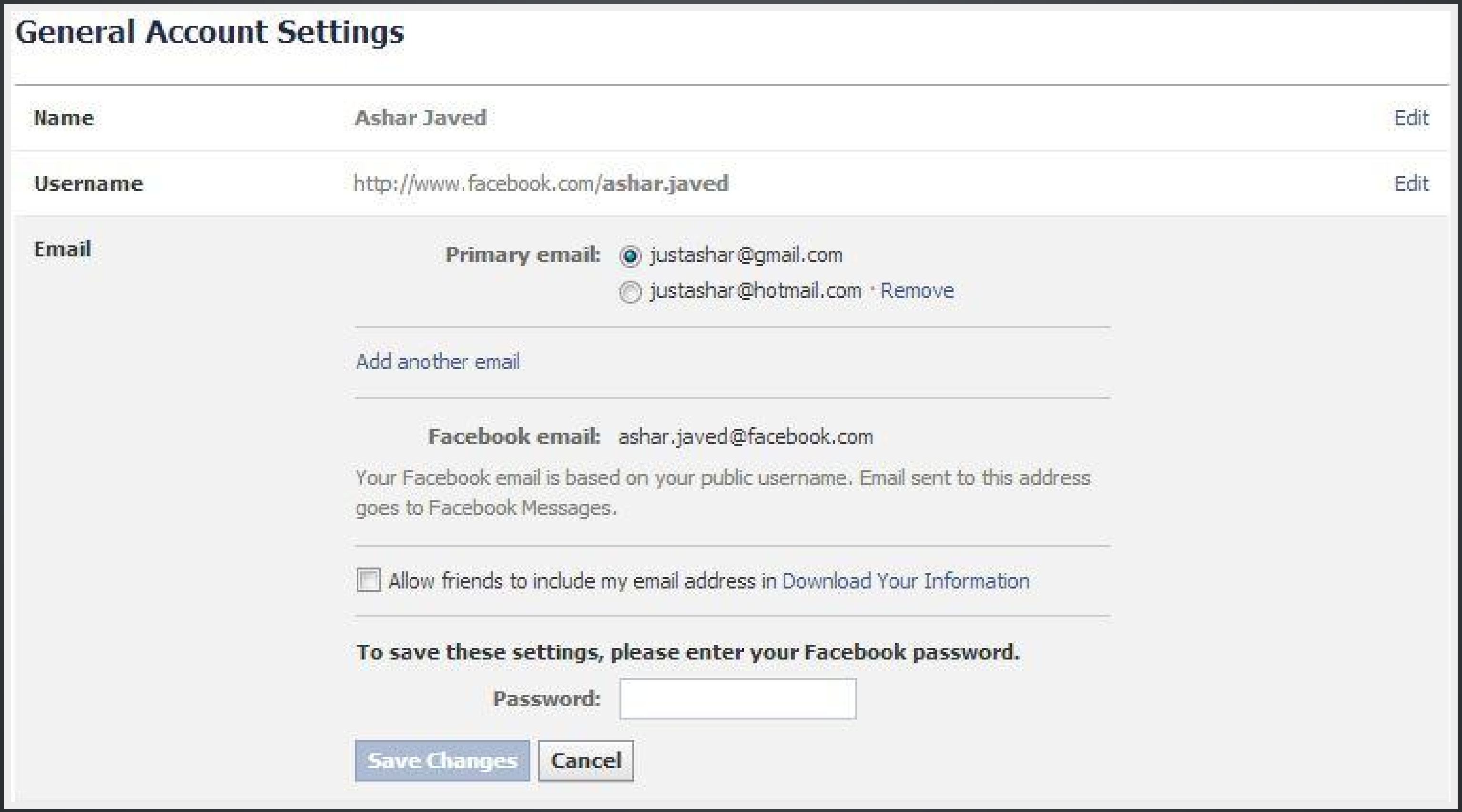
Thanks for fixing your account information. Your account is unlocked and your information has been restored.

Turn On Extra Security Features

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

□ Send me an email if someone logs into my account from an unknown device

ANOTHER INTERESTING ASPECT IN CASE IF LEGITIMATE USER WILL BE ABLE TO REGAIN ACCESS TO HIS ACCOUNT



General Account Settings

Name	Ashar Javed	Edit
Username	http://www.facebook.com/**ashar.javed**	Edit
Email	Primary email: ● justashar@gmail.com ○ justashar@hotmail.com · Remove	

Add another email

Facebook email: ashar.javed@facebook.com

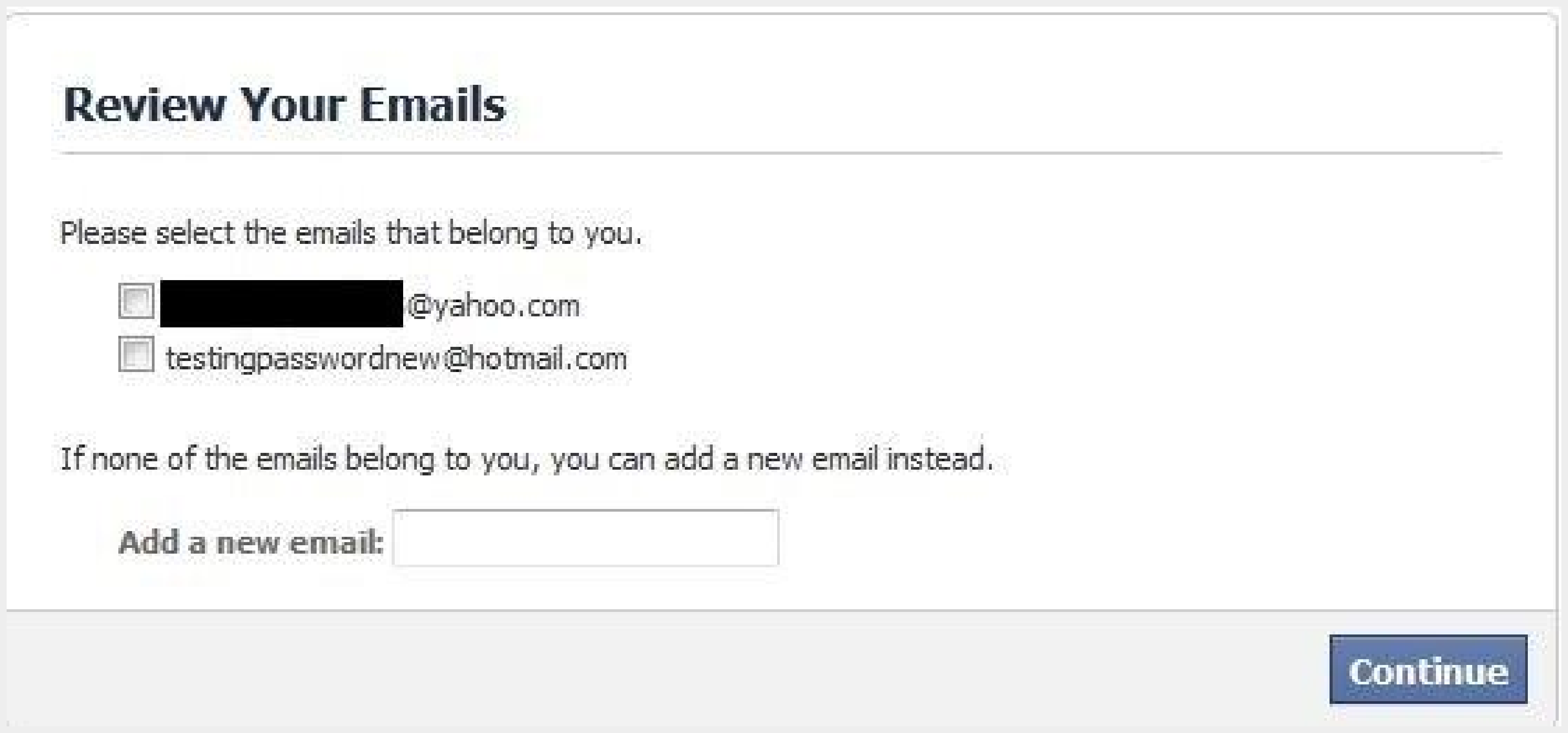
Your Facebook email is based on your public username. Email sent to this address goes to Facebook Messages.

□ Allow friends to include my email address in Download Your Information

To save these settings, please enter your Facebook password.

Password:

REMEMBER (5TH STEP) I.E.,



Review Your Emails

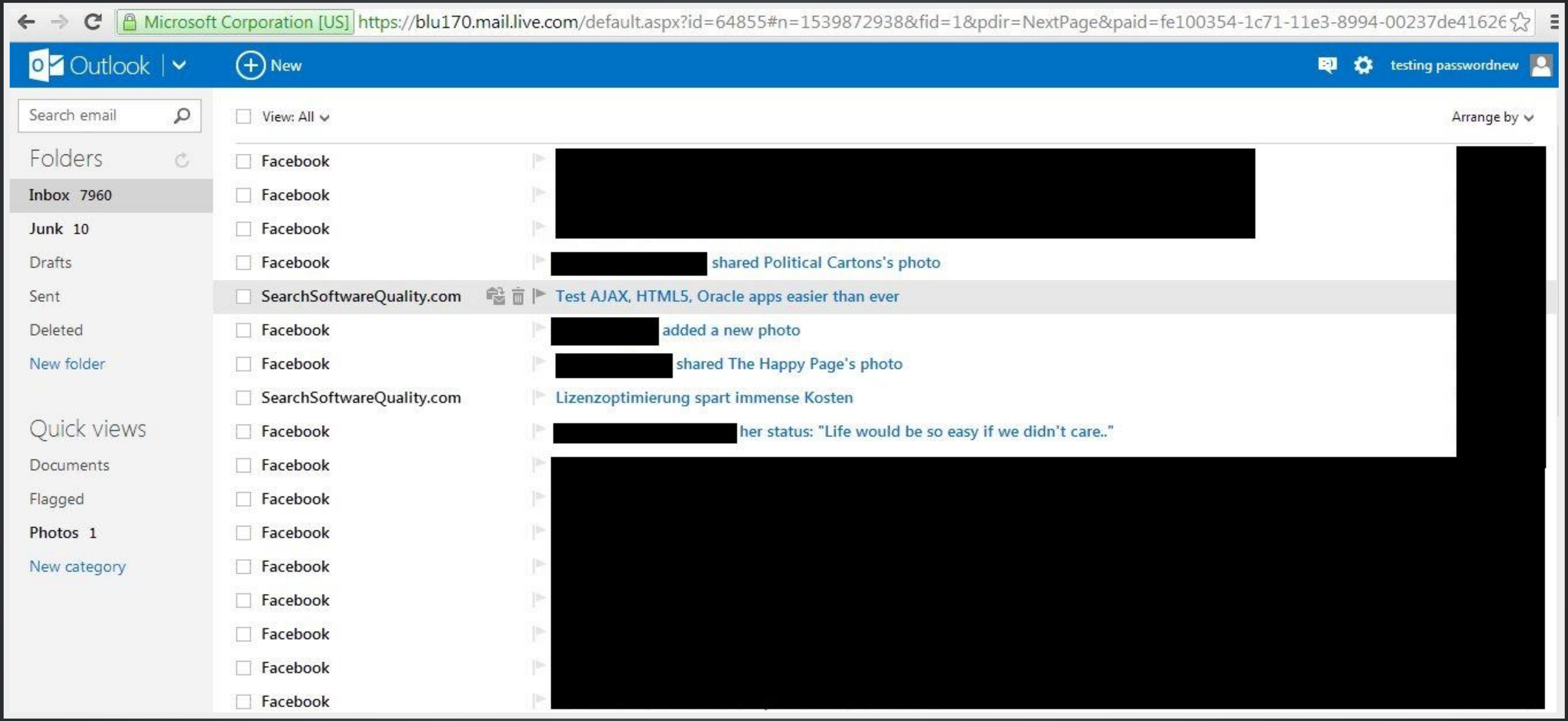
Please select the emails that belong to you.

- □ [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:

SNAPSHOT OF ATTACKER'S EMAIL BOX



https://blu170.mail.live.com/default.aspx?id=64855#n=1539872938&fid=1&pdir=NextPage&paid=fe100354-1c71-11e3-8994-00237de4162

Folders

- Inbox 7960
- Junk 10
- Drafts
- Sent
- Deleted
- New folder

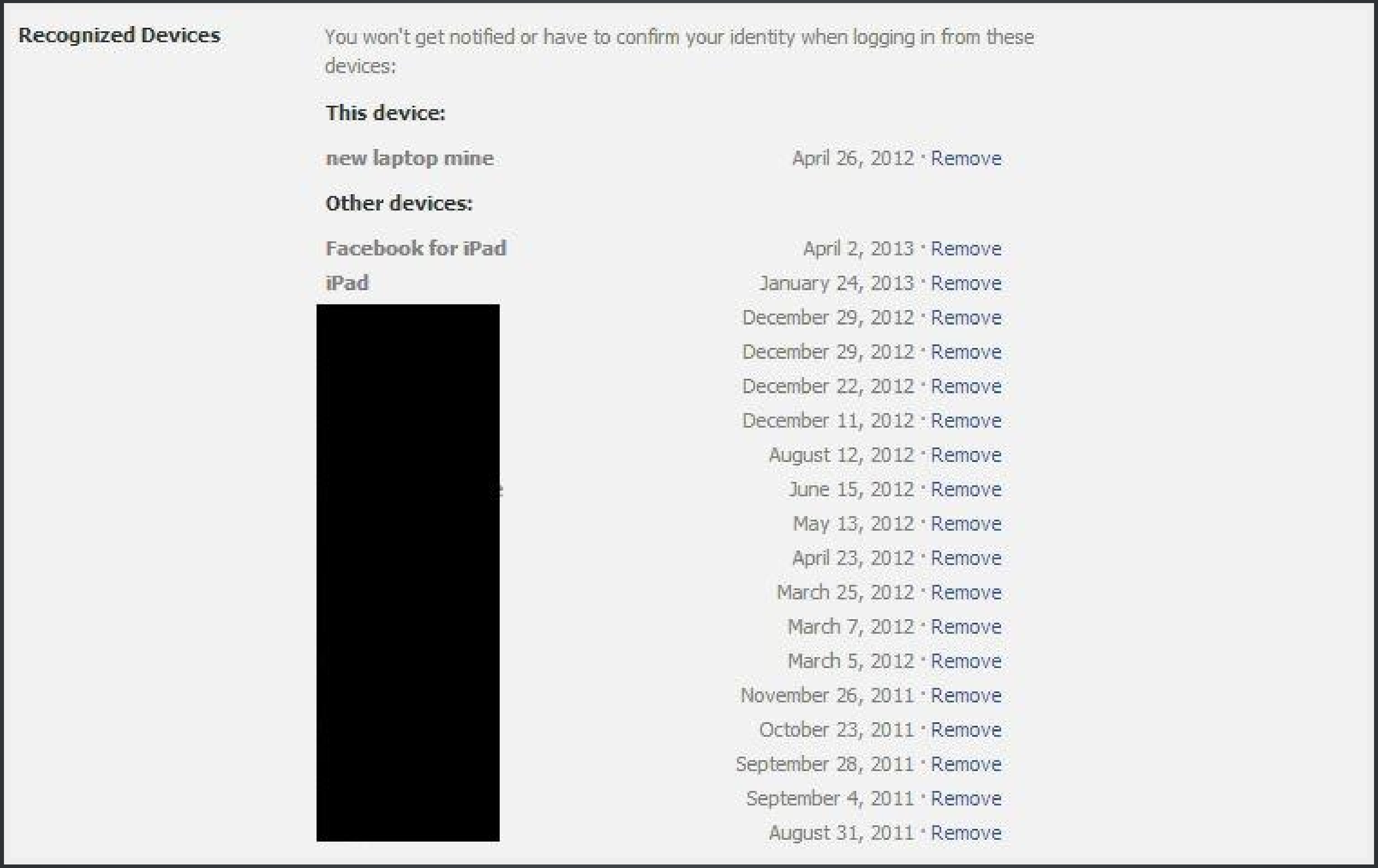
Quick views

- Documents
- Flagged
- Photos 1
- New category

□ Facebook	[redacted]
□ Facebook	[redacted]
□ Facebook	[redacted]
□ Facebook	[redacted] shared Political Cartons's photo
□ SearchSoftwareQuality.com	Test AJAX, HTML5, Oracle apps easier than ever
□ Facebook	[redacted] added a new photo
□ Facebook	[redacted] shared The Happy Page's photo
□ SearchSoftwareQuality.com	Lizenzoptimierung spart immense Kosten
□ Facebook	[redacted] her status: "Life would be so easy if we didn't care.."
□ Facebook	[redacted]
□ Facebook	[redacted]
□ Facebook	[redacted]
□ Facebook	[redacted]
□ Facebook	[redacted]
□ Facebook	[redacted]
□ Facebook	[redacted]
□ Facebook	[redacted]

[redacted]

RECOGNIZED DEVICES



Recognized Devices

You won't get notified or have to confirm your identity when logging in from these devices:

This device:

new laptop mine April 26, 2012 · Remove

Other devices:

Facebook for iPad April 2, 2013 · Remove

iPad January 24, 2013 · Remove

[redacted]

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 ...

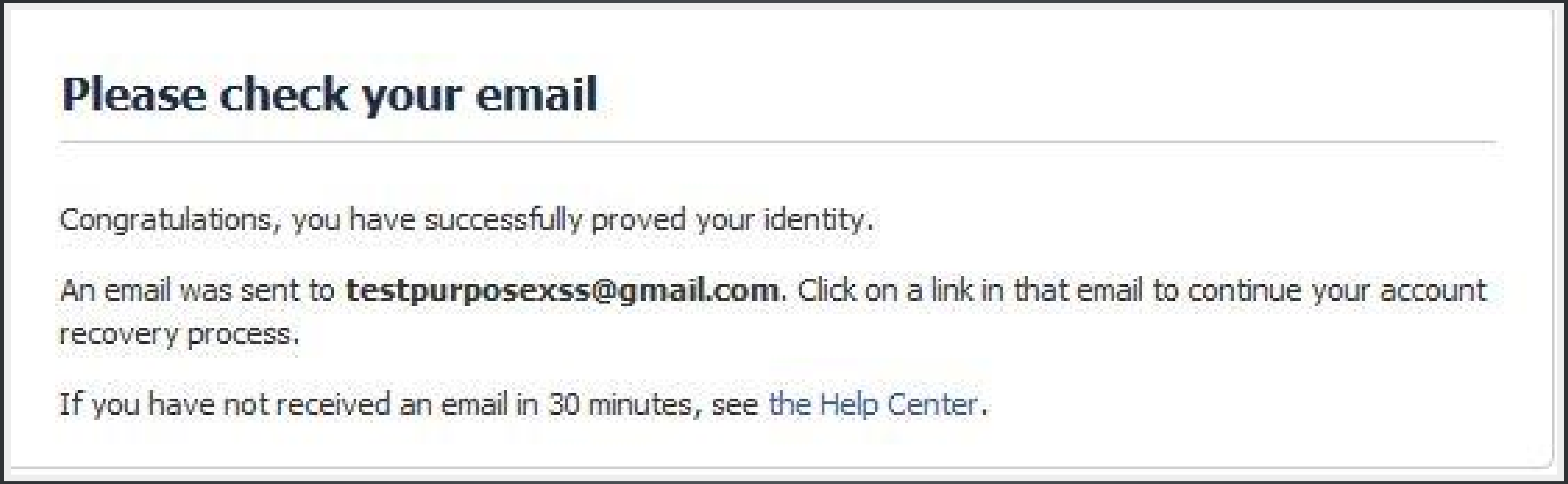
DISAVOW PROCESS

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.

FOR A MOMENT FORGOT DISAVOW



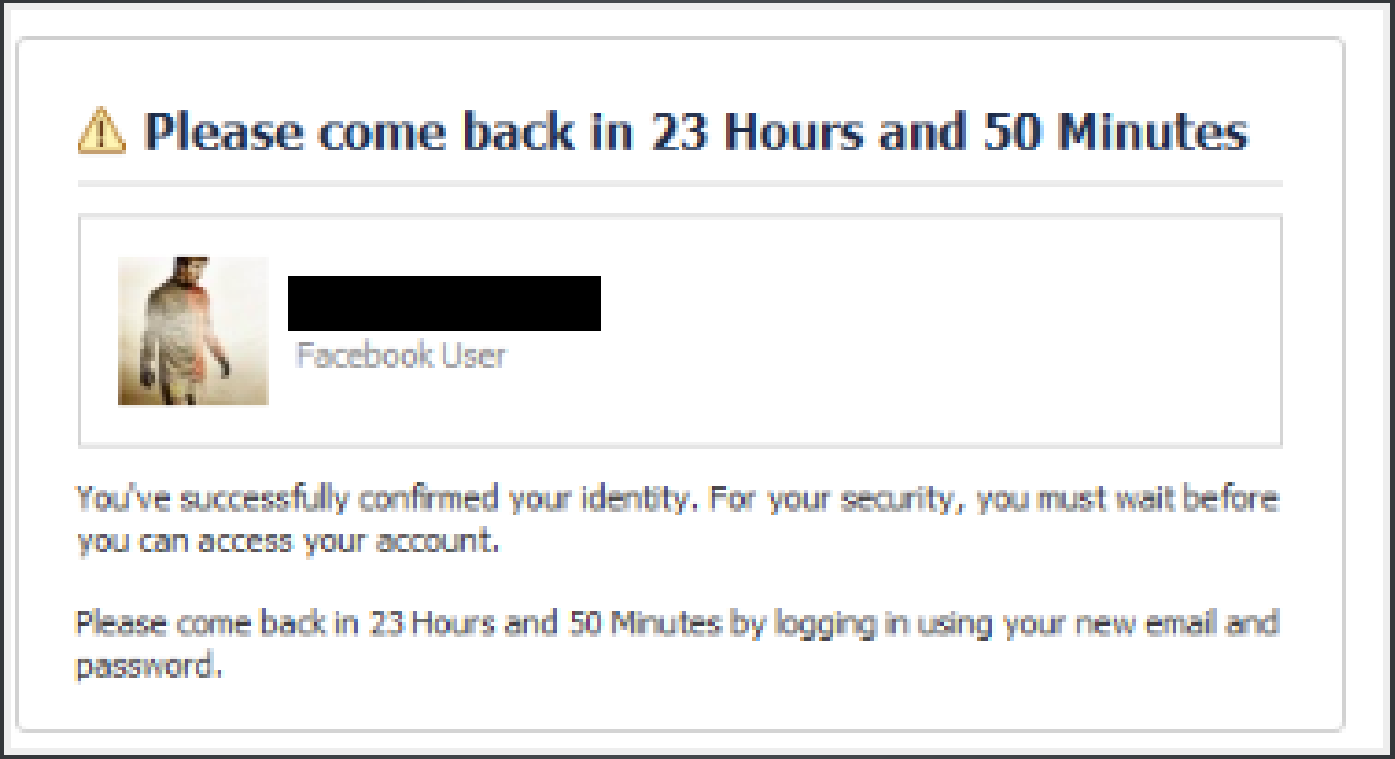
Please check your email

Congratulations, you have successfully proved your identity.

An email was sent to **testpurposexss@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 ...



⚠ Please come back in 23 Hours and 50 Minutes

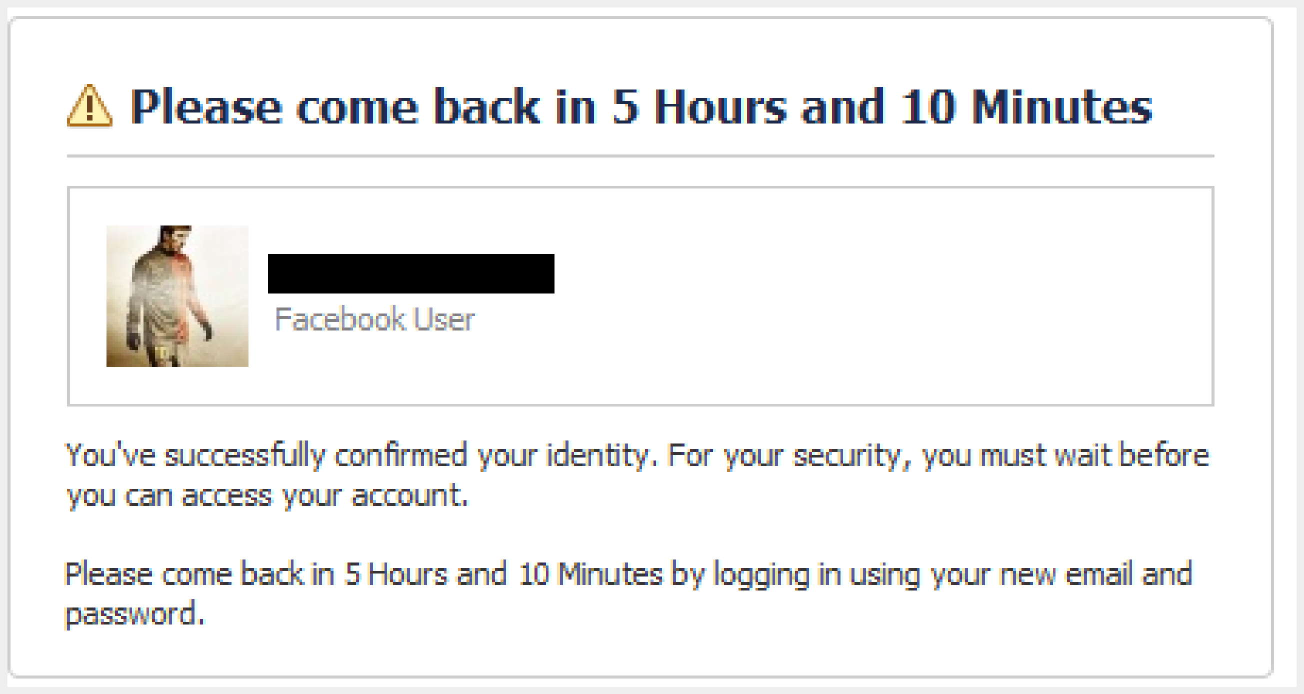
[redacted]

Facebook User

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

Please come back in 23 Hours and 50 Minutes by logging in using your new email and password.

24 HOUR LOCKED OUT PERIOD ...



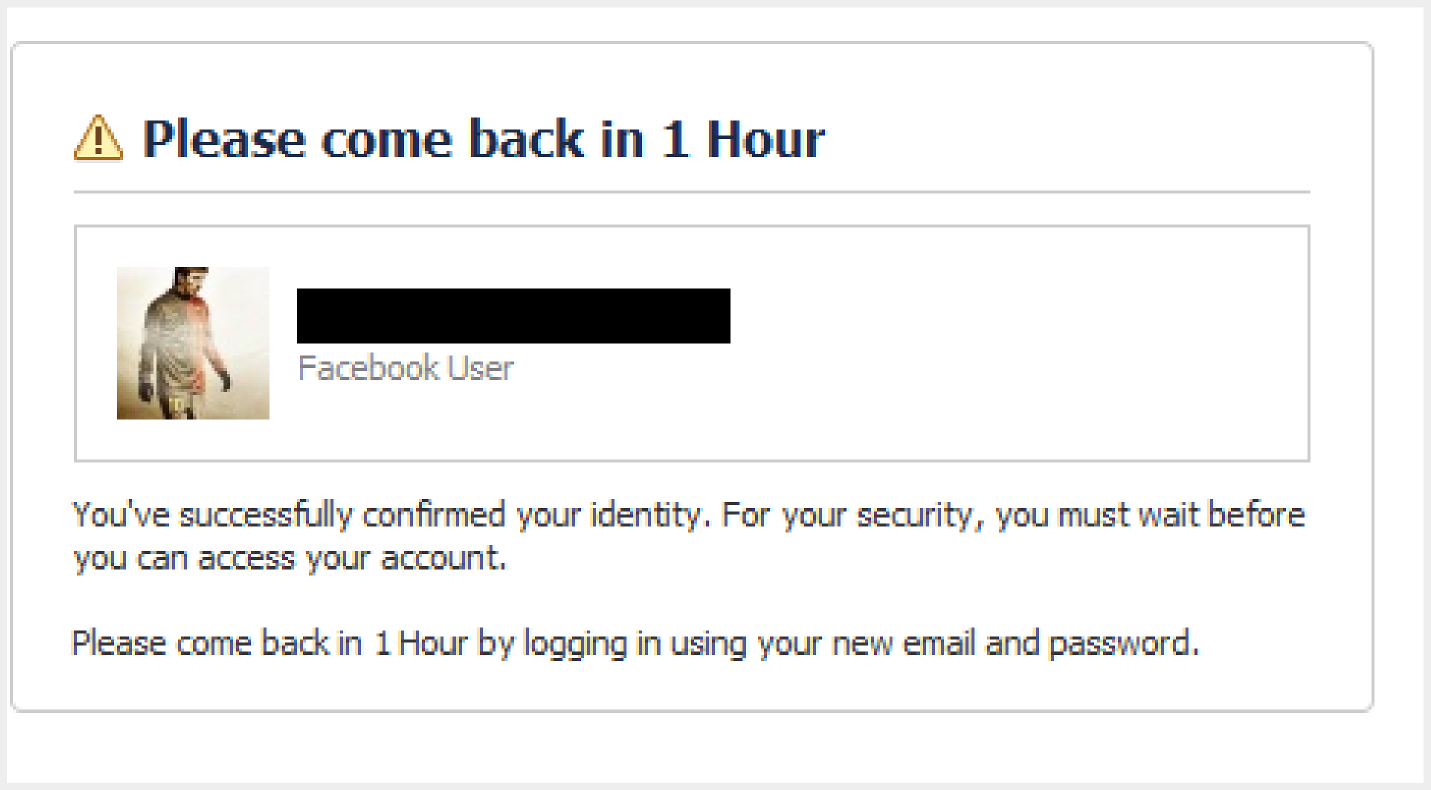
⚠ Please come back in 5 Hours and 10 Minutes

[redacted]
Facebook User

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 ...



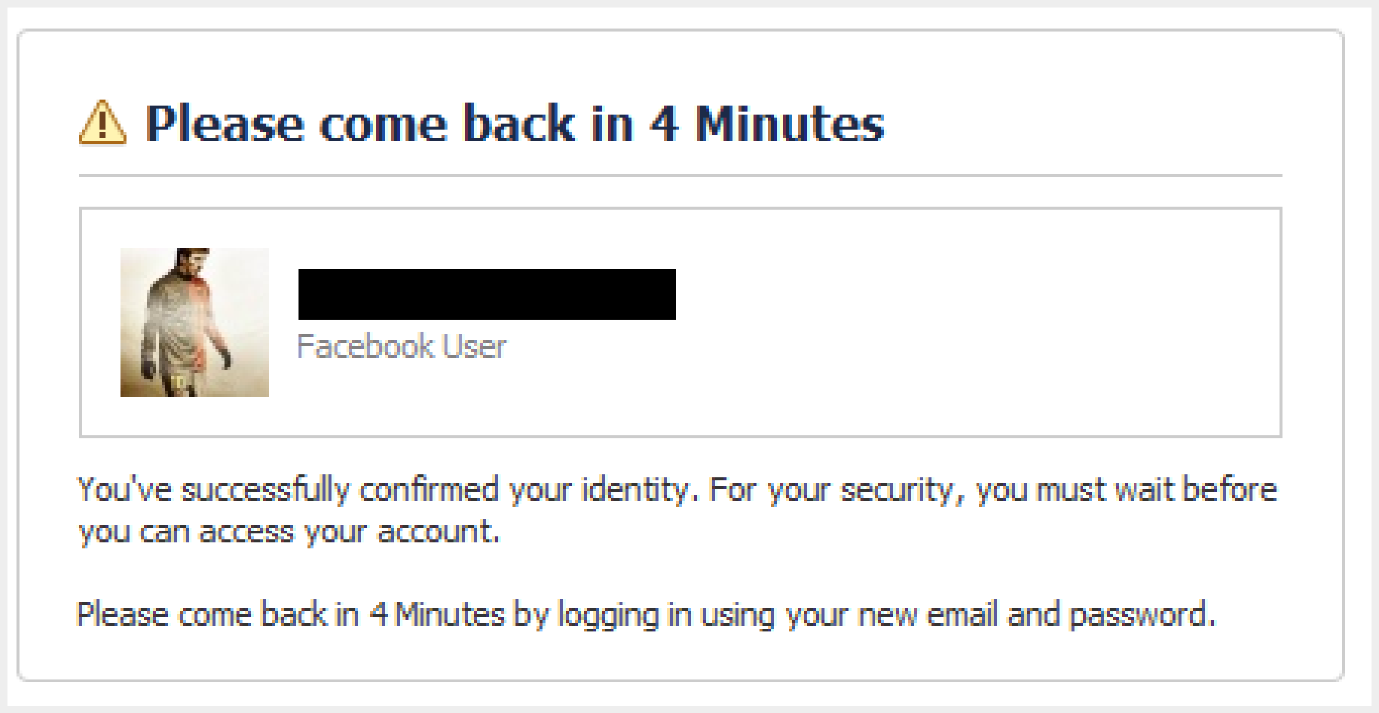
⚠ Please come back in 1 Hour

[redacted]
Facebook User

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 ...



⚠ Please come back in 4 Minutes

[redacted]

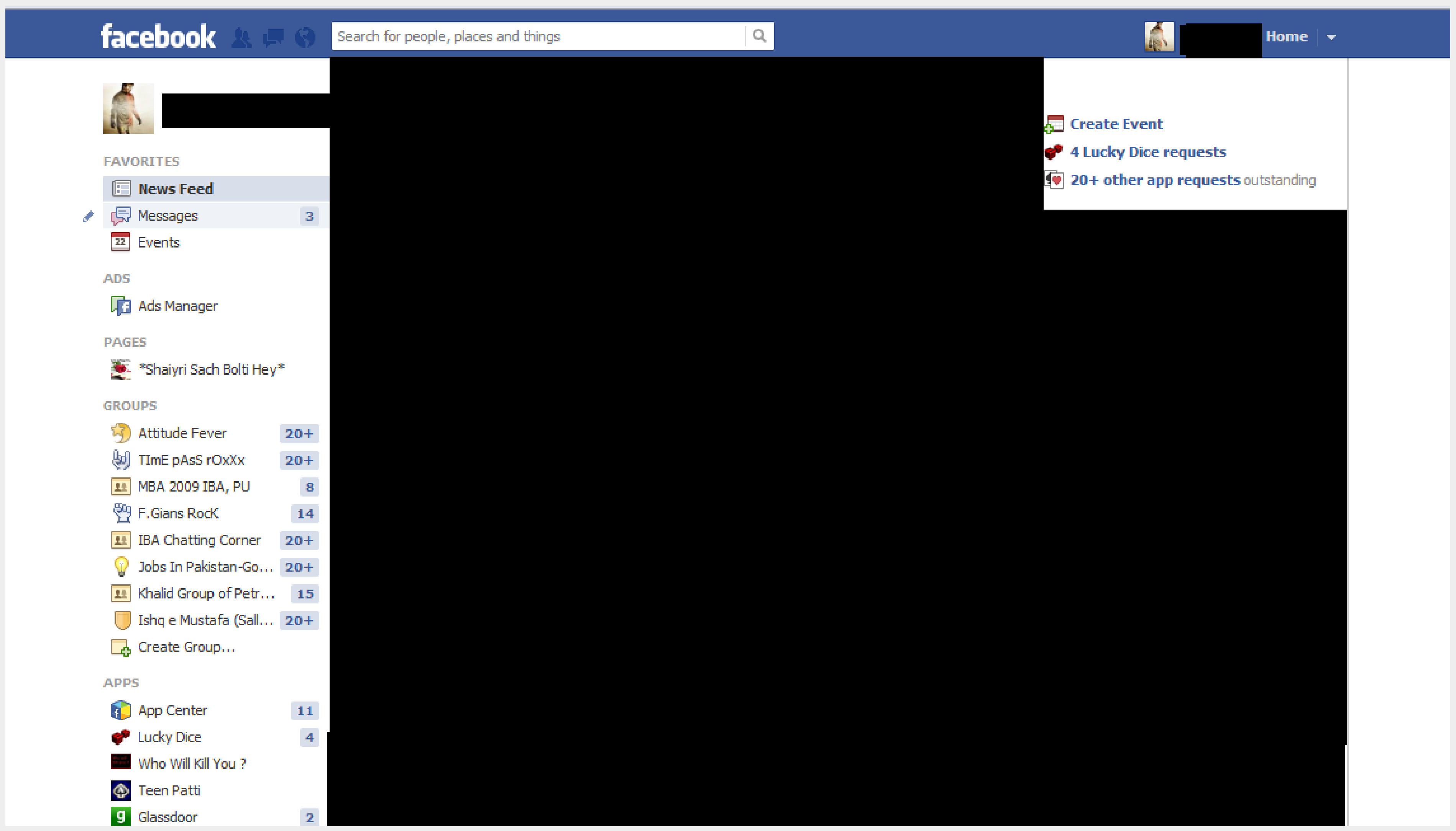
Facebook User

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

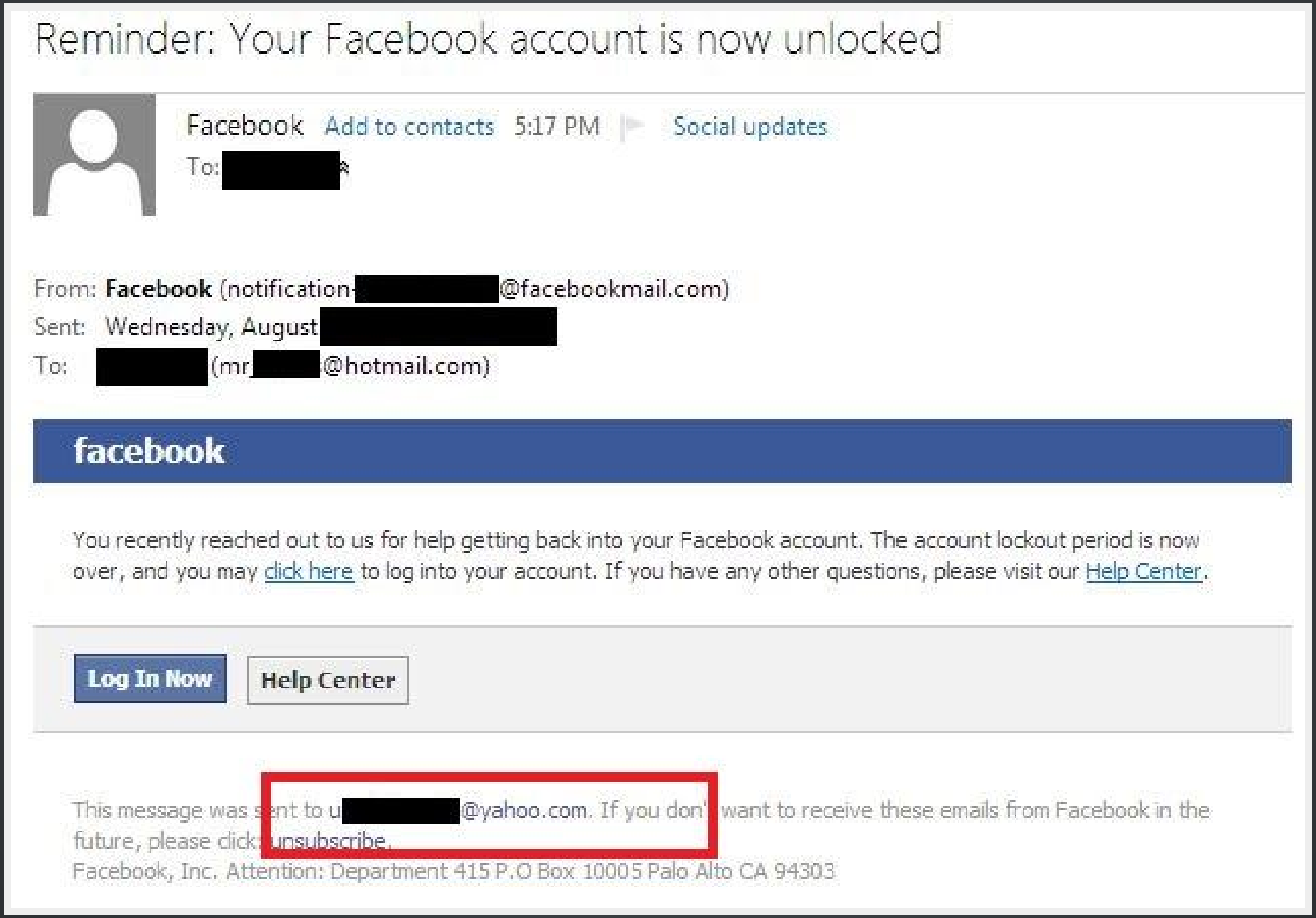
Please come back in 4 Minutes by logging in using your new email and password.

GAME OVER FOR VICTIM...

HERE WE GO...


facebook
Search for people, places and things
[redacted]
Home
[redacted]
[redacted]
Create Event
4 Lucky Dice requests
20+ other app requests outstanding
FAVORITES
News Feed
Messages 3
Events
ADS
Ads Manager
PAGES
Shaiyri Sach Bolti Hey
GROUPS
Attitude Fever 20+
TImE pAsS rOxXx 20+
MBA 2009 IBA, PU 8
F.Gians RocK 14
IBA Chatting Corner 20+
Jobs In Pakistan-Go... 20+
Khalid Group of Petr... 15
Ishq e Mustafa (Sall... 20+
Create Group...
APPS
App Center 11
Lucky Dice 4
Who Will Kill You ?
Teen Patti
Glassdoor 2

ANOTHER EMAIL FROM FACEBOOK AND LEAKED EMAIL ADDRESS OF THE VICTIM



Reminder: Your Facebook account is now unlocked

Facebook Add to contacts 5:17 PM Social updates

To: [redacted]

From: **Facebook** (notification-[redacted]@facebookmail.com)

Sent: Wednesday, August [redacted]

To: [redacted] (mr_[redacted]@hotmail.com)

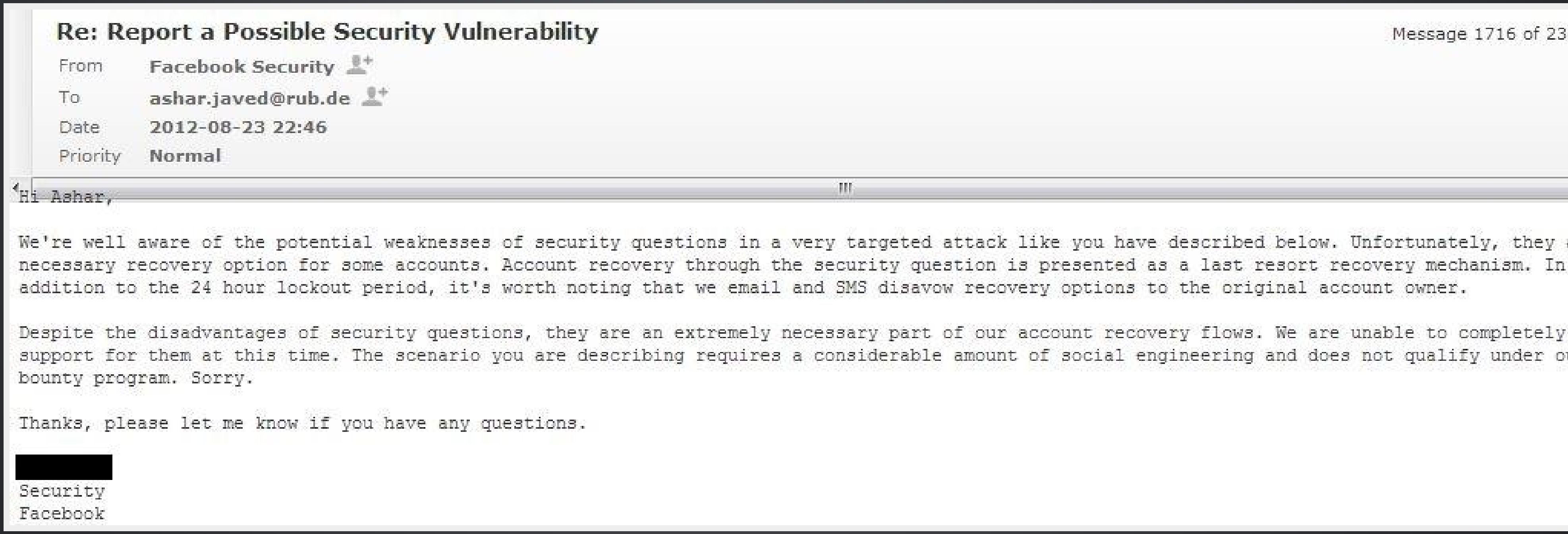
You recently reached out to us for help getting back into your Facebook account. The account lockout period is now over, and you may click here to log into your account. If you have any other questions, please visit our Help Center.

This message was sent to u[redacted]@yahoo.com. If you don't want to receive these emails from Facebook in the future, please click: unsubscribe.

Facebook, Inc. Attention: Department 415 P.O Box 10005 Palo Alto CA 94303

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

Message 1716 of 23

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 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 lockout period, it's worth noting that we email and SMS disavow 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 o bounty program. Sorry.

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

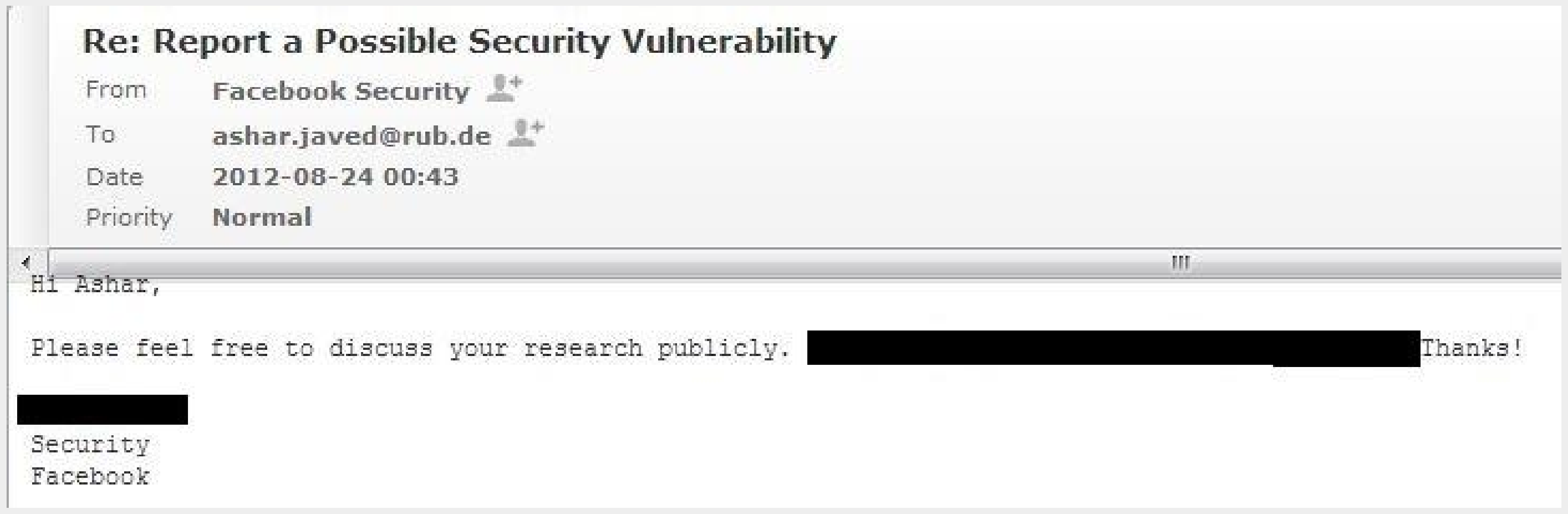
[redacted]
Security
Facebook

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?

ON 24-08-2012



Re: Report a Possible Security Vulnerability

From Facebook Security

To ashar.javed@rub.de

Date 2012-08-24 00:43

Priority Normal

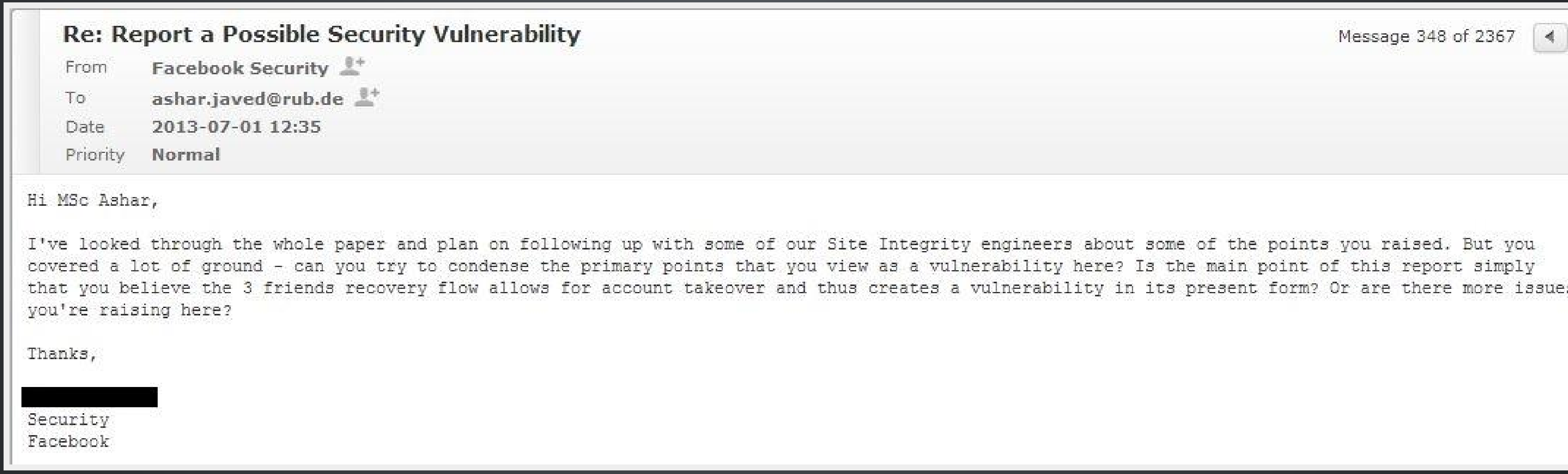
Hi Ashar,

Please feel free to discuss your research publicly. [redacted] Thanks!

[redacted]

Security
Facebook

BUT I HAVE WAITED UNTIL THE COMPLETE EMPIRICAL STUDY & AGAIN SENT THE TECHNICAL REPORT/RESEARCH PAPER ON 27-06-2013



Re: Report a Possible Security Vulnerability

Message 348 of 2367

From Facebook Security

To ashar.javed@rub.de

Date 2013-07-01 12:35

Priority Normal

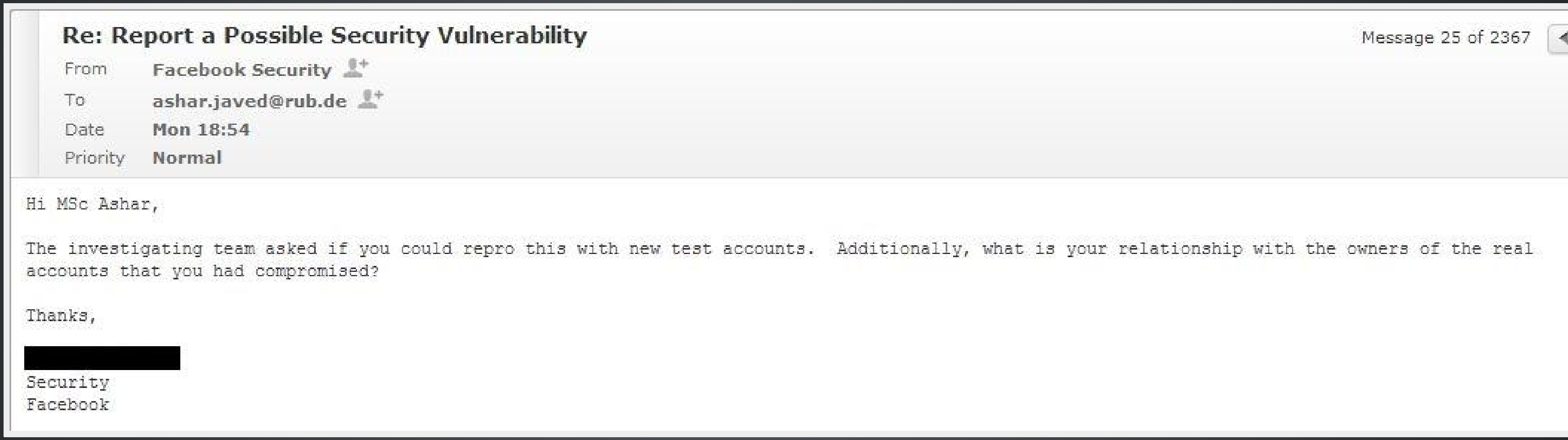
Hi MSc Ashar,

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 issue you're raising here?

Thanks,

[redacted]
Security
Facebook

ANSWER FROM SECURITY TEAM ON 09-09-2013



Re: Report a Possible Security Vulnerability

Message 25 of 2367

From Facebook Security

To ashar.javed@rub.de

Date Mon 18:54

Priority Normal

Hi MSc Ashar,

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,

[redacted]
Security
Facebook

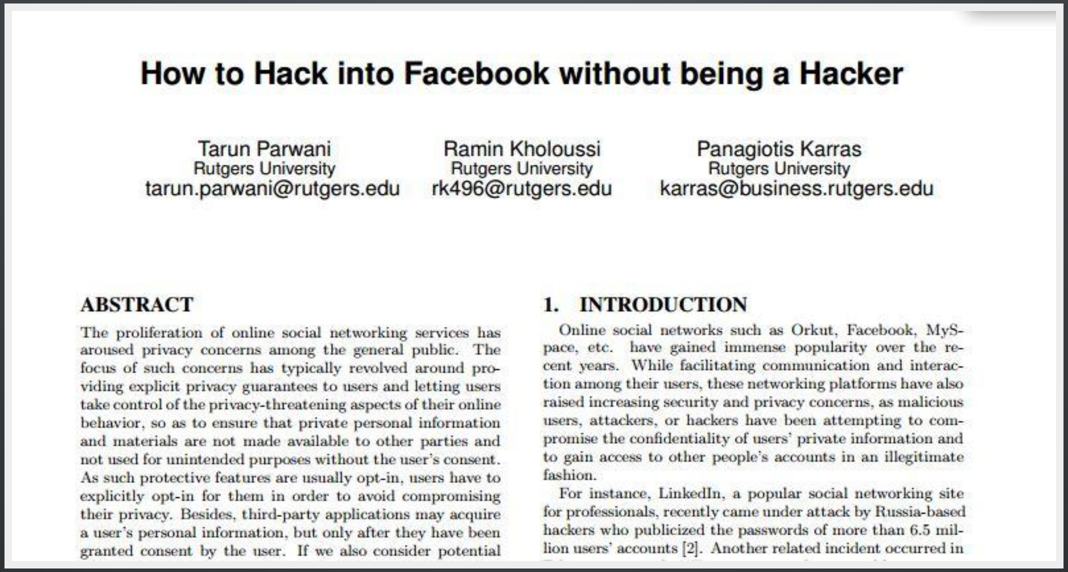
SORRY FACEBOOK :-(

It doesn't makes 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)



How to Hack into Facebook without being a Hacker

Tarun Parwani
Rutgers University
tarun.parwani@rutgers.edu

Ramin Kholoussi
Rutgers University
rk496@rutgers.edu

Panagiotis Karras
Rutgers University
karras@business.rutgers.edu

ABSTRACT

The proliferation of online social networking services has aroused privacy concerns among the general public. The focus of such concerns has typically revolved around providing explicit privacy guarantees to users and letting users take control of the privacy-threatening aspects of their online behavior, so as to ensure that private personal information and materials are not made available to other parties and not used for unintended purposes without the user's consent. As such protective features are usually opt-in, users have to explicitly opt-in for them in order to avoid compromising their privacy. Besides, third-party applications may acquire a user's personal information, but only after they have been granted consent by the user. If we also consider potential

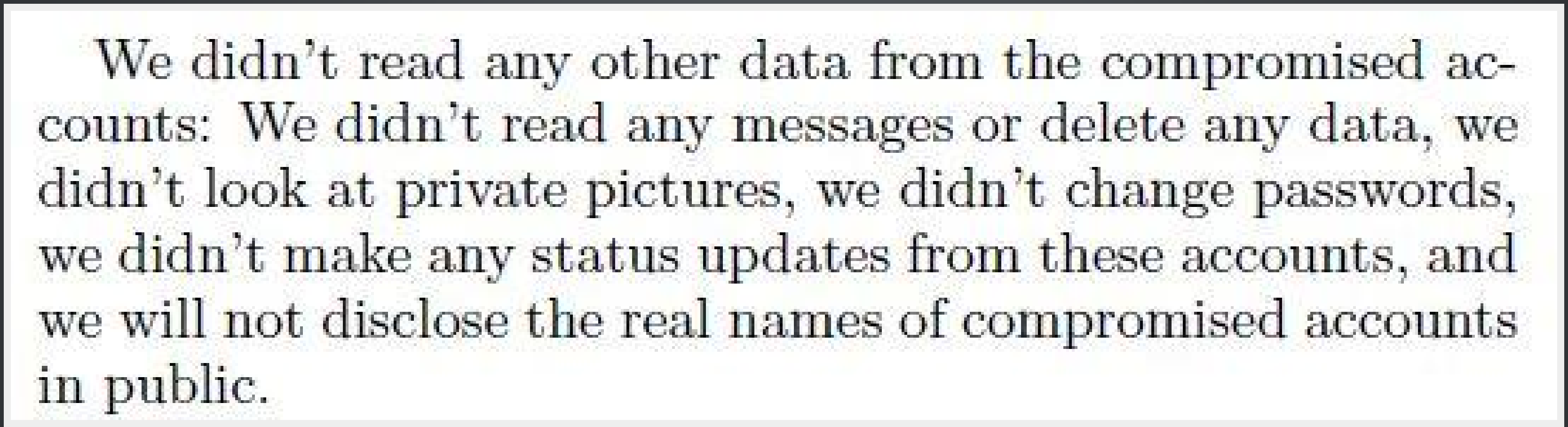
1. INTRODUCTION

Online social networks such as Orkut, Facebook, MySpace, etc. have gained immense popularity over the recent years. While facilitating communication and interaction among their users, these networking platforms have also raised increasing security and privacy concerns, as malicious users, attackers, or hackers have been attempting to compromise the confidentiality of users' private information and to gain access to other people's accounts in an illegitimate fashion.

For instance, LinkedIn, a popular social networking site for professionals, recently came under attack by Russia-based hackers who publicized the passwords of more than 6.5 million users' accounts [2]. Another related incident occurred in

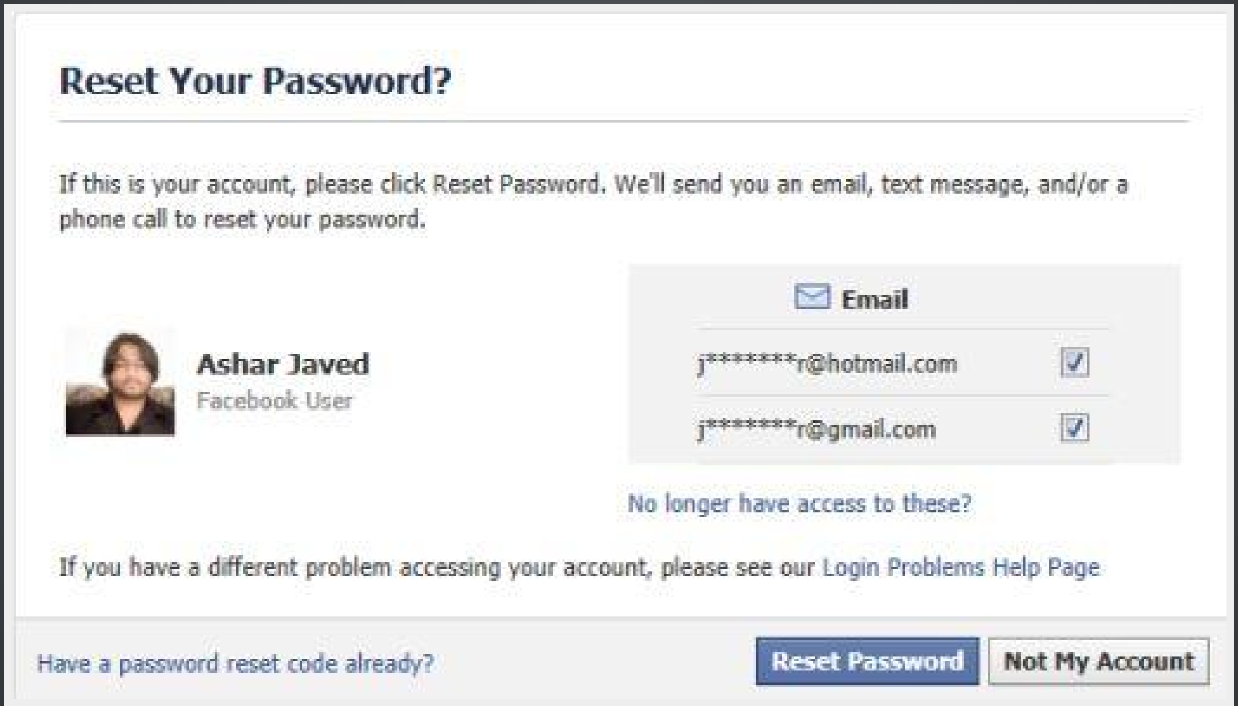
FINALLY

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



Reset Your Password?

If this is your account, please click Reset Password. We'll send you an email, text message, and/or a phone call to reset your password.

Ashar Javed
Facebook User

Email

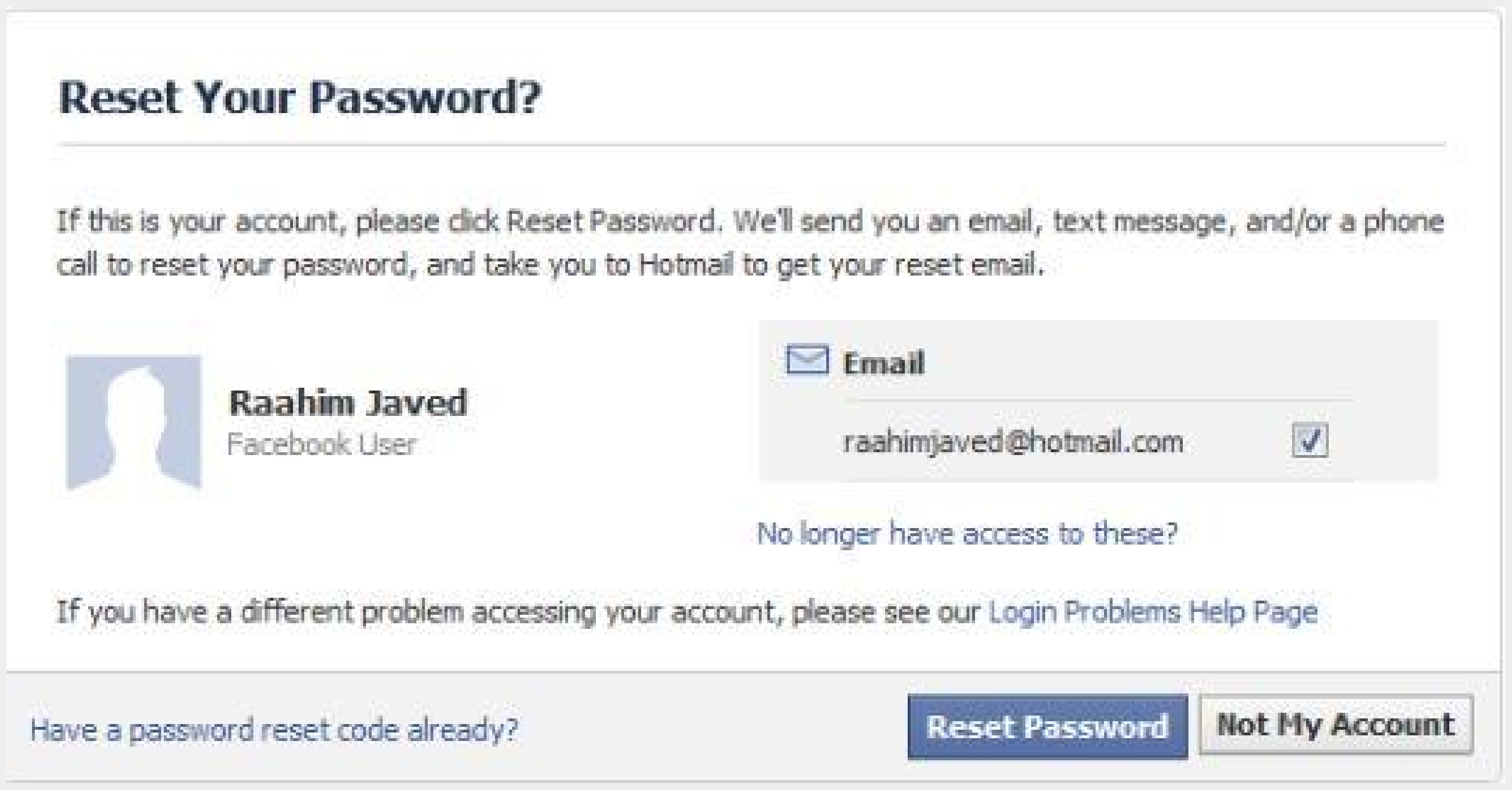
j********r@hotmail.com ☑

j********r@gmail.com ☑

No longer have access to these?

If you have a different problem accessing your account, please see our Login Problems Help Page

WHERE IS MASKING? EMAIL ADDRESS EXPOSED



Reset Your Password?

If this is your account, please click Reset Password. We'll send you an email, text message, and/or a phone call to reset your password, and take you to Hotmail to get your reset email.

Raahim Javed
Facebook User

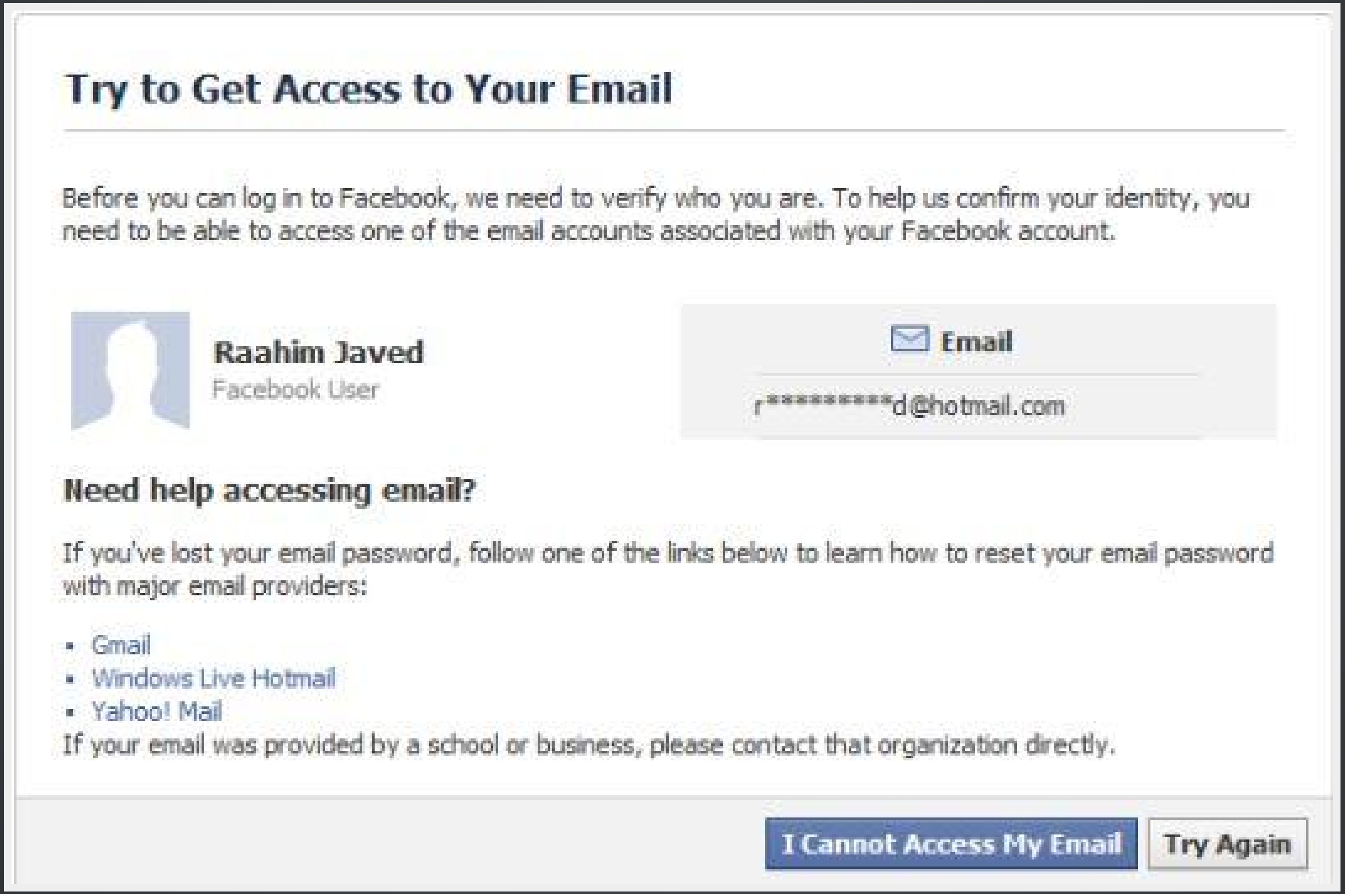
Email

raahimjaved@hotmail.com ☑

No longer have access to these?

If you have a different problem accessing your account, please see our Login Problems Help Page

AFTER 5-10 MINUTES MASKING AFFECT APPEARS



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.

Raahim Javed
Facebook User

Email
r*********d@hotmail.com

Need help accessing email?

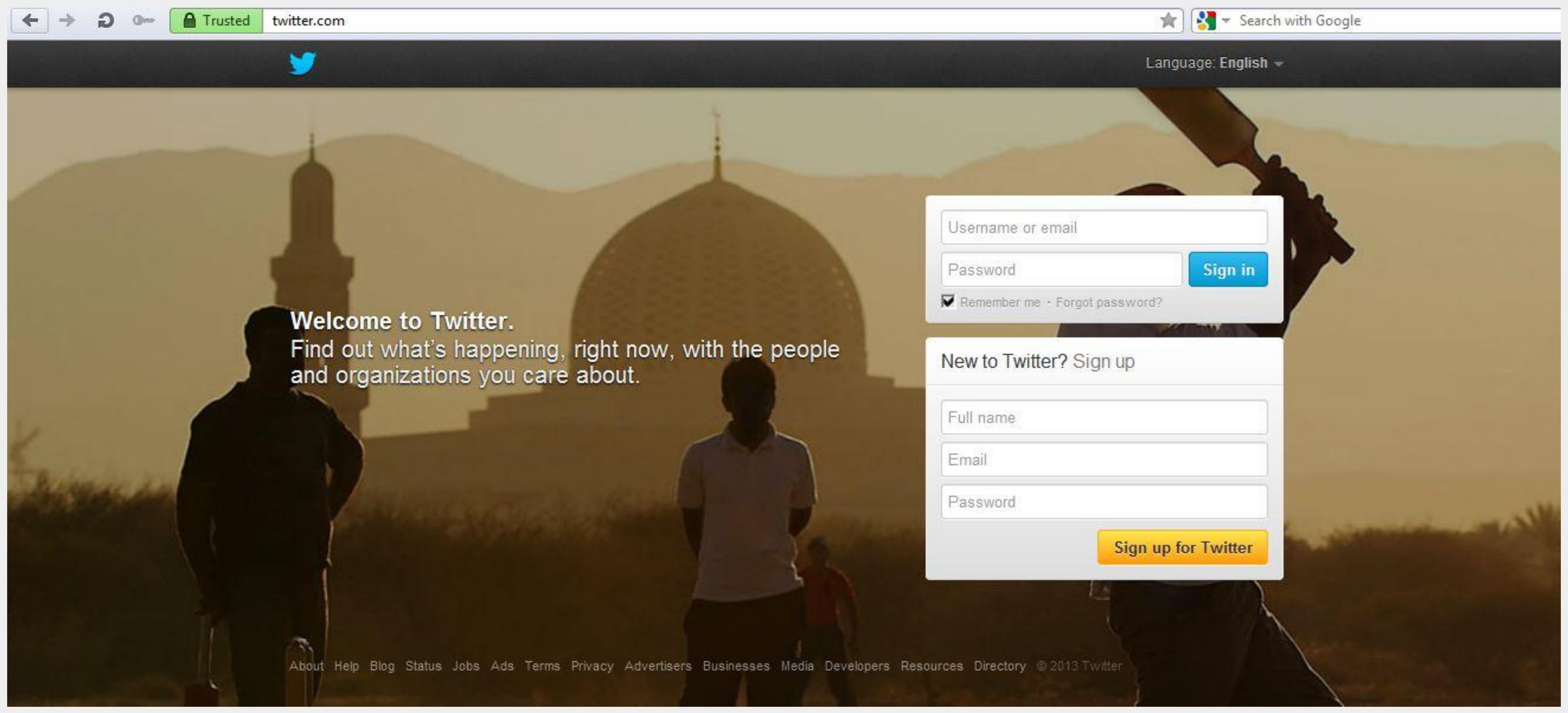
If you've lost your email password, follow one of the links below to learn how to reset your email password with major email providers:

- Gmail
- Windows Live Hotmail
- Yahoo! Mail

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

WHAT ABOUT OTHER 49 SOCIAL NETWORKS' PASSWORD RESET FUNCTIONALITY?

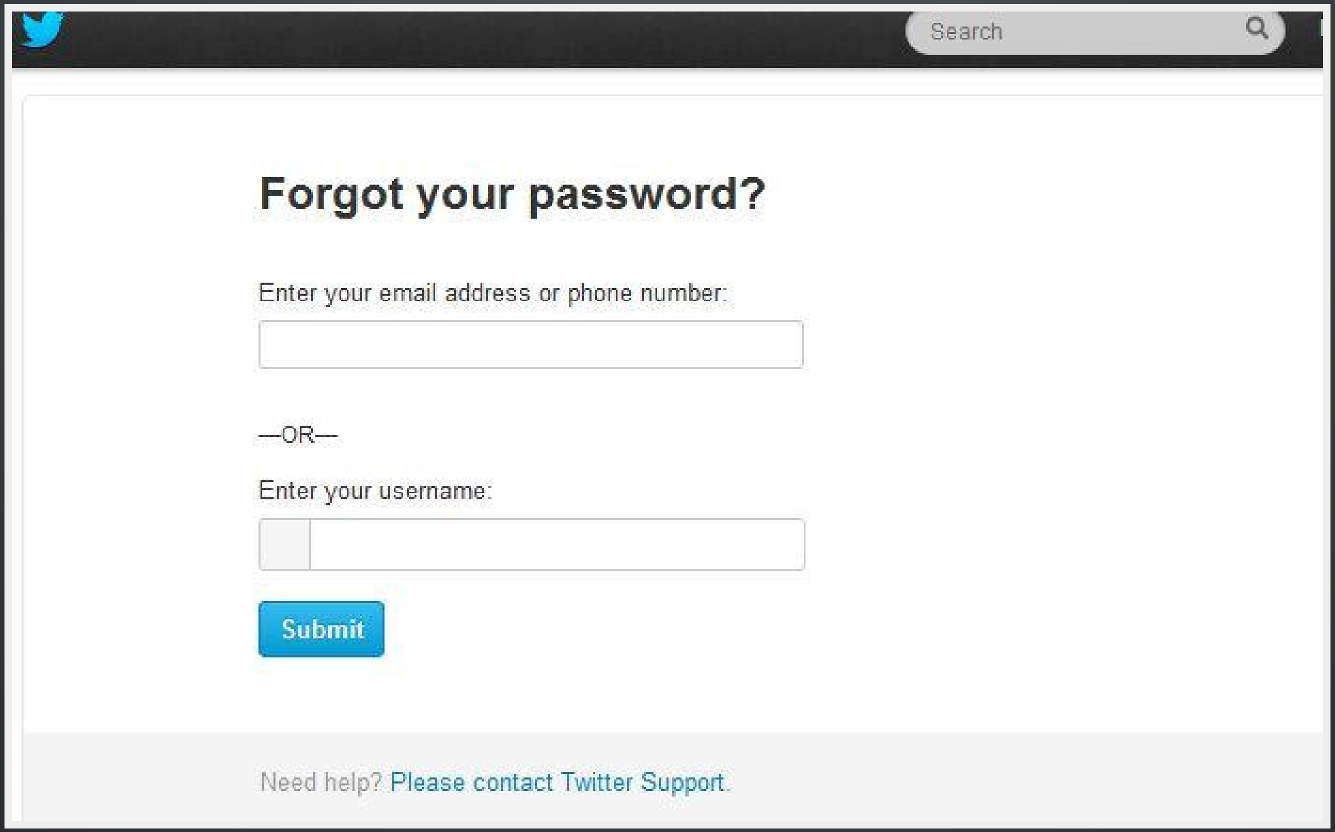
TWITTER (HTTPS://TWITTER.COM/?LANG=EN)


Trusted
twitter.com
Search with Google
Language: English
Username or email
Password
Sign in
Remember me · Forgot password?
New to Twitter? Sign up
Full name
Email
Password
Sign up for Twitter
About Help Blog Status Jobs Ads Terms Privacy Advertisers Businesses Media Developers Resources Directory © 2013 Twitter

Welcome to Twitter.
Find out what's happening, right now, with the people and organizations you care about.

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?

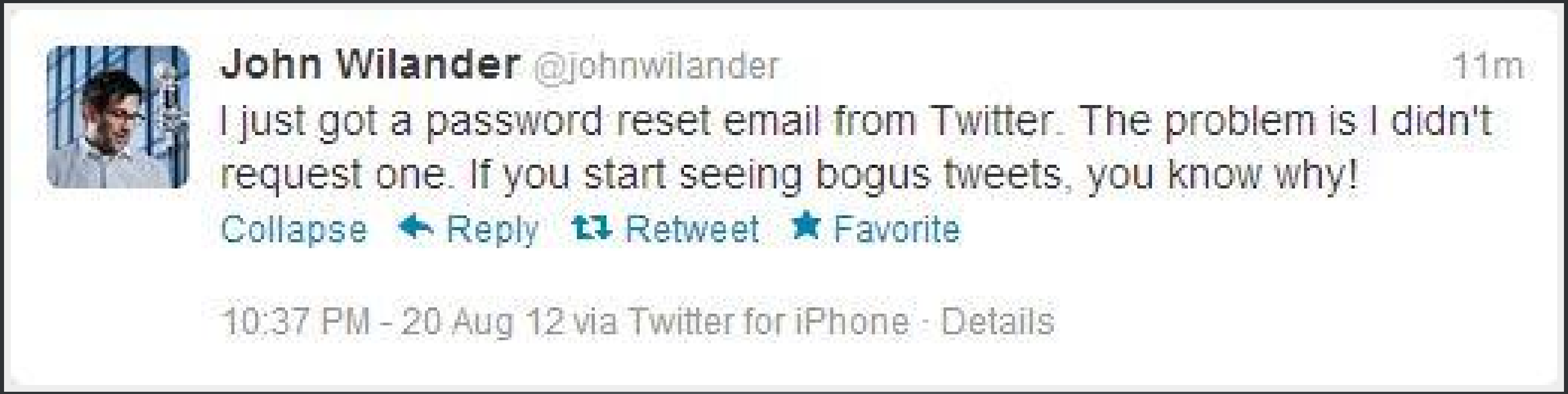
Enter your email address or phone number:

—OR—

Enter your username:

Need help? Please contact Twitter Support.

JUST FOR FUN ...

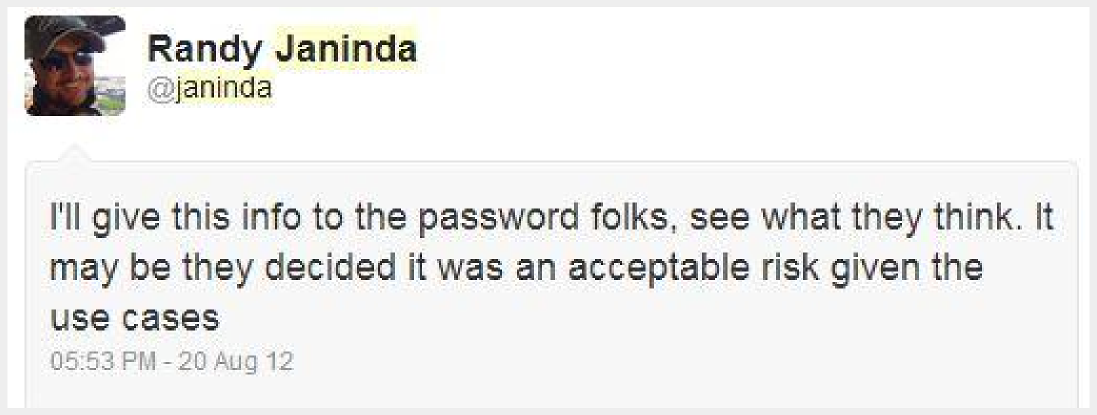


John Wilander @johnwilander 11m

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

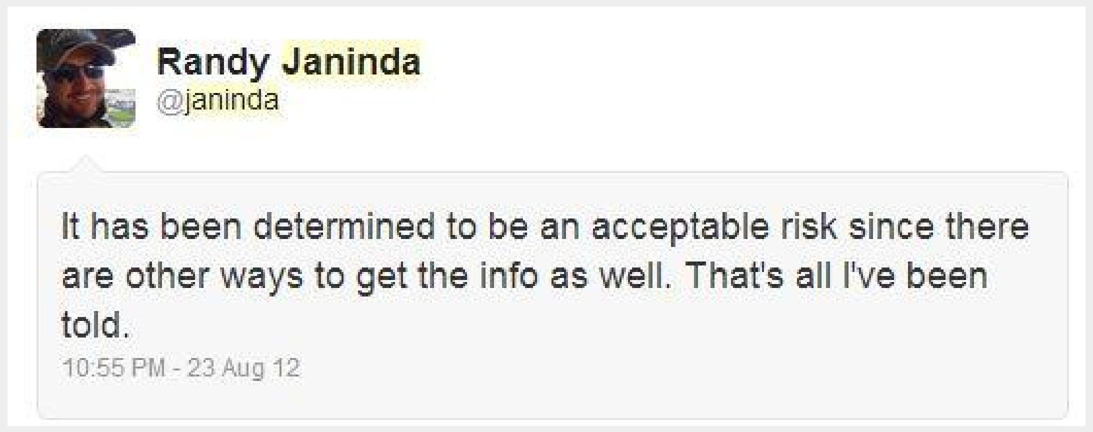
I REPORTED THIS TO TWITTER SECURITY TEAM & THIS IS WHAT THEY THINK ABOUT IT



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

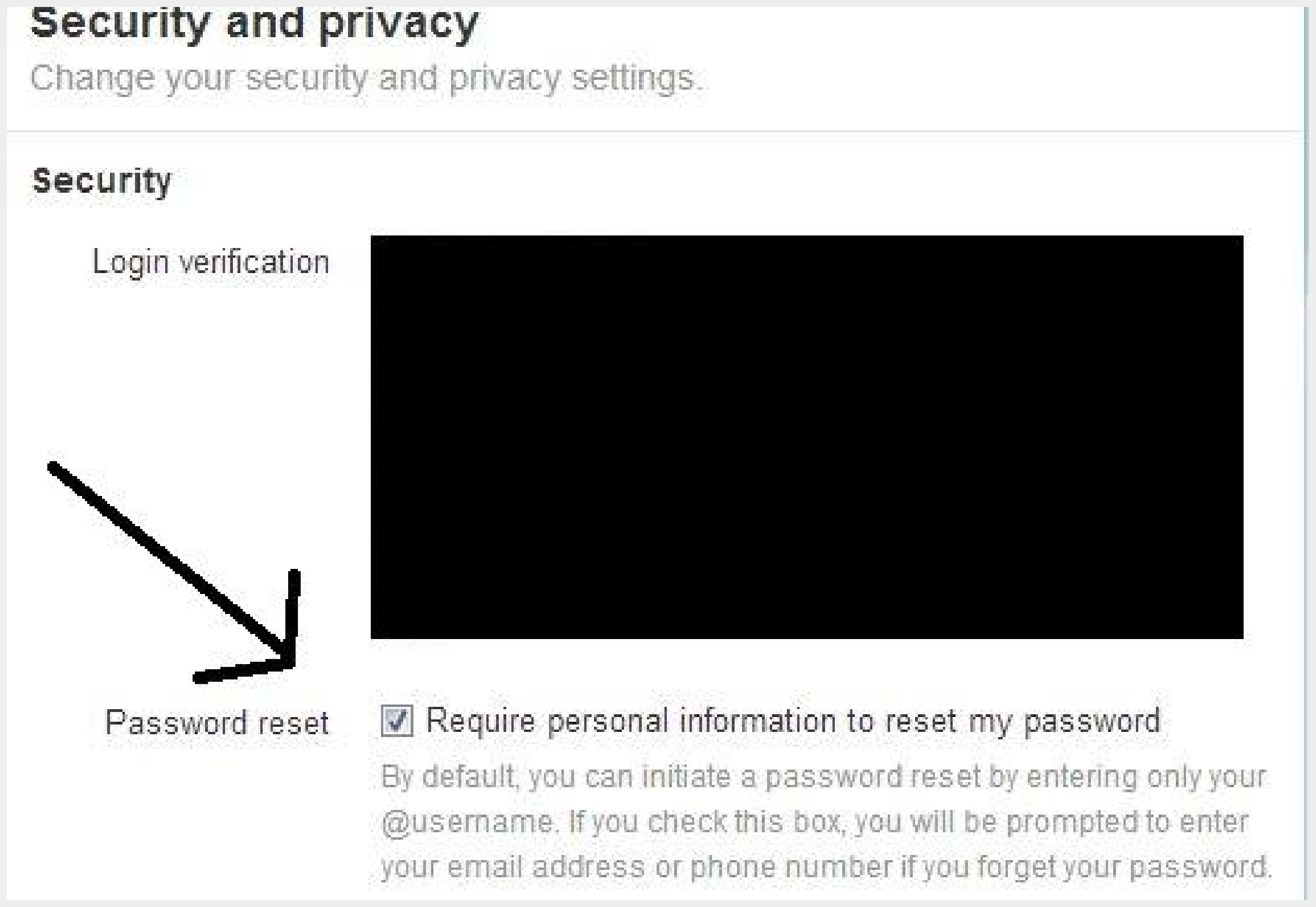


Randy Janinda
@janinda

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

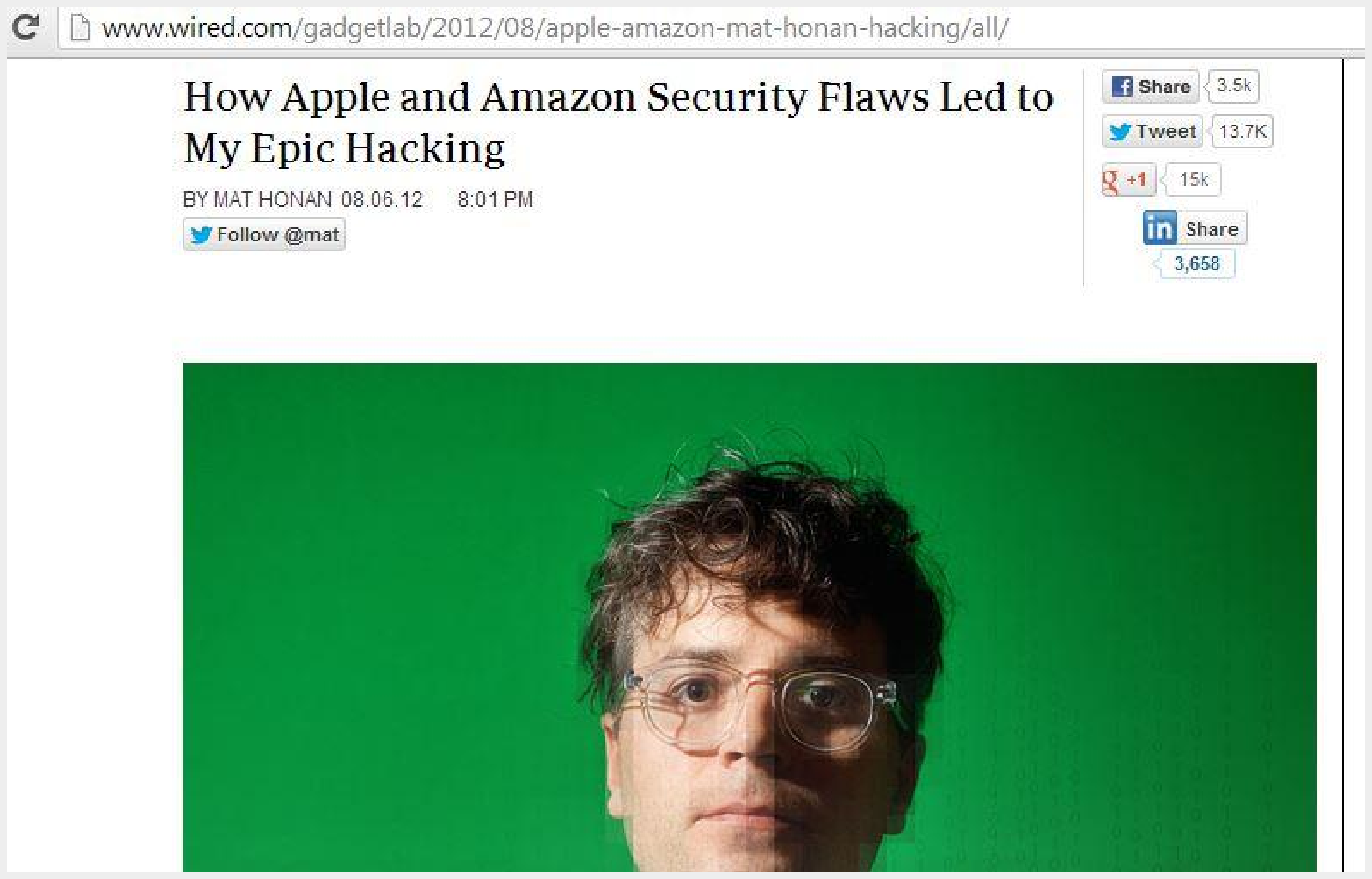
[redacted]

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.

MAT HONAN'S STORY



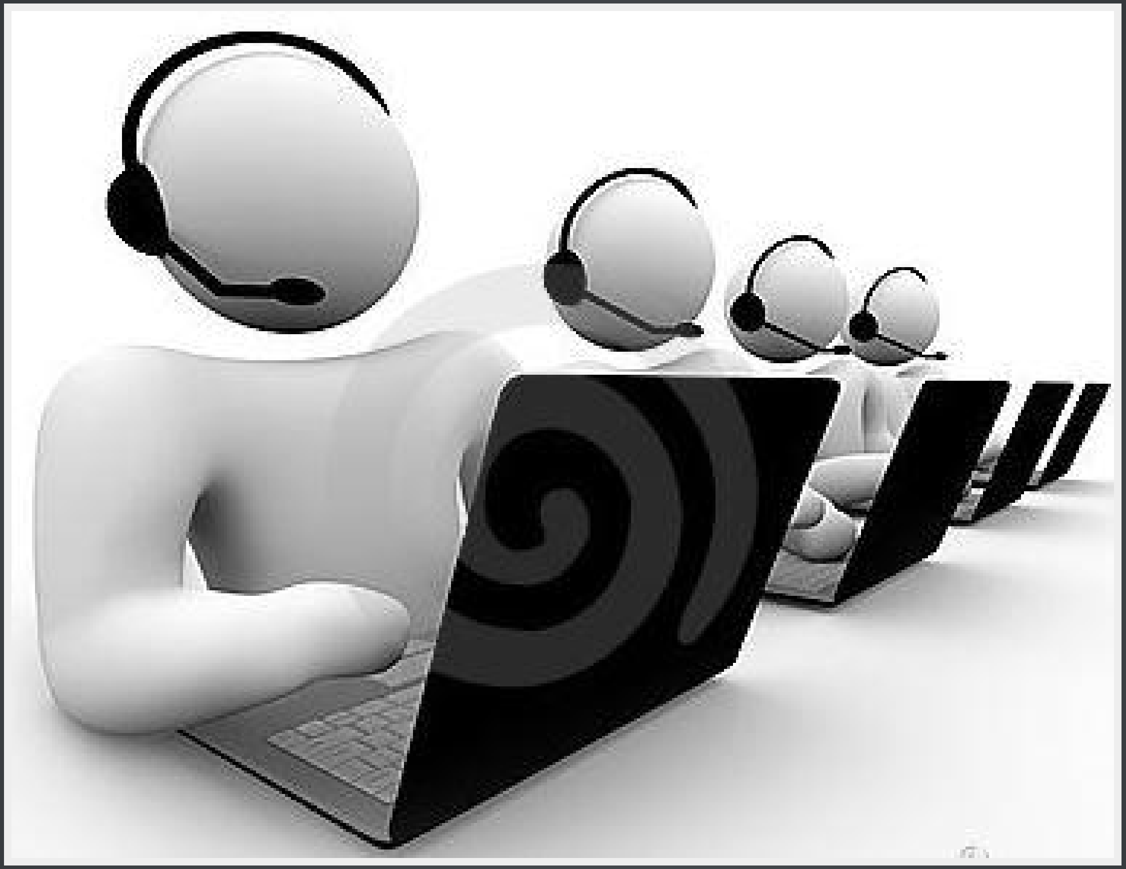
www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking/all/

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

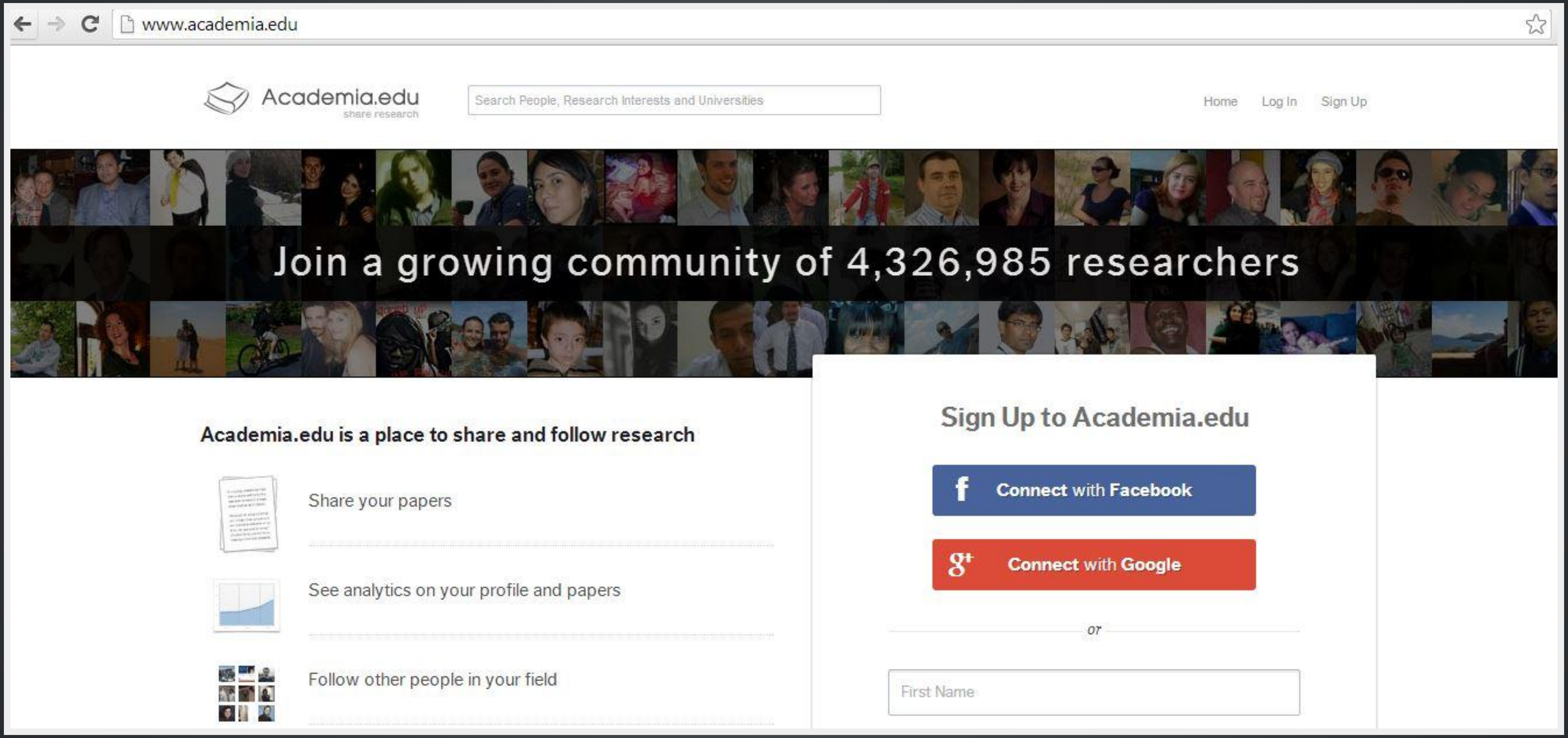
AND

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/)



www.academia.edu

Academia.edu
share research

Search People, Research Interests and Universities

Home Log In Sign Up

Join a growing community of 4,326,985 researchers

Academia.edu is a place to share and follow research

Share your papers

See analytics on your profile and papers

Follow other people in your field

Sign Up to Academia.edu

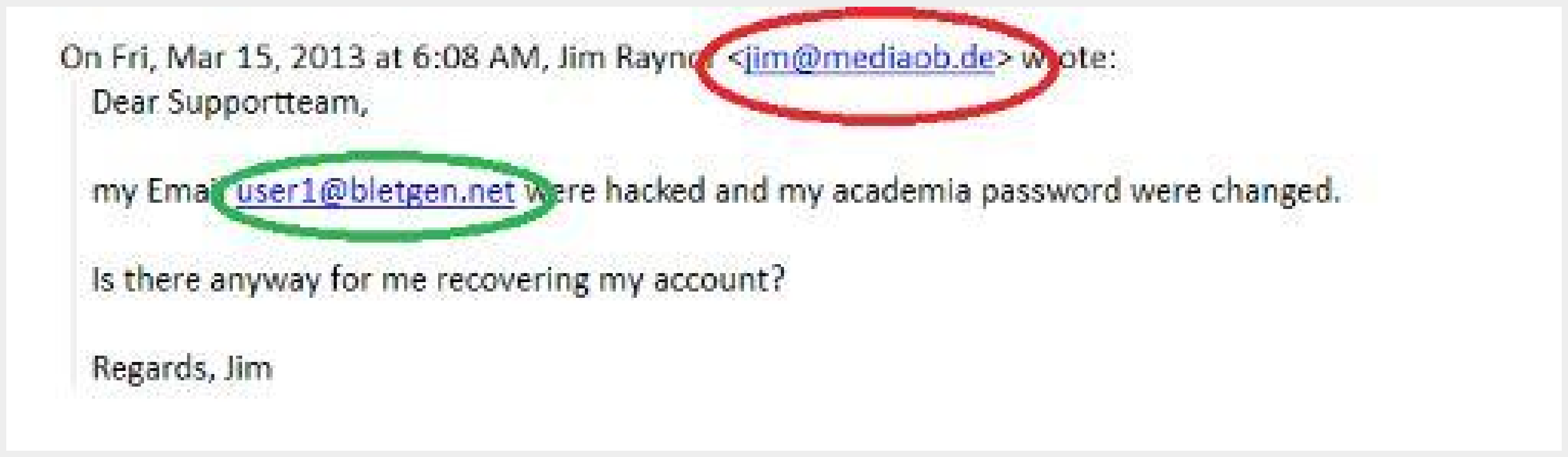
Connect with Facebook

Connect with Google

or

First Name

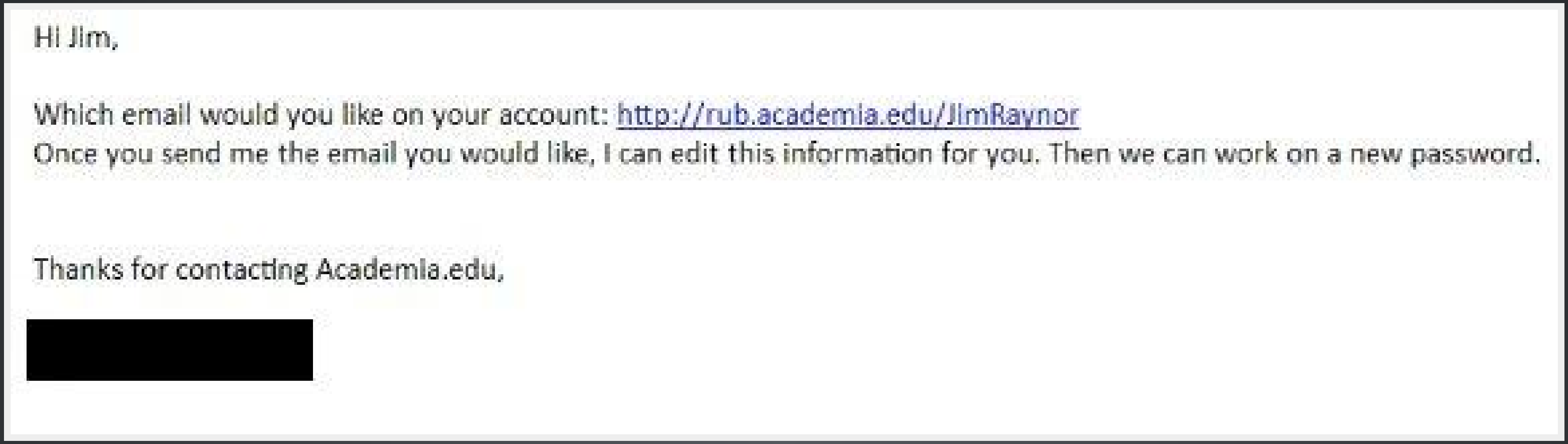
OUR EMAIL TO ACADEMIA



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

INITIAL RESPONSE FROM ACADEMIA



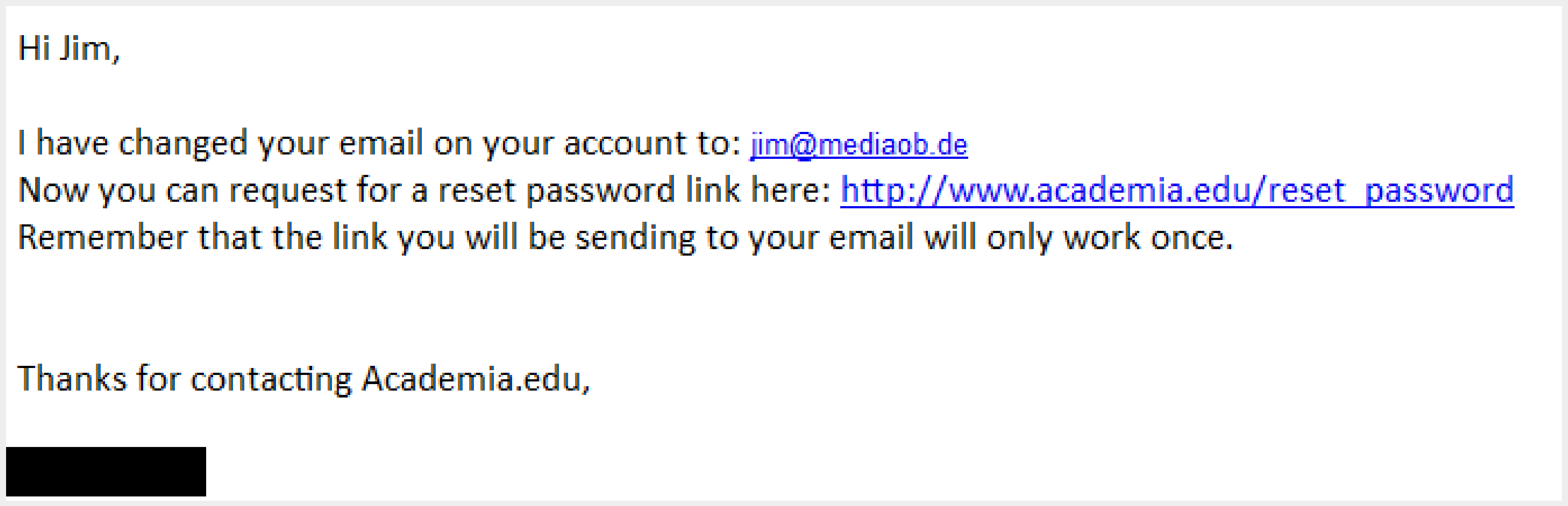
Hi Jim,

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,

[redacted]

FINAL RESPONSE OF ACADEMIA SUPPORT TEAM



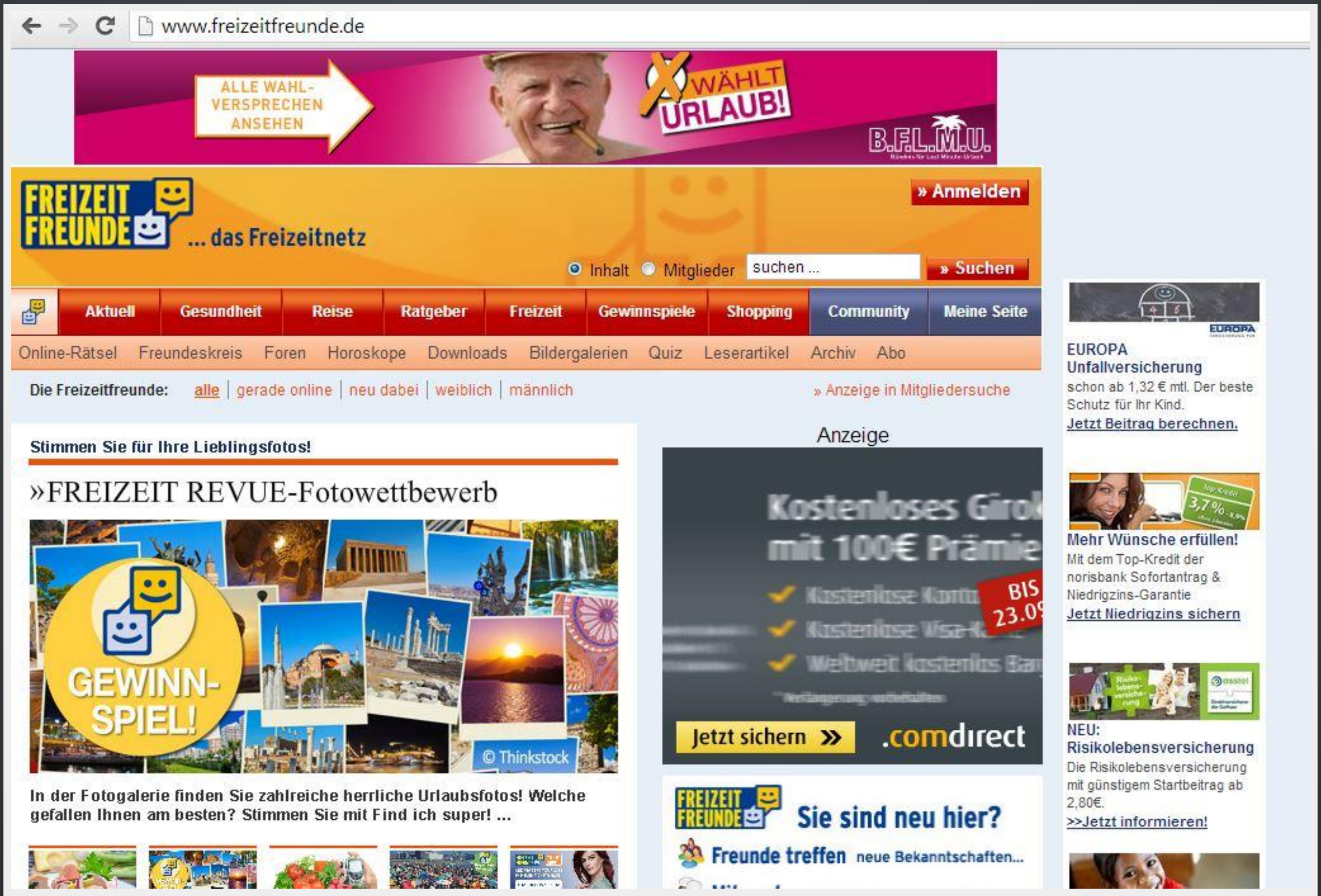
Hi Jim,

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,

[redacted]

FREIZEITFREUNDE (A GERMAN-SPECIFIC SOCIAL NETWORKING SITE) (HTTP://WWW.FREIZEITFREUNDE.DE/)


www.freizeitfreunde.de
ALLE WAHL-VERSPRECHEN ANSEHEN
X WÄHLT URLAUB!
B.F.L.M.U.
FREIZEIT FREUNDE ... das Freizeitnetz
» Anmelden
● Inhalt ○ Mitglieder suchen ... » Suchen
Aktuell Gesundheit Reise Ratgeber Freizeit Gewinnspiele Shopping Community Meine Seite
Online-Rätsel Freundeskreis Foren Horoskope Downloads Bildergalerien Quiz Leserartikel Archiv Abo
Die Freizeitfreunde: alle | gerade online | neu dabei | weiblich | männlich
» Anzeige in Mitgliedersuche
GEWINN-SPIEL!
© Thinkstock
Anzeige
Kostenloses Girok
mit 100€ Prämie
BIS 23.0
Jetzt sichern »
.comdirect
FREIZEIT FREUNDE Sie sind neu hier?
Freunde treffen neue Bekanntschaften...
EUROPA
Top-Kredit 3,7 %
asstel

Stimmen Sie für Ihre Lieblingsfotos!

»FREIZEIT REVUE-Fotowettbewerb

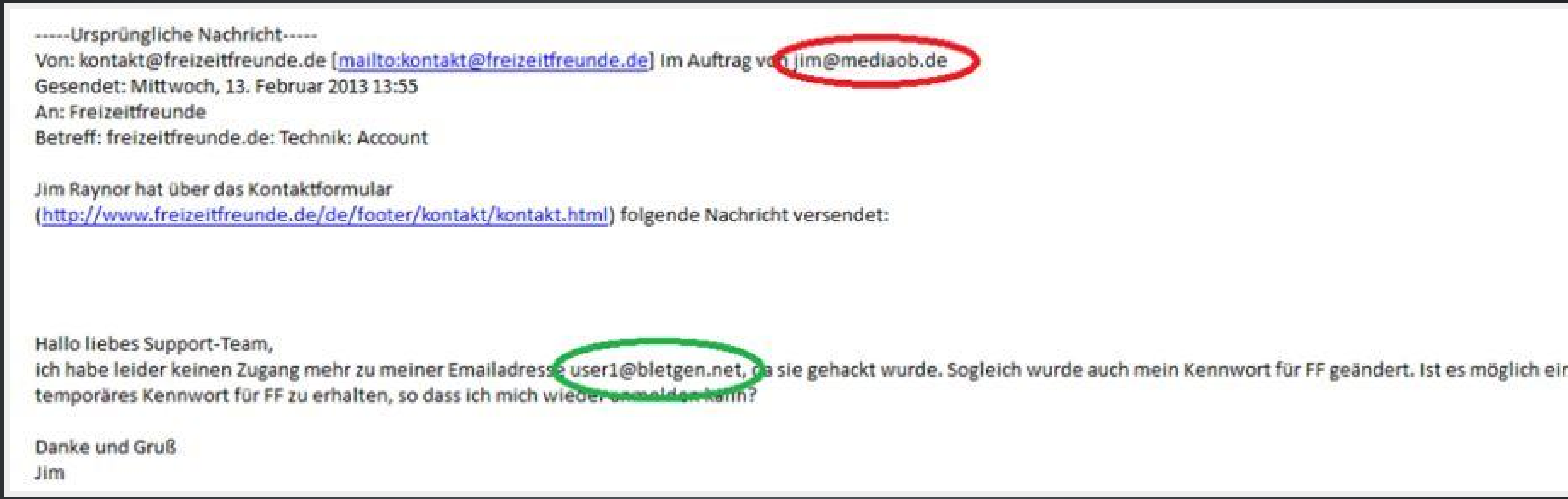
In der Fotogalerie finden Sie zahlreiche herrliche Urlaubsfotos! Welche gefallen Ihnen am besten? Stimmen Sie mit Find ich super! ...

EUROPA Unfallversicherung
schon ab 1,32 € mtl. Der beste Schutz für Ihr Kind.
Jetzt Beitrag berechnen.

Mehr Wünsche erfüllen!
Mit dem Top-Kredit der norisbank Sofortantrag & Niedrigzins-Garantie
Jetzt Niedrigzins sichern

NEU: Risikolebensversicherung
Die Risikolebensversicherung mit günstigem Startbeitrag ab 2,80€.
>>Jetzt informieren!

OUR EMAIL TO THEM ...



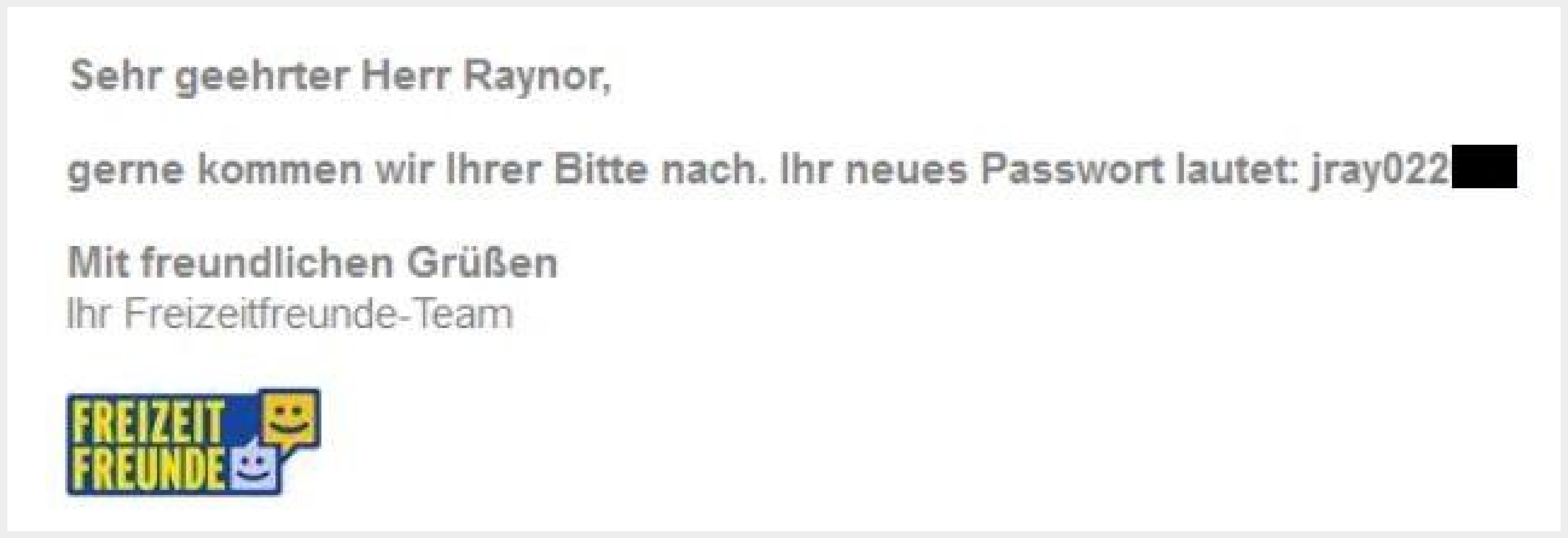
-----Ursprüngliche Nachricht-----
Von: kontakt@freizeitfreunde.de [mailto:kontakt@freizeitfreunde.de] Im Auftrag von jim@mediaob.de
Gesendet: Mittwoch, 13. Februar 2013 13:55
An: Freizeitfreunde
Betreff: freizeitfreunde.de: Technik: Account

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

FREIZEITFREUNDE'S SUPPORT TEAM RESPONSE



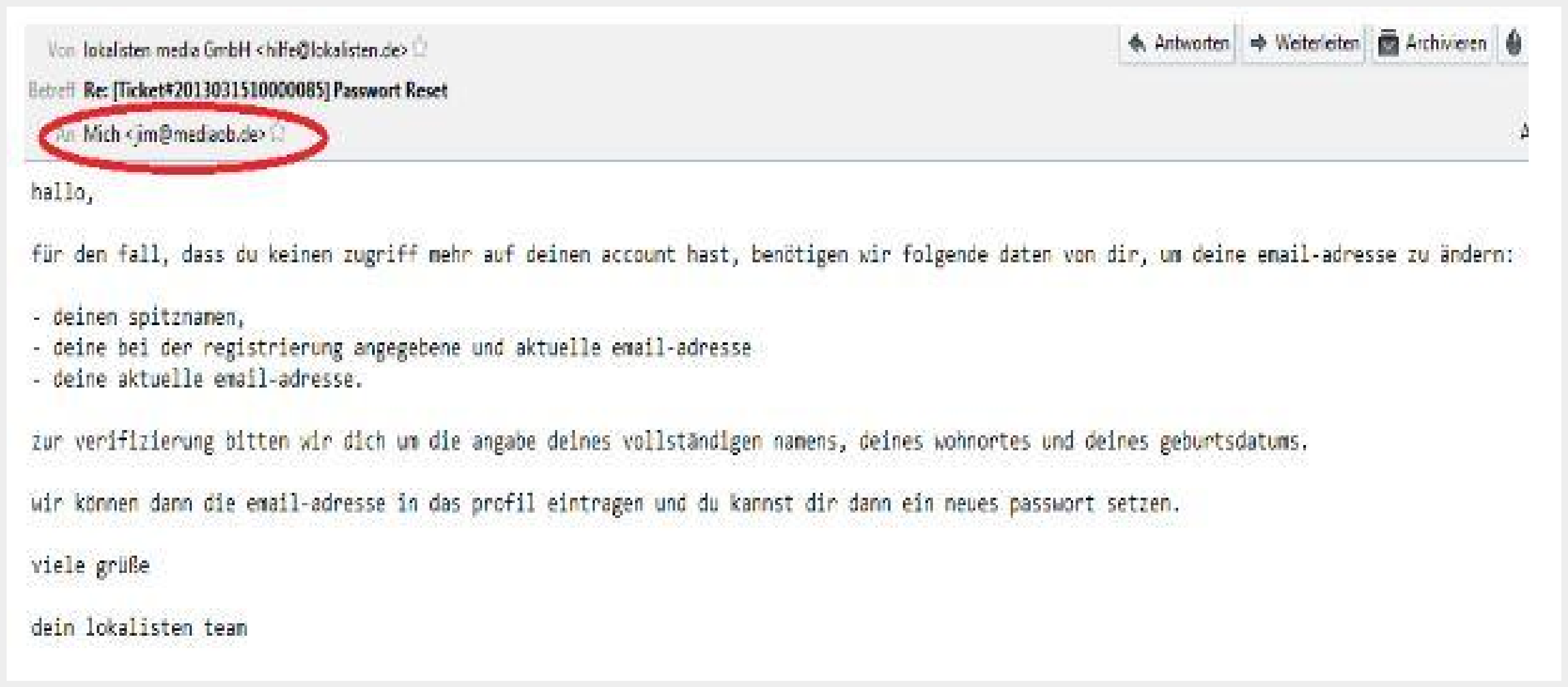
Sehr geehrter Herr Raynor,

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

Mit freundlichen Grüßen
Ihr Freizeitfreunde-Team

LOKALISTEN (A GERMAN SOCIAL NETWORKING SITE) (HTTP://WWW.LOKALISTEN.DE/)

INITIAL RESPONSE ON OUR TICKET



Von: lokalisten media GmbH <hilfe@lokalisten.de>

Betreff: Re: [Ticket#2013031510000085] Passwort Reset

An: Mich <jim@mediacb.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.

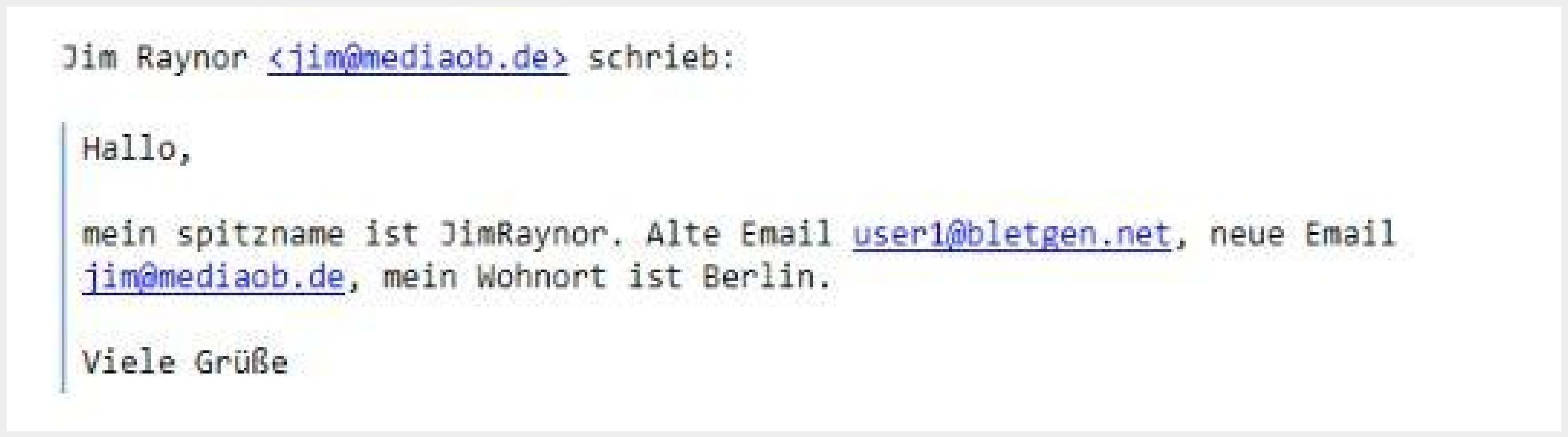
zur verifizierung bitten wir dich um die angabe deines vollständigen namens, deines wohnortes und deines geburtsdatums.

wir können dann die email-adresse in das profil eintragen und du kannst dir dann ein neues passwort setzen.

viele grüße

dein lokalisten team

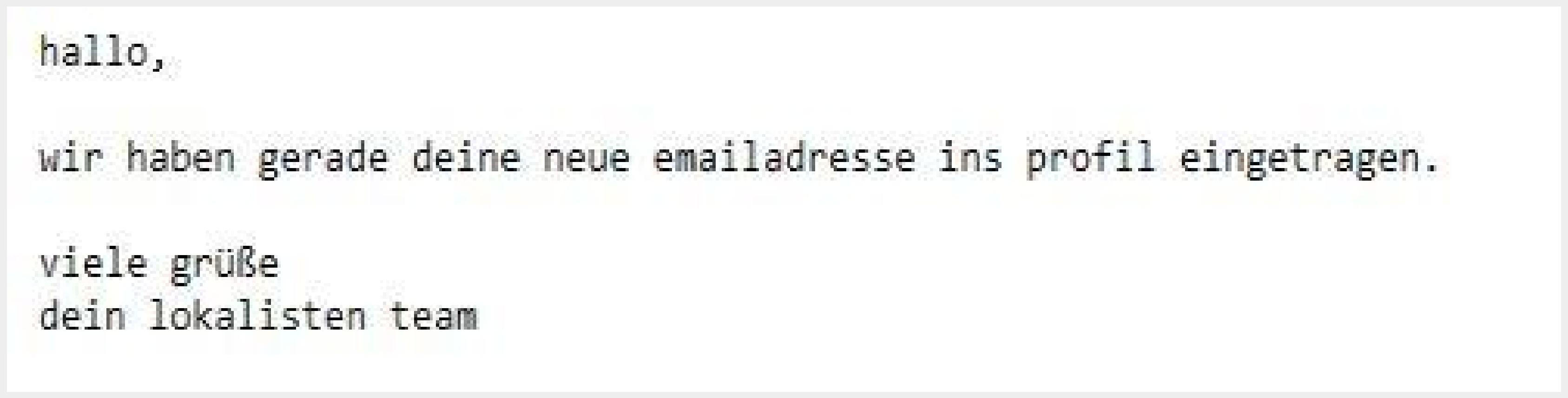
OUR RESPONSE WITHOUT "DATE OF BIRTH"



Jim Raynor <jim@mediaob.de> schrieb:

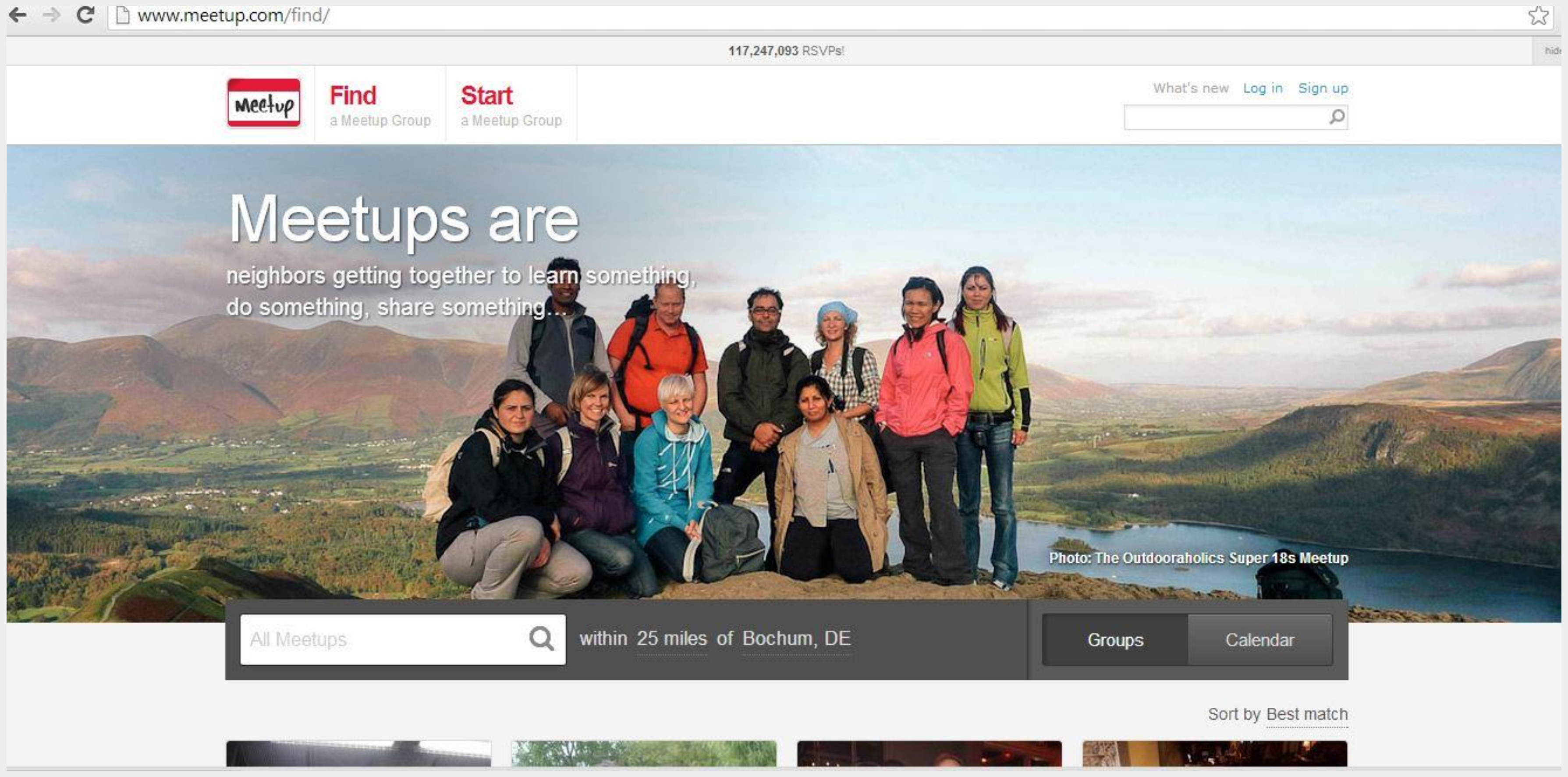
> Hallo,
>
> mein spitzname ist JimRaynor. Alte Email user1@bletgen.net, neue Email jim@mediaob.de, mein Wohnort ist Berlin.
>
> Viele Grüße

LOKALISTEN'S SUPPORT TEAM FINAL RESPONSE

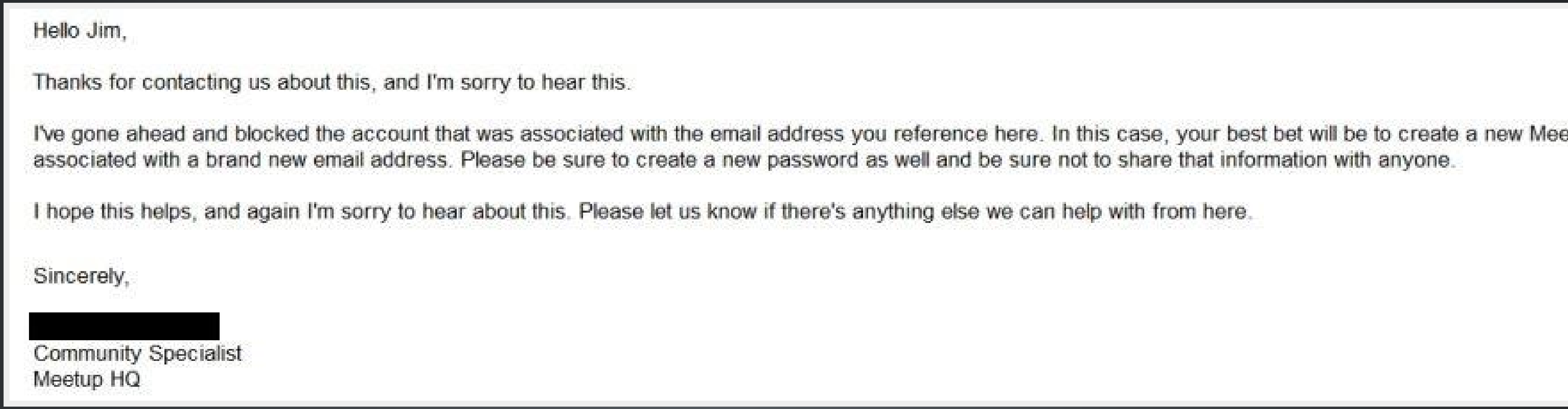


```
hallo,

wir haben gerade deine neue emailadresse ins profil eingetragen.

viele grüße
dein lokalisten team
```

MEETUP (HTTP://WWW.MEETUP.COM/FIND/)



SUPPORT TEAM BLOCKS ACCOUNT :)



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 Mee 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.

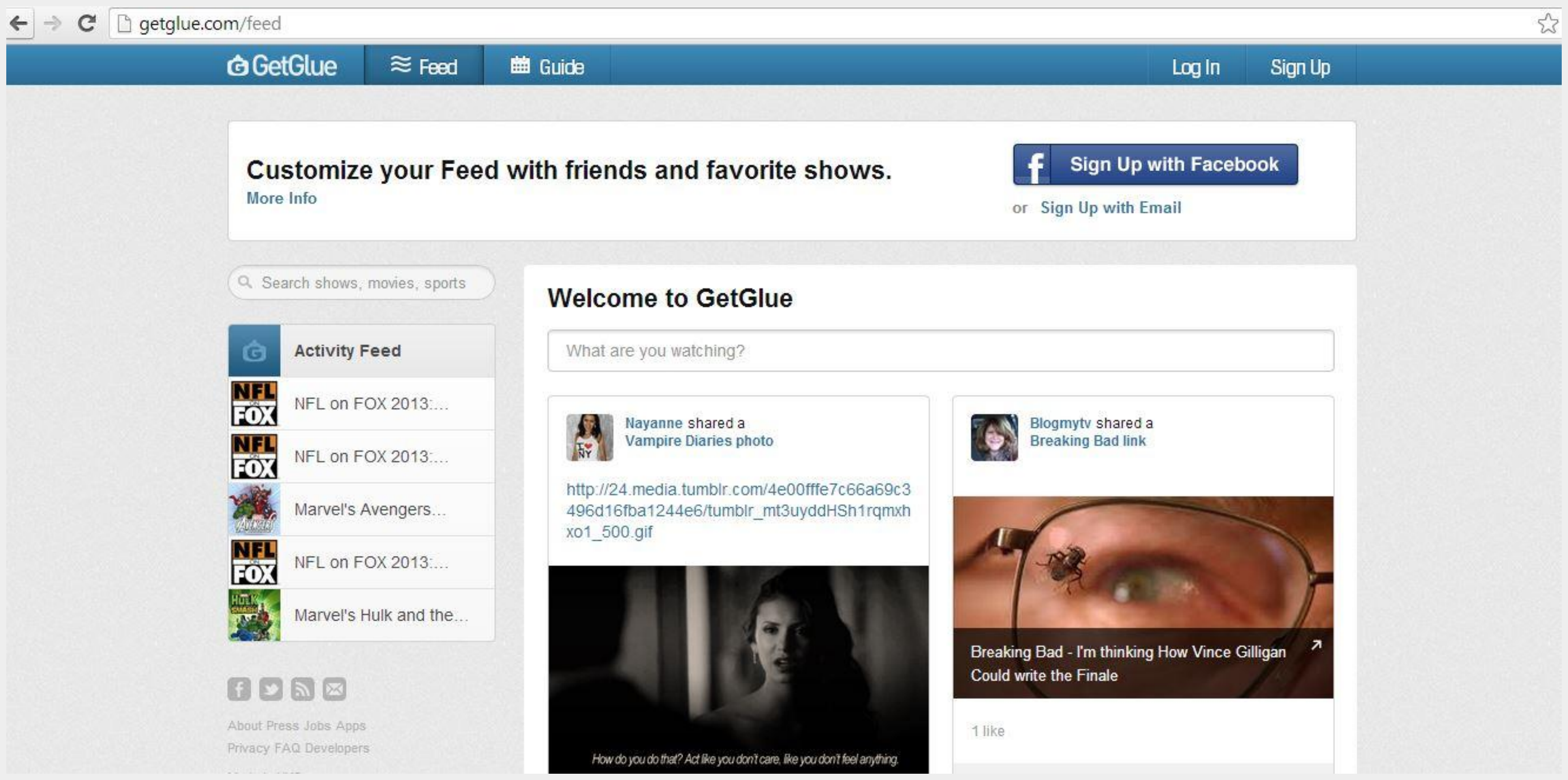
I hope this helps, and again I'm sorry to hear about this. Please let us know if there's anything else we can help with from here.

Sincerely,

[redacted]
Community Specialist
Meetup HQ

GETGLUE (SOCIAL NETWORKS FOR TV FANS)

HTTP://GETGLUE.COM/FEED



Customize your Feed with friends and favorite shows.
More Info

Sign Up with Facebook
or Sign Up with Email

Welcome to GetGlue

What are you watching?

Nayanne shared a Vampire Diaries photo

http://24.media.tumblr.com/4e00fffe7c66a69c3496d16fba1244e6/tumblr_mt3uyddHSh1rqmxhxo1_500.gif

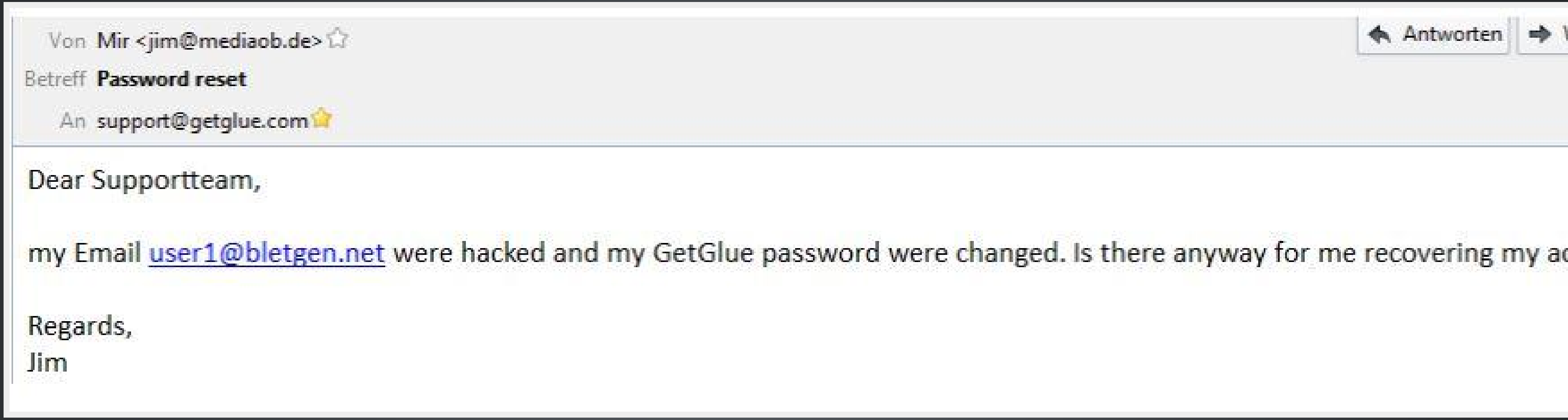
How do you do that? Act like you don't care, like you don't feel anything.

Blogmytv shared a Breaking Bad link

Breaking Bad - I'm thinking How Vince Gilligan Could write the Finale

1 like

OUR EMAIL TO THEIR SUPPORT TEAM



Von Mir <jim@mediaob.de>

Betreff **Password reset**

An support@getglue.com

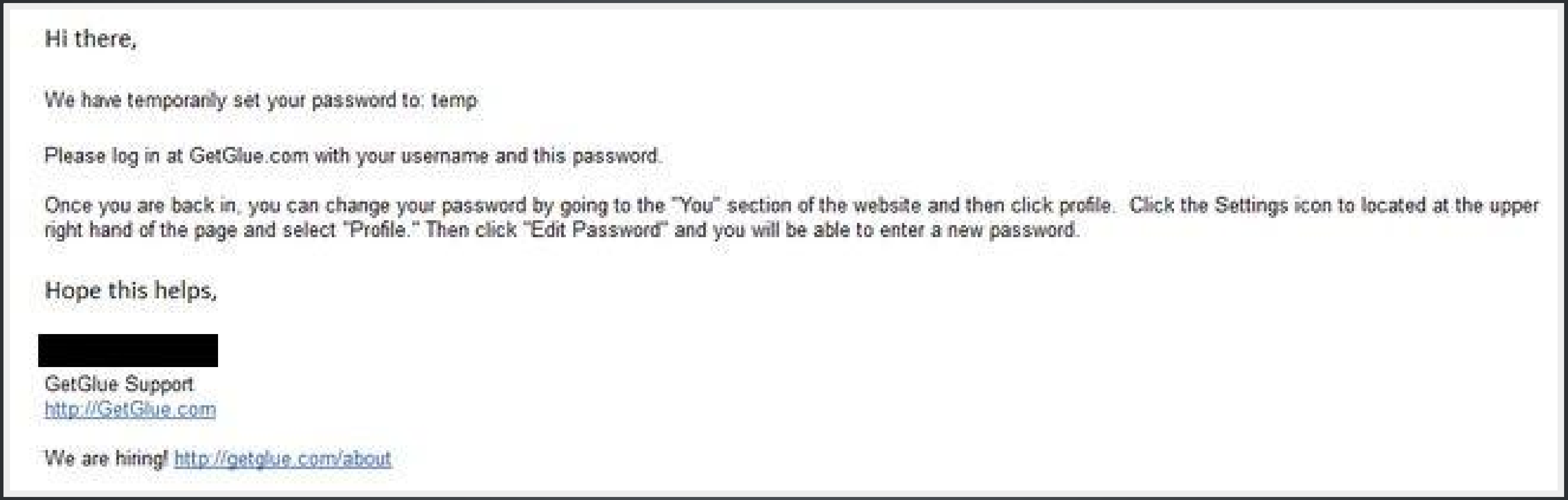
Dear Supportteam,

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

Regards,
Jim

GETGLUE'S SUPPORT TEAM RESPONSE

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



Hi there,

We have temporarily set your password to: temp

Please log in at GetGlue.com with your username and this password.

Once you are back in, you can change your password by going to the "You" section of the website and then click profile. Click the Settings icon to located at the upper right hand of the page and select "Profile." Then click "Edit Password" and you will be able to enter a new password.

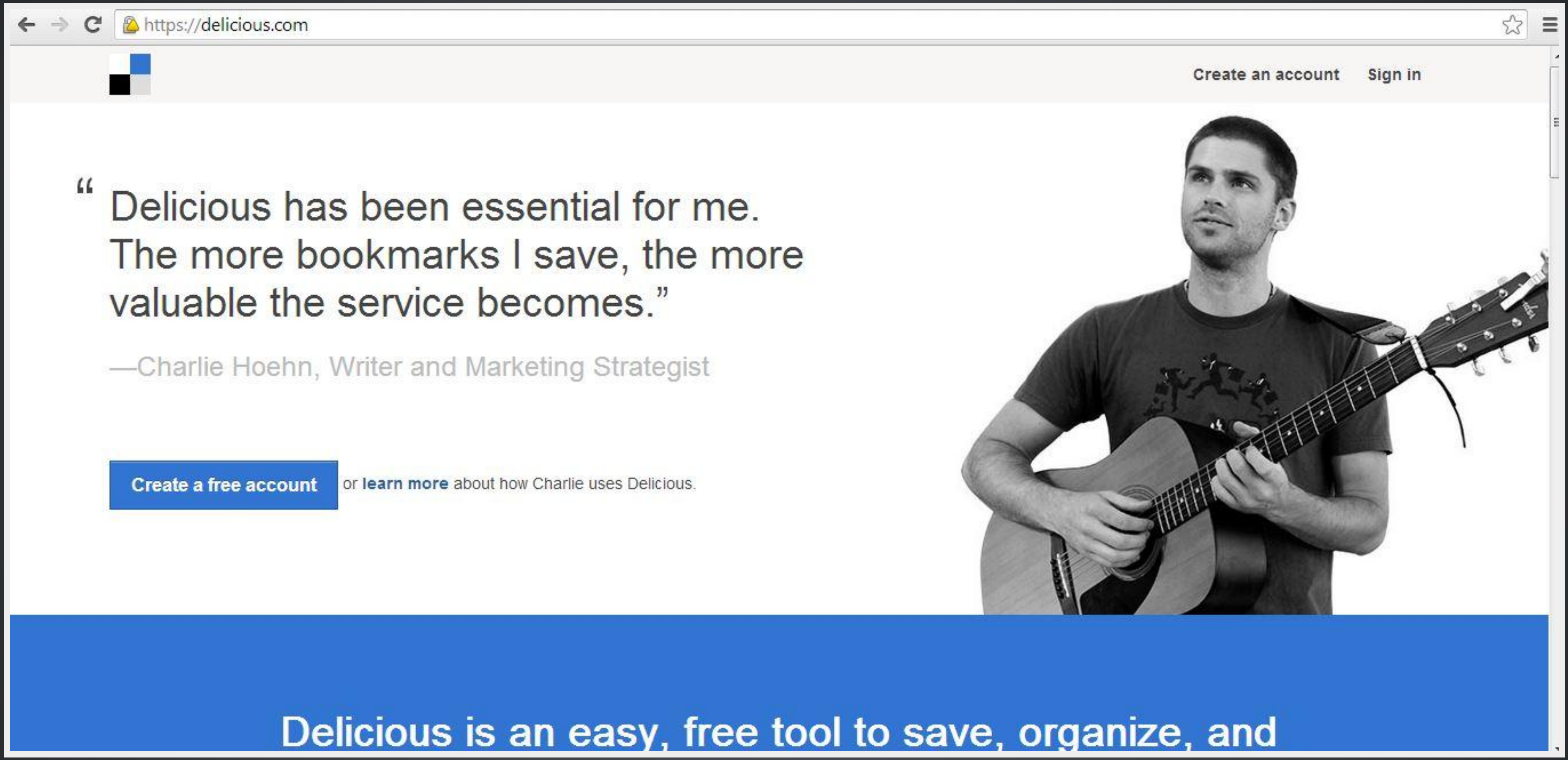
Hope this helps,

[redacted]

GetGlue Support
http://GetGlue.com

We are hiring! http://getglue.com/about

DELICIOUS (HTTPS://DELICIOUS.COM/)



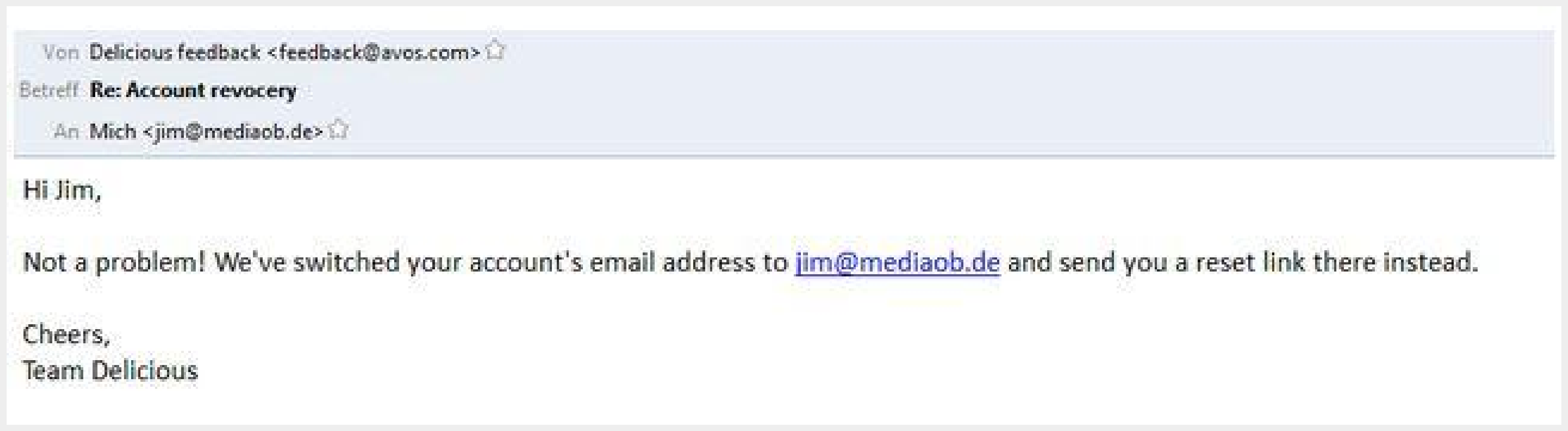
> “Delicious has been essential for me. The more bookmarks I save, the more valuable the service becomes.”
>
> —Charlie Hoehn, Writer and Marketing Strategist

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.



Von Delicious feedback <feedback@avos.com>
Betreff **Re: Account revocery**
An Mich <jim@mediaob.de>

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

FACEBOOK AS SSO

Out of 50 surveyed social networks, we found

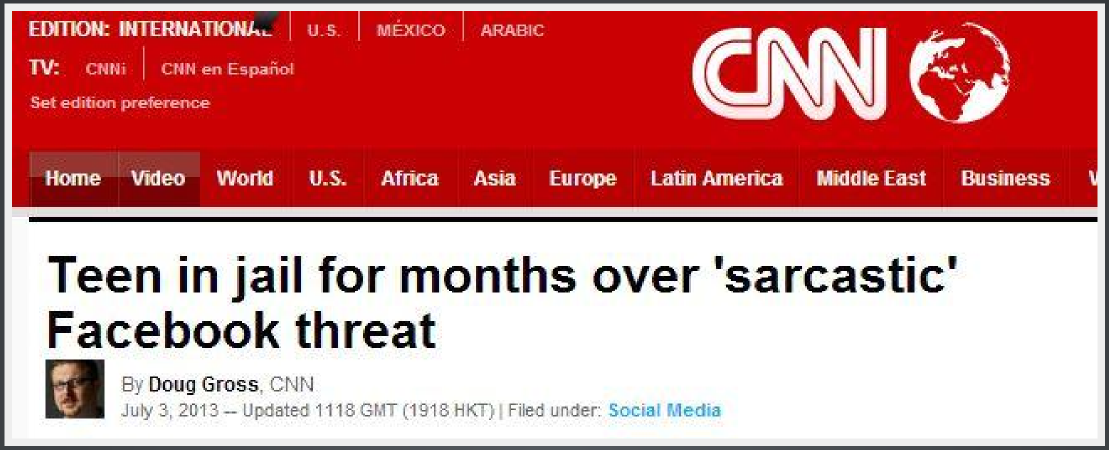
26 use Facebook as login-provider (SSO)
24 don't have this feature

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

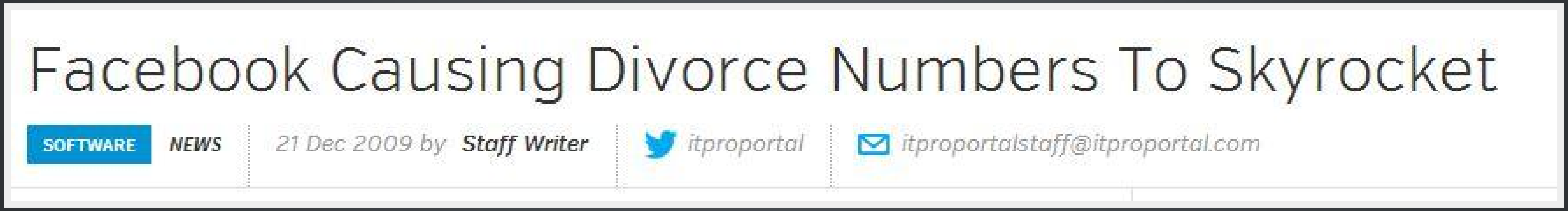
HAVOC EXAMPLES



Teen in jail for months over 'sarcastic' Facebook threat

By Doug Gross, CNN
July 3, 2013 -- Updated 1118 GMT (1918 HKT) | Filed under: Social Media

http://goo.gl/2FVTz8



Facebook Causing Divorce Numbers To Skyrocket

21 Dec 2009 by Staff Writer | itproportal | itproportalstaff@itproportal.com

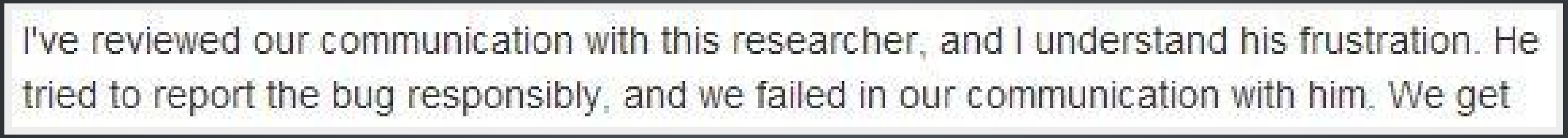
http://goo.gl/uuO7Kq

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

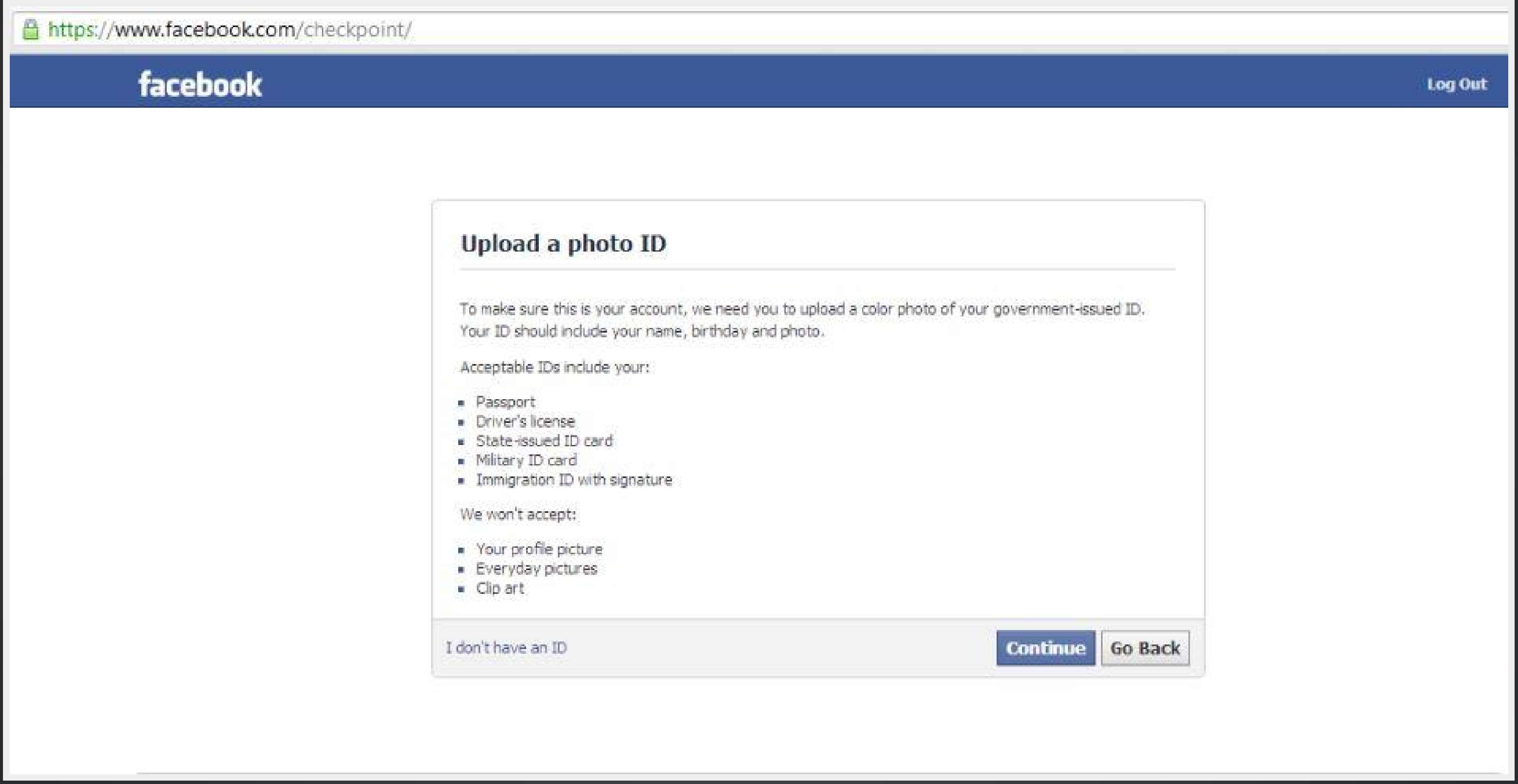
- Train your support teams.
- Facebook should raise the bar as far as communication with the researchers or bug submitters is concerned.
- For Facebook: Please don't send TOO MANY EMAILS because users start believing that these are spam emails.
- Joe wrote in his post (**http://goo.gl/Wf6QMZ**):



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 HOPE NOW FACEBOOK SECURITY TEAM'S REACTION

THANKS!