



Facebook Tips for Teens

When we talk about security, we're talking about **scams, viruses, and hacks** that could infect your **computer or your Facebook account** and result in a lot of annoyance for you and your friends. When your login information is stolen, this is often known as **phishing**.

Security isn't just an issue on Facebook, but all over the web, which is why it's important to **be aware online**, and to learn how to protect your accounts and your computer.

Here are some ways to be smart and aware on Facebook:

- **If a link or message seems weird, don't click on it.** This is true of all spam—whether a chain letter, an ad, or a phishing scam. If it seems weird for an old friend to write on your Wall and post a link, that friend may have gotten phished. Let the person know, and don't click on links you don't trust.
- **Be aware of where you enter your password.** Just because a page on the Internet looks like Facebook, it doesn't mean it is. Learn to tell the difference between a good link and a bad one.
- **Report any spam or abuse you see on discussion boards and Walls.** Those report links are there for a reason. The sooner we find spam, the sooner we can remove it and eliminate spammers from the site.
- **Don't use the same password on Facebook that you use in other places on the web.** If you do this, phishers or hackers who gain access to one of your accounts will easily be able to access your others too. You might find yourself locked out of your email and even your bank account.
- **Never share your password with anyone.** Don't do it. Facebook will never ask for your password through any form of communication. If someone pretending to be a Facebook employee asks you for it, don't give it out, and report the person immediately.
- **Don't click on links or open attachments in suspicious emails.** Fake emails can be very convincing, and hackers can spoof the "From:" address so the email looks like it's from Facebook. If the email looks weird, don't trust it, and delete it from your inbox.

- **Add a security question.** If your account ever does get stolen, you might need this to prove your identity to Facebook. If you haven't already done so, you can add a security question from the "Account Settings" page.

Fake Emails

We've received reports of fake emails that look like they came from Facebook. These emails include false notifications for things like friend requests, messages, events, photos, and videos. Sometimes, they also include links to false Facebook pages that then prompt you to download malware. Never click on links in suspicious emails, and if you do accidentally download malware, follow the instructions on the "Resources" tab to clean up your computer.

Photo/Video Spam

Look out for wall posts or messages claiming there's a photo or video of you on another site. These are usually phishing sites. They'll ask you to create an account in hopes that you'll use the same login and password on their site that you use for Facebook. Once you've created an account, the spammer will use your login info to try to access your Facebook account, and will then spam all of your friends with the same message. This is another good reason to use unique logins and passwords for the sites you access on the Internet.

419 Scam

We are currently working with people whose accounts have been affected by "419" scams. Please use caution if you receive messages from friends claiming to be stranded and asking for money. If you have **received or sent a message** like this, please use [this form](#) so that we can make sure your and your friends' accounts are secure.

The Koobface Worm

We're currently helping our users with the recently discovered "[Koobface](#)" worm and phishing sites. If your account has recently been used to send spam, please visit one of the online antivirus scanners from the Helpful Links list, and reset your password [here](#).

False Chain Letter

Recently, some users received a message claiming that Facebook is becoming overpopulated and suggesting that accounts will be deleted. This message is false and did not come from Mark Zuckerberg or Facebook. It can be safely disregarded and deleted.

If spam has been sent from your account:

- Reset your Facebook password **immediately**. You can do this by clicking on the "Forgot Your Password" [link](#) on the login page or by going to the Account Settings [page](#) once logged in.
- If you can't reset the password on your account because the email address you use to log in has been changed, or if your account has been disabled, contact our User Operations team [here](#).
- Run a virus scan on your computer, as you may have inadvertently downloaded malware. Free virus scanners are posted below.

If you've seen spam sent from a friend's account:

- Tell your friend to follow the steps above.
- Warn those who received the spam not to click on it, and to delete it from their Walls and Inboxes **immediately**.