

## Koobface

Koobface, and its variants, are viruses that have been spreading on Facebook and MySpace since last year. However, a new, more malicious, variant has just been released.

### What it does:

- Takes control of your machine[5] and uses it to create new accounts on sites such as BlogSpot, Twitter, MySpace, and Facebook. Often, you will see a screen prompting you to enter the words on the page or your computer will shut down. This is to circumvent the security most sites have in place for sensitive functions such as creating new accounts.[8]
- Steals private and sensitive data from your machine
- Logs into any other social networking site you have accessed from your machine (ie- Facebook, MySpace, Friendster, Twitter, etc) and posts itself to your profile in these systems as well.
- Hijacks several search engines including Google. When you click on links in the hijacked search, you will be randomly redirected to other sites. Sites related to internet security appear to be targeted. [2]

### How it spreads:

- Sends a tweet containing a link or posts a link to a video entitled “My home video”, “wow”, or “Hey, check out this video of you 😊😊😊”.
- When you click on the link, you are prompted to download a codec or upgrade your Adobe Flash player. You may also be directed to download Anti-Virus 2008, another known virus. [7]
- Directs you to fake Facebook applications and pages to steal your private data. [4][2]
- Uses your computer to create new user accounts and blogs and then posts itself to these accounts and blogs.

### What it affects:

- MySpace
- Facebook
- Twitter
- Friendster
- Blogs (BlogSpot, Google’s blog platform, LiveJournal, etc)

## How to protect yourself:

The US Computer Emergency Response Team recommends the following steps to help protect you and your computer from viruses:

- Install antivirus software and keep the virus signature files up to date. Make sure you have the latest update of McAfee, released this week, to ensure you are protected from this variant of Koobface.
- Do not follow unsolicited links, including videos.
- Use caution when downloading and installing applications.
- Obtain software applications and updates directly from the vendor's website.
- Refer to the [Staying Safe on Social Networking Sites](#) document for more information on safe use of social networking sites.
- Refer to the [Avoiding Social Engineering and Phishing Attacks](#) document for more information on social engineering attacks. [4]

## Koobface resources

1. <http://mashable.com/2009/08/06/koobface-twitter-facebook/>
2. [http://voices.washingtonpost.com/securityfix/2009/08/from\\_koobface\\_with\\_love.html](http://voices.washingtonpost.com/securityfix/2009/08/from_koobface_with_love.html)
3. <http://en.wikipedia.org/wiki/Koobface>
4. [http://www.us-cert.gov/current/archive/2009/03/04/archive.html#malicious\\_code\\_targeting\\_social\\_networking](http://www.us-cert.gov/current/archive/2009/03/04/archive.html#malicious_code_targeting_social_networking)
5. <http://threatpost.com/blogs/koobface-twitter-attacks-growing-more-sophisticated-124>
6. [http://securitywatch.eweek.com/online\\_malware/koobface\\_crew\\_keeps\\_foot\\_to\\_floor.html](http://securitywatch.eweek.com/online_malware/koobface_crew_keeps_foot_to_floor.html)
7. <http://viewfromthebunker.com/2009/07/17/koobface-continues-to-mutate-in-the-search-for-dollars/>
8. <http://www.finjan.com/MCRCblog.aspx?EntryId=2317>