



Own Your Space

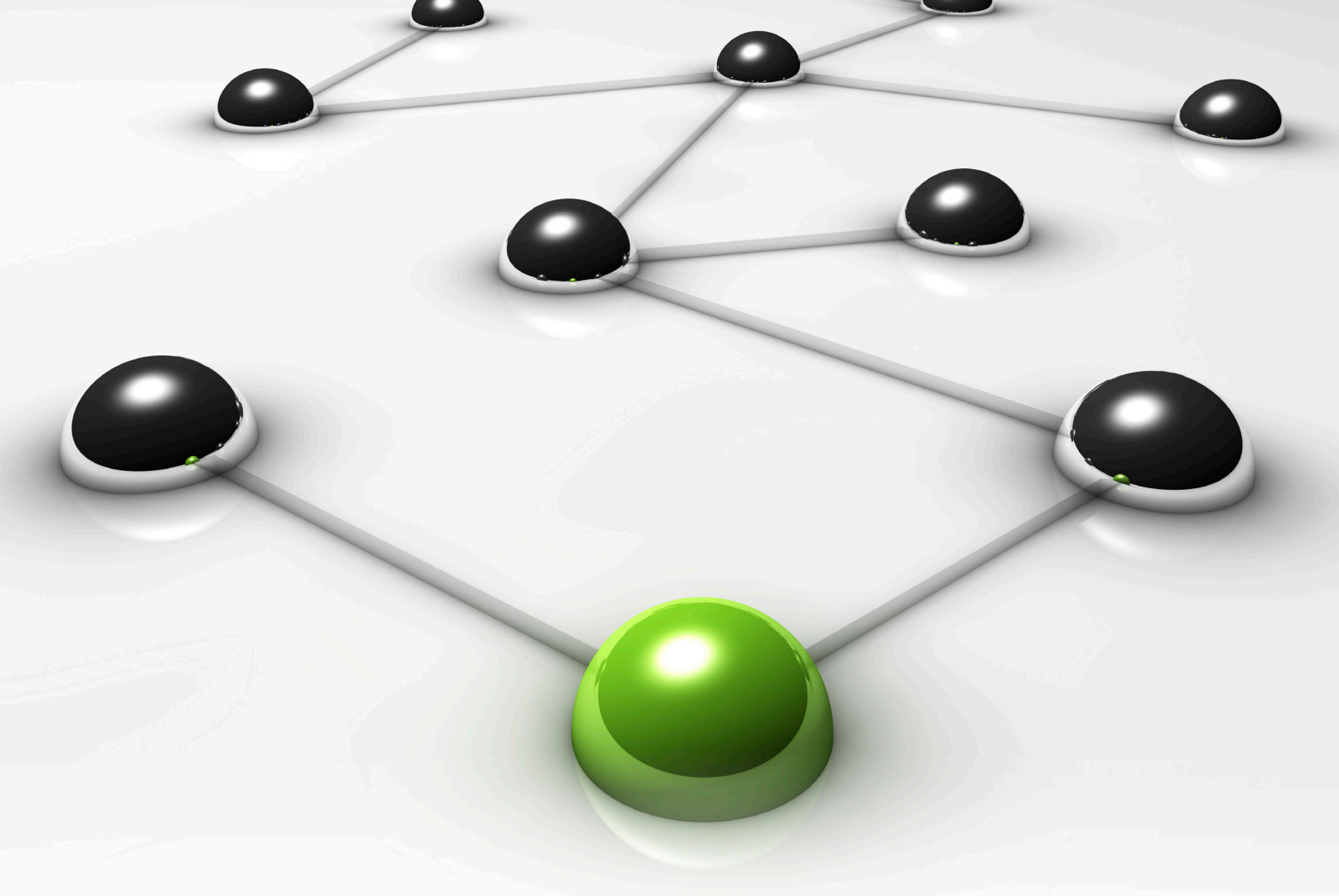
A Guide to Facebook Security

For Young Adults, Parents, and Educators

Linda McCarthy, Keith Watson, and Denise Weldon-Siviy

This online guide explains how you can:

- Protect your Facebook account
- Avoid the scammers
- Use advanced security settings
- Recover a hacked Facebook account
- Stop imposters



If there was any doubt on the incredible power of social networking, consider the more than one billion pieces of content shared each day with over half a billion users. Facebook connects over 500 million people in over 210 countries—indeed, its global population exceeds the size of most European countries, and counts among its members citizens from every single continent in the world.

People on Facebook have great power—they can Friend, Chat, share Status Updates, post Comments, share Links, tag Photos, post Videos, join Groups, create Pages, design Polls, and play together using Applications. They use Facebook to promote causes, interests, and themselves! Facebook allows the world to be more open and connected by giving its users the tools to interact and share in any conceivable way. And, to paraphrase the superhero, with great power comes great responsibility. Just as a city paints sidewalks, and pedestrians look both ways before crossing the street, security on Facebook is a responsibility shared between Facebook and the people who use its platform.

This guide is all about empowering you to Own Your Space—to understand what Facebook is doing to make the site safe and secure and to take the actions that are needed in this new digital world to protect yourself and your account. While the focus of this guide is on Facebook, the lessons here apply to every site you visit online. Throughout the guide, we will highlight the unique tools that Facebook provides so that you can harness your power by protecting your account, using advanced security settings, recovering a hacked Facebook account, and stopping imposters.

Beyond this, we want you to adopt the mantra: Stop. Think. Connect. Facebook has a ton to offer people, and with a little bit of common sense you can stay safe and secure. We hope you find this guide useful. Please join the conversation by visiting the Facebook Security Page at www.facebook.com/security.

Protecting Your Facebook Account

You are the first line of defense in protecting your account. You can take control of your protection by using strong passwords, taking advantage of the many advanced security settings that provide authentication as well as secure communications, and making sure you log out when you are done.

Using good passwords

Using a good password is something that you should do every place you visit on the Internet, not just Facebook. Creating a good password is fairly simple. You want it to be complex enough that it can't be guessed, yet meaningful enough that you can actually remember it.

Have a great password?

- Don't use it for ALL your accounts.
- Don't share it with friends.
- Change it regularly.
- Consider storing it in a password tool.

A good password has at least eight characters, one or more numbers, and at least one special character. Use non-words but associate them with a word. Imagine your pet's name is Buddy, you live on State Street, you're 15, and you like to stargaze at night. A good password for you would be **budstat15***. Or go for something humorous you can remember. One woman set her work password to remind her of why she went to work, **4da\$cash**.

Can't remember that many details? Use a password tool to remember for you. Many browsers now include password vaults. If yours doesn't, consider a free tool like KeePass Password Safe (<http://keepass.info/>). And just in case you still forget, be sure to add a security question and your mobile phone number in the **ACCOUNT SETTINGS** of your Facebook account.

Logging out of Facebook

Logging out of Facebook when you're not using it is a simple and effective way to protect your account. Many people think that if they close the web page or exit the browser that also logs them out of Facebook. It doesn't. The next person who goes to Facebook.com on that computer will find themselves already logged in—to your account. Logging out is crucial when you're accessing Facebook away from home.

But it's also important at home if you share a computer. Just ask Nathan, a 16-year-old who left his Facebook account logged in on the family computer. During one soccer practice, his sister dumped his girlfriend for him by changing his Facebook relationship status to **SINGLE**. Since then, he makes it a point to always log out of Facebook before leaving the house. And remember, if you forget to log out of an active session, you can always remotely close that session from the **ACCOUNT SECURITY** section of the **ACCOUNT SETTINGS** page.

Avoiding the Scammers

It's human nature to avoid dangerous situations. See a piano falling from the roof? You're going to automatically move out of the way. See a scam email, you are going to delete it and report it as spam.

On Facebook, identifying scams is trickier since messages appear to be coming from people you know and trust. So how do you spot a scam on Facebook? Let's begin with a bit of context.

Online scams tend to be moving targets. In the beginning, the obvious scams were email attachments from people you didn't know. Then it was "Security alerts" from banks or credit cards. Today, it can also be a status update from a Friend asking you to watch a new video or visit an "awesome" website.

Conventional Scammers

Scammers hit Facebook for the same reason they target the rest of the Internet. They want access to your information, or your computer, or the money in your pocket. And sometimes they want to trick you into downloading malicious software to your computer. The trick is to recognize the phishers, account thieves, and malware pushers.

Phishers steal personal information, often the data needed for identity theft and fraud. **Phishing** is an attempt to trick users into revealing personal information or financial data. You've already seen phishing scams in your email. On Facebook, phishers can try to scam you from multiple places—in status postings on your profile, in Facebook messages, and in Facebook chat. They can even send you regular email pretending to be Facebook or a popular App like *Farmville* or *Mafia Wars*.

Account thieves try to trick you into logging into a fake Facebook screen in order to steal your Facebook login and password. This is why you should always check the address in your browser bar to make sure you are on Facebook and not some other unrelated site.

Why would anyone want your Facebook account? They hope to access other accounts using your password. They might want to sell your information, or to scam your Friends. People are far more likely to fall for a scam when it comes from someone they trust, like a Friend.

Malware pushers want to install destructive software on your computer. That malicious software, called **malware**, is designed to harm your computer or steal personal information. That malware might do a number of nasty things. It could install spyware to log your keystrokes and collect financial account numbers and passwords. Or even lock up your computer unless you pay a ransom. How do malware pushers target Facebook users? You'll be presented with an offer to download and install new software on your computer. It might be a new game, a digital photo organizer, a digital music player, or any other useful piece of software. Before you download any "free" software, always ask yourself who made it and why it might be free. If it feels a bit dicey, don't download it. You are the first line of defense against malware. Think before you click!

Phishing – *An attempt to trick users into revealing personal information or financial data.*

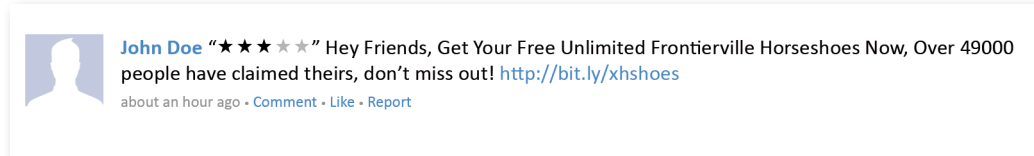
Malware – *Malicious software intended to harm your computer or steal personal information.*

Scammers Who Target Facebook

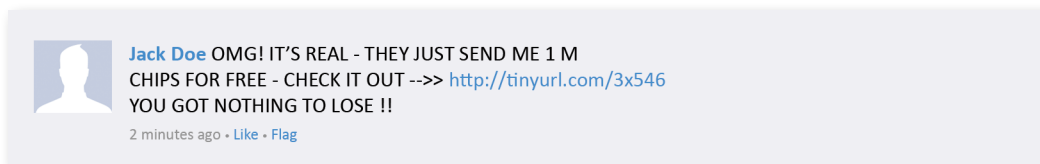
In addition to the run-of-the-mill scams you find all over the Internet, there are several scams that target social networking sites and Facebook users. These include Gaming App scams, Vanity scams, Facebook account thieves, Malicious script scams, and Clickjackers.

Avoiding gaming scams

When we talk about gaming App scams, we don't mean you'll be scammed by the App companies. They're actually as much of a victim as the Facebook users who fall for the scams. If you're an online gamer you already know you have to be careful not to fall for gaming scams. You already see offers for "cheats" and "hacks." A lot of these things that promise to turn you into a great gamer are really designed to steal your personal information.



Many phishing scams pretend to come from popular gaming sites. The danger isn't using known third-party apps like *Frontierville*—it's falling for phishers pretending to offer you game points or clues. The common scams offer prizes like free virtual objects. Other lures claim that your account has been suspended and provide a link for you to remedy the problem. Some of these scams will arrive on your Wall, but a lot will go directly to your email. Why? Numbers. *Farmville* has over 16 million players. Any spammer hitting a large email list with a phishing lure is bound to net a good number of *Farmville* players simply because there are so many *Farmville* players.



You may also see Wall postings like the previous one. Click on the link and you'll be directed to a fake Facebook login page. If you log into the fake page, you're giving your Facebook password directly to the scammer. How can you tell this is a phishing scam? Facebook will never direct you to the homescreen once you are logged in.

Facebook will never direct you to the homescreen once you are logged in.

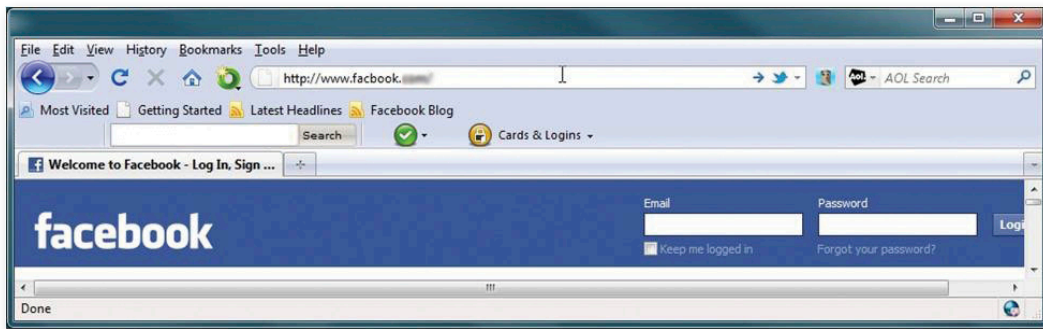
This scammer also used a link shortening service for the above attack. While link shortening services are very helpful because they simplify very long URLs, the downside is that you may not know where they point to until you click. Use extra caution when clicking on these short links.

Avoiding Facebook account thieves

When Facebook accounts are stolen, it's usually because the victim was tricked into using a fake Facebook login screen.

So how do the scammers trick you? Scammers try to catch you off guard and hit you with the fake Facebook login WHILE you're actually using Facebook. The scammer might post a status update on your Wall that includes a link to something enticing. They might do this using an account they've stolen from one of your Friends so they gain your trust. The message will be something that will grab your attention. It might be scandalous photos, a sneak preview of a hot upcoming film, or a weird video. When you click on the link, you're asked to log into Facebook again. Except that you're not on Facebook anymore. The link actually takes you to a different website, so when you re-enter your Facebook login credentials, you're handing them over to a scammer.

Unlike the insanely horrible email scams written in poor English by scammers, most of the fake Facebook login screens are pretty believable.



This fake log-in screen above is recognizable because of the missing “e” in “Facbook” on the address bar. That’s a well-thought scam since most people automatically insert missing vowels while reading without even realizing it.

How do you avoid subtle scams like this one? Remember that Facebook will never contact you by sending you a Facebook message or posting a status message on your Wall. And, ALWAYS, look carefully at both the link in the address bar and links you click. If it looks suspicious—DON’T CLICK. If Facebook does contact you, it will be via the regular email account that you provided when you opened your Facebook account.

Always look at the link and DON’T click on it if it looks suspicious.

Also, remember that Facebook only needs you to log in once each session. If you’re asked to log in again—it’s NOT Facebook.

Avoiding malicious script scam

Malicious script scam is one of the sneakier attacks being used on Facebook users. A common con using this attack method claims to allow you to see who’s been looking at your profile. This enticing scam tries to trick you into pasting text into your browser address bar.



The “unique code” shown above is the malicious script. While you’re being patient as instructed, the script is setting up your profile to spam all of your Friends.

In response to detecting these kind of attacks, Facebook added checks to help detect scripts being pasted into the address bar. So if you do paste a script, Facebook will ask you to confirm that you really want to paste that script—and even tell you why it’s a bad idea. Pay attention to these warnings.

Don’t paste a script into your browser address bar unless you know exactly what it does and how.

How do you avoid malicious script scam? Don’t paste a script into your browser address bar unless you know *exactly* what it does and *how*. Also give your Friends a heads up if you start seeing spam from them. Your Friends may be completely clueless that their Facebook accounts have been hacked. Let them know to change their passwords and how to recover a hacked account if needed. (Read on to learn how to recover a hacked account.)

Avoiding clickjacking

Clickjacking is a technique used by attackers to trick users into clicking on links or buttons that are hidden from view. Clickjacking is possible because of a security weakness in web browsers that allows web pages to be layered and hidden from view. You think you are clicking on a standard button, like the **PLAY** button on an enticing video, but you are really clicking on a hidden link. Since you can't see the clickjacker's hidden link, you have no idea what you're really doing. You could be downloading malware or making all your Facebook information public without realizing it.

One form of clickjacking is to hide a **LIKE** button underneath a dummy button. That's called Likejacking. A scammer might trick you into saying that you like a product you've never heard of in an underhanded bid to create viral marketing buzz. At first glance, likejacking sounds more annoying than harmful, but that's not always true. If you're scammed into liking Justin Bieber, the world isn't likely to end. But you may be helping to spread spam or possibly sending Friends somewhere that contains malware.

How can you avoid being jacked? Technologically, you can minimize your risk by staying current on browser updates. The browser companies are continually adding updates to shut down vulnerabilities that allow clickjackers and other scammers to operate. If you're using Firefox, also consider installing the NoScript add-on. Beyond that, pay attention to what you're getting and from whom. Would a college professor really share a post about watching hidden camera videos? If a post from one of your Friends seems suspicious, don't click on it!

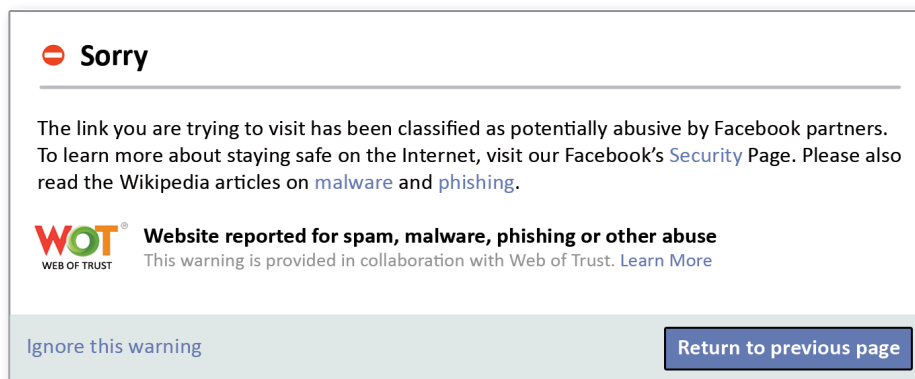
A suspicious post could be a sign that your Friend's Facebook account has been hijacked or that your Friend has been clickjacked to **LIKE** or **SHARE** something without knowing it. If you know your Friends, you'll know what those Friends really would **LIKE** or **SHARE**. That's why one of your best protections against scams is not confirming Friend requests from people you don't actually know.

Another great tool to help you avoid clickjacking is Web of Trust (WOT). WOT is a free browser tool that maintains a database of known safe sites as well as malicious sites reported by the WOT community. Attempt to visit a known malicious site and WOT warns you in advance. The WOT download is simple to install; just visit www.mywot.com.

Security Tips

- Keep software up to date.
- Don't click on suspicious links.
- Use available security tools.

Facebook also has checks in place to detect malicious and spammy websites. Adding WOT to the existing Facebook checks gives you one more tool in your arsenal against hackers. The two checks work together to provide a joint warning system if you attempt to visit a site reported to have malware, phishing, or spam:



Clickjacking – *A technique used by attackers to trick users into clicking on links or buttons that are hidden from view.*

Using Advanced Security Settings

Facebook takes a number of steps behind-the-scenes to keep the site secure. Facebook also provides tools that people can use to protect their accounts and online reputations. Those tools include options for secure browsing, one-time passwords, single sign-on, the ability to monitor account activities, login approvals, the ability to remotely end account activity, and social authentication.

Using secure browsing

Secure browsing allows you to use Facebook safely in public hot spots. When you shop online, your web browser uses some very strong encryption to transmit data. Encryption is a technique used to scramble data that you don't want anyone else to see.

The SSL **protocol** encrypts the transmission of data and is called using *https* or *secure browsing*.

Secure browsing is an advanced setting on Facebook that you can configure. Using https to connect to Facebook does several important things. First, on an open wireless network, it prevents attackers from stealing your Facebook network connection or eavesdropping on your communication. It also uses certificate verification to make sure that if your browser says you're connected to Facebook, you really are connected to Facebook and not an imposter website pretending to be Facebook.

To enable https, go to the **ACCOUNT SECURITY** section of your Facebook **ACCOUNT SETTINGS** and tell Facebook to **BROWSE FACEBOOK ON A SECURE CONNECTION (HTTPS) WHENEVER POSSIBLE**.

How can you tell that https is working? When SSL is in use, you will know that your communication between websites is secure because you'll see an "https" at the beginning of the URL. You'll also see a padlock. Look for that padlock icon on your web browser. If you see the padlock, your secure browsing setting is locked up!



Using one-time passwords

It's always a little risky accessing your Facebook account from a computer you don't own. You never really know where that computer's been. It might be infected with a keystroke logger that could record your every move, including the password to your Facebook account. You can't really prevent that, but you can make sure the password captured won't work by using a one-time password.

To use a one-time password, you need to first register and verify your cell phone with Facebook. Once you do, you can obtain a one-time password by texting the message "otp" (for "one-time password") to 32665 (FBOOK). Facebook will text back a temporary password that you can use to log into your Facebook account instead of using your normal password. If that password is recorded, it doesn't matter because it only works once. Even better, it's only good for 20 minutes. It's a good idea to use a one-time password any time you use someone else's computer.

Using single sign-on

One of the most important steps to protect your information is to have a different password for every account you hold. Of course, remembering all of those passwords is difficult. Facebook has opened its user account system to other websites to use. This means that you can use your Facebook account to access other websites that support Facebook login. The first time you use your Facebook login from a new site, Facebook will ask for your permission to share your information with that website. If you allow this, the website can log you in automatically by recognizing that you're already logged into Facebook. This is a great feature! The more sites you allow to recognize your Facebook login, the fewer usernames and passwords you need to remember.

Protocol – *A protocol is a set of rules that computers use to communicate with each other.*

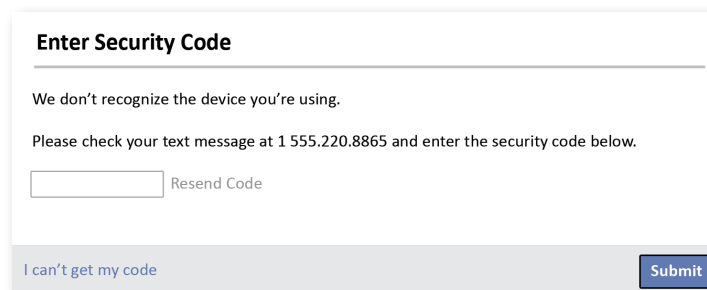
Monitoring account activity

When you access your account, Facebook recognizes your computer or cell phone. If you'd like, Facebook can even tell you when your account is being accessed from somewhere else.

In the **ACCOUNT SECURITY** section of your **ACCOUNT SETTINGS**, you can use the **LOGIN NOTIFICATIONS** to ask Facebook to send you an email if a different computer or mobile device logs into your account. If the new login isn't you, follow the link in the email to boot the intruder out. If you prefer, you can have Facebook send you a text instead of an email.

You can even boot out the intruder yourself. In the **ACCOUNT SECURITY** section of your **ACCOUNT SETTINGS** you'll find a list of computers associated with your account and account activity. If there are computers in the list that you no longer use or have never used, you can remove them from the list. In the **ACCOUNT ACTIVITY** section, you'll find the most recent activity and other active sessions. If any of these look suspicious, just click on **END ACTIVITY**. This immediately logs out that session.

Another cool security feature is **LOGIN APPROVALS**. If you have a cell phone, Facebook can send you a text message with a unique code to use when you log into Facebook from a different computer. With this enabled, you'll be asked to enter a code that you receive via text message once you try to login. This is a great feature that adds another level of security for people who login to Facebook from remote locations. Make sure you have your cell phone and go to the **ACCOUNT SECURITY** section of your **ACCOUNT SETTINGS** to configure. Once you configure these settings, the very next time you login from a different computer a text message will be sent to your phone with the approval code. Below you can see the Facebook screen asking you to enter that code.



Using social authentication

When websites want to prevent an automated program from trying to register a lot of fake accounts, they ask it to do something only a human can do. These are often tests that involve solving a simple math puzzle, answering a simple question, or typing a series of letters and numbers from a picture. When you see a picture with weird words, that's called a CAPTCHA or Completely Automated Public Turing test to tell Computers and Humans Apart. These simple pictures prevent attackers from using software to create a lot of accounts to send spam or phishing lures on a large scale.

Facebook uses a similar test called Social Authentication when Facebook sees your account in use but thinks the user may not be you. For example, if you live in Indiana and your account is accessed from India, Facebook gets suspicious.

Why Social Authentication? Well, Facebook IS a social network! More importantly, Facebook wanted an easy way to identify you that wouldn't be compromised if your account was. Obviously, if someone else really is using your account they've either guessed or stolen your password so asking for that wouldn't help.

Know all your Friends?

Facebook assumes you do. If you access your account from a strange place—like while vacationing in Europe—Facebook verifies your identity by having you identify your Friends in tagged photos.

This is where your Friends come in. If Facebook suspects that someone else is trying to use your account, they'll ask you to identify your Friends. Literally. Facebook creates a series of pictures from your Friends list and sets it up like a multiple-choice exam. Each photo has a list of names. You need to select the name that matches the Friend tagged in that photo. Since it's very unlikely that a scammer would recognize your Friends by sight, this is a great test.

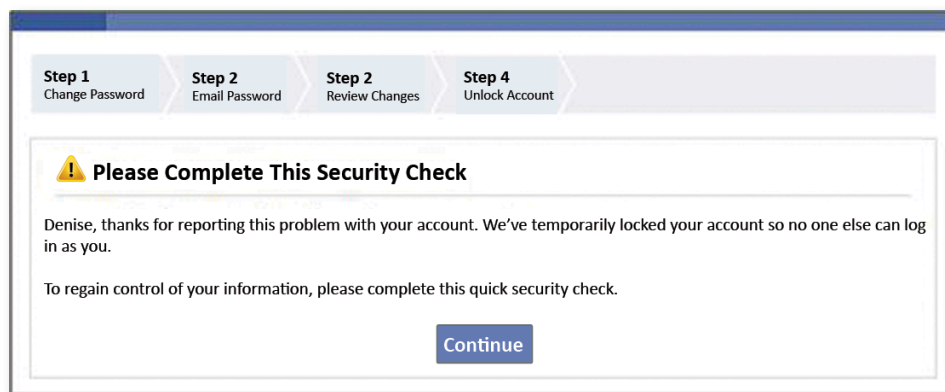
Recovering a Hacked Facebook Account

There are a number of signs that can indicate that your Facebook account has been hacked. You might notice Status updates that you didn't post or receive replies to Facebook messages you didn't send. That *might* mean that your account has been hacked. Immediately change your password and make sure you're using the advanced security settings.

A certain indication that your account has been hacked is not being able to log in. This happens when the scammer who hacked your account changes your password. You can't change it back because you no longer know what it is. Some scammers will even reset personal information so you can't verify who you are.

The Facebook team is dedicated to helping you protect your account. Facebook has built systems that look for and block suspicious activity, phony posts, and messages. Facebook also has a well-defined process if your account is stolen to help you shut down the scammer and recover your own account.

If your account is compromised, go to <http://www.Facebook.com/hacked> and ask Facebook to **SECURE YOUR ACCOUNT**.



The screenshot shows a four-step process for recovering a hacked Facebook account. The steps are: Step 1: Change Password, Step 2: Email Password, Step 2: Review Changes, and Step 4: Unlock Account. The current step is Step 2: Review Changes, which is highlighted. Below the steps, there is a warning icon and the text: "Please Complete This Security Check". The text continues: "Denise, thanks for reporting this problem with your account. We've temporarily locked your account so no one else can log in as you. To regain control of your information, please complete this quick security check." A "Continue" button is located at the bottom right of the security check area.

As soon as you report this, Facebook locks your account. While you can't use it yet, the scammer can't access it either. Facebook will then ask you to **PLEASE COMPLETE THIS SECURITY CHECK** to unlock your account.

Facebook makes this pretty simple so follow their four-step process to reclaim your account.

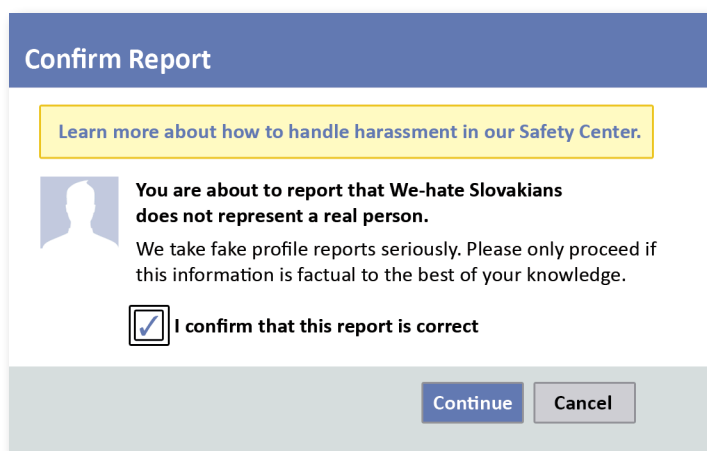
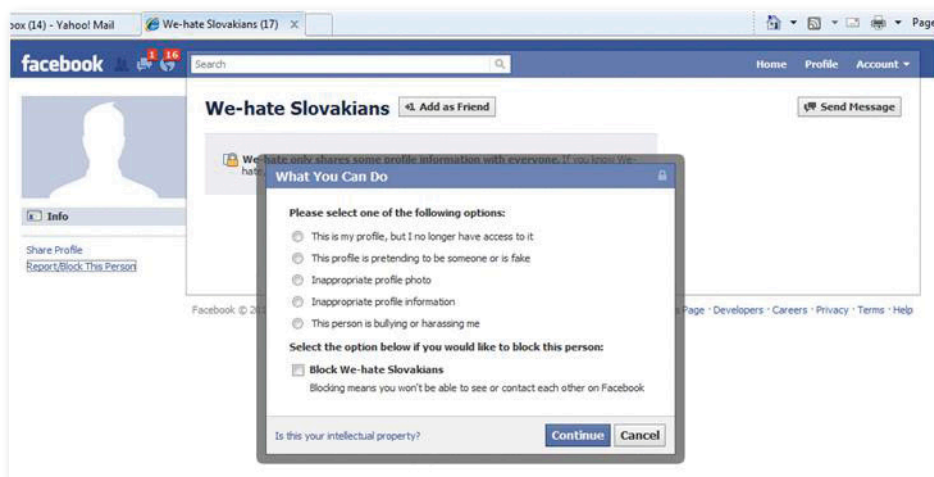
Once you've recovered your account, be sure to set up advanced security features to add an extra layer of security to your account. In particular, be sure to enable secure browsing (https) and set login notifications so Facebook will let you know immediately when your account is accessed.

Stopping Imposters

It's a sad thing when a good account goes bad by being stolen. It's a sick thing when an account STARTS bad because it was created to harass, embarrass, or bully someone. That's what an imposter account is—when someone pretends to BE you by putting up a Facebook page. Imposter pages are created to harass or bully the person being impersonated. If you see an imposter page, you should report it to Facebook immediately.

The link to **REPORT/BLOCK THIS PERSON** is available at the bottom-left side of every Facebook profile.

You can report people who are impersonating you or a Friend. You can also use this link to report fake people, businesses pretending to be people, and hate groups masquerading as people.



If you're reporting a fake person or inappropriate information, that's all you need to do. Facebook will thank you for reporting the problem, then they'll investigate your claim and close the account if warranted.

If you're reporting an imposter or a cyberbully, there's an added step. Because one way to harass people on Facebook has been to pretend that they're harassing you, Facebook won't proceed until you provide a valid phone number. Apparently, bullies don't like to give out their phone numbers. Once you provide a valid phone number, Facebook will send a code to your phone that you'll need to enter to confirm this report before they begin their investigation.

Securing Your Future

Security risks will always be a moving target. Remember the “stalker Apps” promising to show you who was viewing your profile that everyone fell for last year? Or this year’s links promising funny edited pictures of you or pictures you are tagged in? No such photos existed of course, but the enticing links are sent to try and catch users off guard. New threats appear all of the time.

Today’s risk may be obsolete tomorrow. The trick is to recognize tomorrow’s risk when it arrives. Facebook’s security team is working hard to protect you, but you need to participate in keeping your account safe. To learn more about security and to stay posted on threats and new Facebook security features, check out the **FACEBOOK SECURITY** and **FACEBOOK SAFETY** pages.



Top Tips for Staying Secure on Facebook

- Only Friend people you know.
- Create a good password and use it only for Facebook.
- Don't share your password.
- Change your password on a regular basis.
- Share your personal information only with people and companies that need it.
- Log into Facebook only ONCE each session. If it looks like Facebook is asking you to log in a second time, skip the links and directly type www.facebook.com into your browser address bar.
- Use a one-time password when using someone else's computer.
- Log out of Facebook after using someone else's computer.
- Use secure browsing whenever possible.
- Only download Apps from sites you trust.
- Keep your anti-virus software updated.
- Keep your browser and other applications up to date.
- Don't paste script (code) in your browser address bar.
- Use browser add-ons like Web of Trust and Firefox's NoScript to keep your account from being hijacked.
- Beware of "goofy" posts from anyone—even Friends. If it looks like something your Friend wouldn't post, don't click on it.
- Scammers might hack your Friends' accounts and send links from their accounts. Beware of enticing links coming from your Friends.

Remember to STOP | THINK | CONNECT!

To learn more on protecting yourself online please check out the *Stop. Think. Connect.* campaign both on and off Facebook. Head over to the Facebook Security Page to take the Security Quiz so you too can test your knowledge and learn best practices for staying secure online.

About the Team

The Facebook Security Guide is co-written by renowned authors in the security industry.

Linda McCarthy is the former Senior Director of Internet Safety at Symantec. Linda brings 20 years of experience in areas of security education, auditing, and product development.

Keith Watson is a security research engineer at Purdue University. His research areas: security architecture, biometrics, digital forensics, privacy and secure programming.

Denise Weldon-Siviy is a teacher and editor with two decades of editing experience and a house full of teenage Facebook users.



STOP | THINK | CONNECT™



This work is licensed under a Creative Commons Attribution-NoDerivs 3.0 Unported License.