hello fellow hackers. in this article, i will tell you the "rules" i live by as a gray hat hacker. a gray hat hacker is, in theory, a hacker who makes the wrong decisions for the right reasons. an example of something typical gray hat would be to hack a company, and go report the vulnerability to them, even if you didn't have permission to do it. but i think being a gray hat is more than that. being a gray hat is kind of being the hero who doesn't follow the rules all the time. what i think a gray hat is is someone who uses their knowledge in the name of their own morals. so, here are those "rules" i talked about earlier.

1. **remain in plain sight**. gray hats are not always welcome everywhere. so keeping a low profile is required to be a successful gray hat. make yourself as anonymous as possible. use I2P and TOR as much as possible. use fake emails, usernames, and whatnot. this may seem a little bit paranoid, but keep in mind that all of this can be used against you one day.
2. **just because you probably will act outside of the law, doesn't mean you can use your hacking for personal gain**. this is maybe the most important rule to a gray hat. even if you act outside the law, it doesn't mean you can use your knowledge for your own personal gain. as a gray hat, you are there to use your hacking to help the rest of the world, not yourself.
3. **Knowledge is your weapon**. a gray hat's weapon is a computer and it's bullet is knowledge. when you run into someone, both in real life or virtually, who seems to act like a fool, don't argue with them. educate them. do not raise your voice in a discussion, improve your point.
4. **Knowledge is also open source**. knowledge is what makes us different from animals, and thus, denying it to someone else should be seen as a crime.
5. **Stay away from the innocent**. simply don't involve anyone who doesn't have anything to do with something.

i think it is these 5 rules that define a gray hat. what do you think? do you agree/disagree? did i miss something? comment your opinion below!

-Phoenix750

It's good to password-protect your PC to make sure that your personal files, folders, and important documents are safe and can't be modified without your permission. Though, entering the password all of the time before using your computer might frustrate you.

Here, you will be find an easy way to remove passwords in such a way that Windows will automatically get to the desktop without asking you to enter the system password. Though, you can restore it back whenever you feel that your system is not safe anymore.

**How to Bypass Password Login**

1. Start typing "netplwiz" (without quotes) in the Windows 8 start screen and hit enter to launch the "User Accounts" control panel (*on older versions of Windows, click "User Accounts Control Panel"*).

[](http://img.wonderhowto.com/img/original/96/81/63489708799507/0/634897087995079681.jpg)

Image via [wonderhowto.com](http://wonderhowto.com)

1. Enter your password if prompted.
2. In the window that opens, uncheck the box stating "Users must enter a username and passwords to use this computer" and click OK (*on older versions of windows, first double-click the account you wish to automatically log in*).

[](http://img.wonderhowto.com/img/original/60/27/63489708819179/0/634897088191796027.jpg)

Image via [wonderhowto.com](http://wonderhowto.com)

1. Enter and reenter the existing account password(s) if you're asked.

[](http://img.wonderhowto.com/img/original/73/86/63489708896555/0/634897088965557386.jpg)

That's it. From now on, you will not see the password screen anymore.

However, If you don't want to use this feature anymore and are interested in getting your old Windows 8 password screen back, you can restore it by following the above steps—except the 3rd one where you need to select the check box, which we have de-selected previously.

You can follow the same steps to bypass password screen on previous version of Windows too, not just Windows 8.

Despite the security concerns that have plagued Facebook for years, most people are sticking around and new members keep on joining. This has led Facebook to break records numbers with over [one billion monthly active users](http://newsroom.fb.com/Key-Facts) as of October 2012—and around 600 million active daily users.

We share our lives on Facebook. We share our birthdays and our anniversaries. We share our vacation plans and locations. We share the births of our sons and the deaths of our fathers. We share our most cherished moments and our most painful thoughts. We divulge every aspect of our lives. We even clamor to see the [latest versions even before they're ready](http://galaxy-note-3.wonderhowto.com/how-to/get-facebooks-future-android-look-your-galaxy-note-3-right-now-0154041/) for primetime.

But we sometimes forget who's watching.

We use Facebook as a tool to connect, but there are those people who use that connectivity for malicious purposes. We reveal what others can use against us. They know when we're not home and for how long we're gone. They know the answers to our security questions. People can practically steal our identities—and that's just with the visible information we purposely give away through our public Facebook profile.

[](http://img.wonderhowto.com/img/original/22/19/63491552697702/0/634915526977022219.jpg)

The scariest part is that as we get more comfortable with advances in technology, we actually become more susceptible to hacking. As if we haven't already done enough to aid hackers in their quest for our data by sharing publicly, those in the know can get into our emails and Facebook accounts to steal every other part of our lives that we intended to keep away from prying eyes.

In fact, you don't even have to be a [**professional hacker**](http://null-byte.wonderhowto.com/how-to/hack-like-a-pro/) to get into someone's Facebook account.

It can be as easy as [**running Firesheep on your computer**](http://tag.wonderhowto.com/firesheep/) for a few minutes. In fact, Facebook actually allows people to get into someone else's Facebook account without knowing their password. All you have to do is choose three friends to send a code to. You type in the three codes, and voilà—you're into the account. It's as easy as that.

In this article I'll show you these, and a couple other ways that hackers (and even regular folks) can hack into someone's Facebook account. But don't worry, I'll also show you how to prevent it from happening to you.

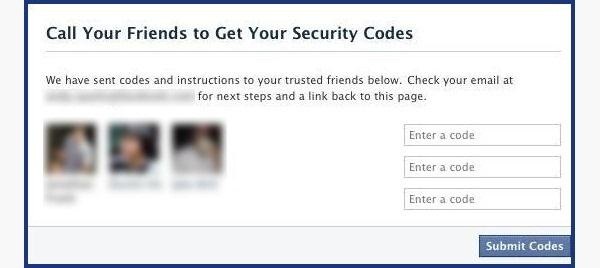
**Method 1: Reset the Password**

The easiest way to "hack" into someone's Facebook is through resetting the password. This could be easier done by people who are friends with the person they're trying to hack.

* The first step would be to get your friend's Facebook email login. If you don't already know it, try looking on their Facebook page in the Contact Info section.
* Next, click on **Forgotten your password?** and type in the victim's email. Their account should come up. Click **This is my account**.
* It will ask if you would like to reset the password via the victim's emails. This doesn't help, so press **No longer have access to these?**
* It will now ask **How can we reach you?** Type in an email that you have that also isn't linked to any other Facebook account.
* It will now ask you a question. If you're close friends with the victim, that's great. If you don't know too much about them, make an educated guess. If you figure it out, you can change the password. Now you have to wait 24 hours to login to their account.
* If you don't figure out the question, you can click on **Recover your account with help from friends**. This allows you to choose between three and five friends.

[](http://img.wonderhowto.com/img/original/64/79/63491552940204/0/634915529402046479.jpg)

* It will send them passwords, which you may ask them for, and then type into the next page. You can either create three to five fake Facebook accounts and add your friend (especially if they just add anyone), or you can choose three to five close friends of yours that would be willing to give you the password.

[](http://img.wonderhowto.com/img/original/88/34/63491552960437/0/634915529604378834.jpg)

**How to Protect Yourself**

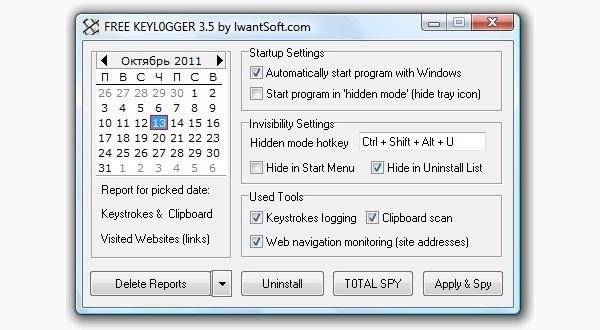
* Use an email address specifically for your Facebook and don't put that email address on your profile.
* When choosing a security question and answer, make it difficult. Make it so that no one can figure it out by simply going through your Facebook. No pet names, no anniversaries—not even third grade teacher's names. It's as easy as looking through a yearbook.
* Learn about recovering your account from friends. You can select the three friends you want the password sent to. That way you can protect yourself from a friend and other mutual friends ganging up on you to get into your account.

**Method 2: Use a Keylogger**

**Software Keylogger**

A software keylogger is a program that can record each stroke on the keyboard that the user makes, most often without their knowledge. The software has to be downloaded manually on the victim's computer. It will automatically start capturing keystrokes as soon as the computer is turned on and remain undetected in the background. The software can be programmed to send you a summary of all the keystrokes via email.

CNET has [Free Keylogger](http://download.cnet.com/Free-Keylogger/3000-2162_4-10419683.html), which as the title suggests, is free. If this isn't what you're looking for, you can search for other free keyloggers or pay for one.

[](http://img.wonderhowto.com/img/original/29/09/63491553875660/0/634915538756602909.jpg)

**Hardware Keylogger**

These work the same way as the software keylogger, except that a USB drive with the software needs to be connected to the victim's computer. The USB drive will save a summary of the keystrokes, so it's as simple as plugging it to your own computer and extracting the data. You can look through [Keelog](http://www.keelog.com/) for prices, but it's bit higher than buying the software since you have the buy the USB drive with the program already on it.

[](http://img.wonderhowto.com/img/original/22/50/63491553951991/0/634915539519912250.jpg)

**How to Protect Yourself**

* Use a firewall. Keyloggers usually send information through the internet, so a firewall will monitor your computer's online activity and sniff out anything suspicious.
* Install a password manager. Keyloggers can't steal what you don't type. Password mangers automatically fill out important forms without you having to type anything in.
* Update your software. Once a company knows of any exploits in their software, they work on an update. Stay behind and you could be susceptible.
* Change passwords. If you still don't feel protected, you can change your password bi-weekly. It may seem drastic, but it renders any information a hacker stole useless.

**Method 3: Phishing**

This option is much more difficult than the rest, but it is also the most common method to hack someone's account. The most popular type of *phishing* involves [**creating a fake login page**](http://null-byte.wonderhowto.com/inspiration/social-engineering-part-2-hacking-friends-facebook-password-0130323/). The page can be sent via email to your victim and will look exactly like the Facebook login page. If the victim logs in, the information will be sent to you instead of to Facebook. This process is difficult because you will need to create a web hosting account and a fake login page.

[](http://img.wonderhowto.com/img/original/13/97/63491554017324/0/634915540173241397.jpg)

The easiest way to do this would be to **follow our guide on** [**how to clone a website**](http://null-byte.wonderhowto.com/how-to/hack-like-pro-clone-any-website-using-httrack-0152420/) to make an exact copy of the facebook login page. Then you'll just need to tweak the submit form to copy / store / email the login details a victim enters. If you need help with the exact steps, there are [**detailed instructions available**](http://null-byte.wonderhowto.com/inspiration/social-engineering-part-2-hacking-friends-facebook-password-0130323/) by Alex Long here on Null Byte. Users are very careful now with logging into Facebook through other links, though, and email phishing filters are getting better every day, so that only adds to this already difficult process. But, it's still possible, especially if you [**clone the entire Facebook website**](http://null-byte.wonderhowto.com/how-to/hack-like-pro-clone-any-website-using-httrack-0152420/).

**How to Protect Yourself**

* Don't click on links through email. If an email tells you to login to Facebook through a link, be wary. First check the URL ([**Here's a great guide on what to look out for**](http://internet.wonderhowto.com/how-to/dont-be-duped-by-malicious-short-links-heres-you-verify-destination-url-before-clicking-0139644/)). If you're still doubtful, go directly to the main website and login the way you usually do.
* Phishing isn't only done through email. It can be any link on any website / chat room / text message / etc. Even ads that pop up can be malicious. Don't click on any sketchy looking links that ask for your information.
* Use anti-virus & web security software, like Norton or McAfee.

**Method 4: Stealing Cookies**

Cookies allow a website to store information on a user's hard drive and later retrieve it. These cookies contain important information used to track a session that a hacker can sniff out and steal if they are on the same Wi-Fi network as the victim. They don't actually get the login passwords, but they can still access the victim's account by cloning the cookies, tricking Facebook into thinking the hacker's browser is already authenticated.

[](http://img.wonderhowto.com/img/original/60/09/63484948356086/0/634849483560866009.jpg)

Image via [wikimedia.org](http://wikimedia.org)

[Firesheep](http://tag.wonderhowto.com/firesheep/) is a Firefox add-on that sniffs web traffic on an open Wi-Fi connection. It collects the cookies and stores them in a tab on the side of the browser.

From there, the hacker can click on the saved cookies and access the victim's account, as long as the victim is still logged in. Once the victim logs out, it is impossible for the hacker to access the account.

[](http://img.wonderhowto.com/img/original/62/55/63491554066136/0/634915540661366255.jpg)

**A Couple More Facebook Hacks**

For those with a bit more technical skill, check out the [Same Origin Policy Facebook hack](http://null-byte.wonderhowto.com/how-to/hack-like-pro-hack-facebook-part-1-same-origin-policy-0159452/) and the somewhat easier, [Facebook Password Extractor](http://null-byte.wonderhowto.com/how-to/hack-like-pro-hack-facebook-part-2-facebook-password-extractor-0160523/). We will continue add more Facebook hacks in the near future, so keep coming back here.

**How to Protect Yourself**

* On Facebook, go to your **Account Settings** and check under **Security**. Make sure Secure Browsing is enabled. Firesheep can't sniff out cookies over encrypted connections like HTTPS, so try to steer away from HTTP.
* Full time SSL. Use Firefox add-ons such as [HTTPS-Everywhere](https://www.eff.org/https-everywhere) or [Force-TLS](https://addons.mozilla.org/en-US/firefox/addon/12714/).
* Log off a website when you're done. Firesheep can't stay logged in to your account if you log off.
* Use only trustworthy Wi-Fi networks. A hacker can be sitting across from you at Starbucks and looking through your email without you knowing it.
* Use a VPN. These protect against any sidejacking from the same WiFi network, no matter what website you're on as all your network traffic will be encrypted all the way to your VPN provider.

**Protecting Yourself: Less Is More**

Social networking websites are great ways to stay connected with old friends and meet new people. Creating an event, sending a birthday greeting and telling your parents you love them are all a couple of clicks away.

Facebook isn't something you need to steer away from, but you do need to be aware of your surroundings and make smart decisions about what you put up on your profile. The less information you give out on Facebook for everyone to see, the more difficult you make it for hackers.

If your Facebook account ever gets hacked, check out our guide on [**getting your hacked Facebook account back**](http://hacked-facebook.wonderhowto.com/how-to/get-your-hacked-facebook-account-back-0147366/) for information on restoring your account.

Bonus: If you're interested in who's checking you out, there are some ways you can (kindof) [**track who's viewed your Facebook profile**](http://internet.wonderhowto.com/how-to/track-who-views-your-facebook-profile-0147349/).

Welcome back, my aspiring hackers!

In many of my earlier tutorials, I mentioned the complementary nature of hacking and forensics. Both disciplines, hacking and [forensics](http://null-byte.wonderhowto.com/how-to/forensics/), benefit from a knowledge of the other. In many cases, both disciplines will use the same tool. In this tutorial, we will use another tool that can be used in either discipline—Sysinternals—a suite of tools developed by Mark Russinovich.

These tools proved so effective that Microsoft purchased them in 1996 and continues to [provide them](https://technet.microsoft.com/en-us/sysinternals/bb545021.aspx) free of charge. Originally, they were all command line tools, but since Microsoft purchased them they have put some pretty GUIs on many of the tools.

These are some of the best tools for in-depth analysis of a system. They can be excellent for doing onsite forensics of a live system or incident response analysis of a system you suspect has been hacked. For the hacker who can get physical access to a system or upload these tools to a system, it can provide invaluable information on the potential target.

Windows Sysinternals is particularly useful when we suspect a system has been hacked and we are trying to understand what processes the malware is using and how it is operating.

**Step 1: Install Sysinternals**

As I mentioned earlier, Microsoft provides Windows Sysinternals for free, and you can [download it here](https://technet.microsoft.com/en-us/sysinternals/bb842062.aspx). Once you have install it, you can look in the SysinternalsSuite folder and see the numerous tools available. Here is a list of the tools (in alphabetical order) and their function.

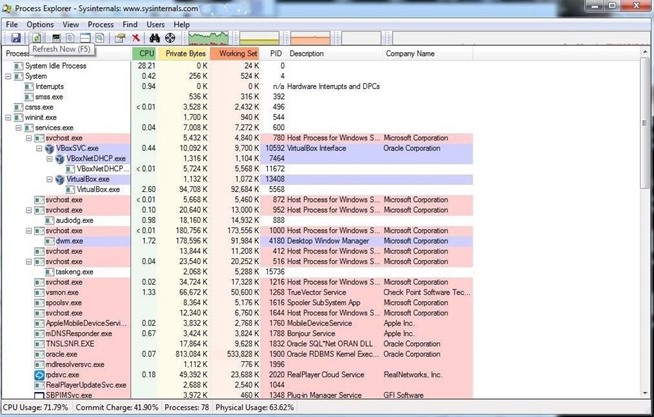
* **AccessChk** - Lets you see what type of access users and groups have to files, directories, registry keys, etc.
* **AccessEnum** - Full view of your file system and registry security settings.
* **AdExplorer** - Active Directory viewer and editor.
* **AdInsight** - LDAP real-time monitoring tool used to troubleshoot Active Directory applications.
* **AdRestore** - Ability to restore deleted Active Directory objects.
* **Autologon** - Easily configure autologon mechanism.
* **Autoruns** - Displays programs that are configured to run at startup.
* **BgInfo** - Displays relevant information about the computer on the desktop, such as computer name, IP address, etc.
* **CacheSet** - An applet to manipulate the working-set parameters of the system file cache.
* **ClockRes** - Shows the resolution of the system clock.
* **Contig** - Defragments a specified file or files.
* **Coreinfo** - Shows you the mapping between logical processors and the physical processor.
* **Ctrl2Cap** - Kernel-mode device driver that filters the system's keyboard class driver.
* **DebugView** - Monitors debug output on your local system.
* **Desktops** - Allows you to organize up to four virtual desktops.
* **Disk2vhd** - Creates VHD (virtual hard disk) versions of physical disks.
* **DiskExt** - Returns information about what disks the partition of a volume is located on.
* **DiskMon** - Logs and displays all hard disk activity.
* **DiskView** - A graphical map of your hard drive.
* **DiskUsage (DU)** - Reports the disk space usage for a specified directory.
* **EFSDump** - Allows you to see who has access to encrypted files.
* **FindLinks** - Reports the file index and hard links that exist for a specified file.
* **Handle** - Displays information about open handles for any process.
* **Hex2dec** - Converts hex to decimal and vice versa.
* **Junction** - Creates junctions (symbolic links that combine directories from multiple locations).
* **LDMDump** - Let's you examine exactly what is stored in a disks copy of the system.
* **ListDLLs** - Reports the DLLs that are loaded into processes.
* **LiveKd** - Allows you to run the Kd and Windbg kernel debuggers.
* **LoadOrder** - Shows the order in which the system loads device drivers.
* **LogonSessions** - Lists currently active logon sessions.
* **MoveFile** - Dumps the content of the pending rename/delete value.
* **NTFSInfo** - Shows you information about NTFS volumes.
* **PageDefrag** - Shows you have fragmented your paging files and registry hives are.
* **PendMoves** - Dumps the content of the pending rename/delete value.
* **PipeList** - Lists the pipes.
* **PortMon** - Monitors and displays all serial and parallel port activity.
* **ProcDump** - Monitors CPU spikes.
* **Process Explorer** - Shows information about which handles and DLL processes are loaded.
* **Process Monitor** - Shows real-time file system, registry, and process/thread activity.
* **PsExec** - Allows you to execute processes on remote systems.
* **PsGetSid** - Allows you to translate SIDs to their display name and vice versa.
* **PsInfo** - Gathers key information about the local or remote system including kernel build and the amount of memory.
* **PsPing** - Implements ping functionality.
* **PsKill** - Can kill processes on local and remote systems.
* **PsList** - Displays information about processes, memory, and threads.
* **PsLoggedOn** - This shows who is using what resources on a local or remote machine.
* **PsLogList** - Allows you to login to remote systems in situations where security credentials do not permit it.
* **PsPasswd** - Allows you to change an account password on local or remote systems.
* **PsService** - A service viewer and controller for Windows.
* **PsShutdown** - Allows you to logoff the console user or lock the console among other things.
* **PsSuspend** - Allows you to suspend processes on the local or a remote system.
* **RAMMap** - A physical memory usage analysis tool to see how Windows is assigning physical memory.
* **RegDelNull** - Allows you to search for and delete registry keys.
* **Registry Usage (RU)** - Reports the registry space usage.
* **RegJump** - Opens [Regedit](http://null-byte.wonderhowto.com/how-to/hack-like-pro-digital-forensics-for-aspiring-hacker-part-5-windows-registry-forensics-0160561/) directly to a specified registry path.
* **RootkitRevealer** - Detects rootkits.
* **SDelete** - Allows you to delete one or more files/directories or to cleanse the free space on a drive.
* **ShareEnum** - Allows you to lock down file shares.
* **ShellRunas** - Allows you to launch programs under different accounts.
* **SigCheck** - Shows file version number, timestamp, and digital signature details.
* **Streams** - Allows you to see which NTFS files have alternate streams associated with them.
* **Strings** - Searches files for a specified string.
* **Sync** - Allows you to flush all file system data to disk.
* **TCPView** - Shows detailed listings of all TCP and UDP endpoints on your system.
* **VMMap** - A process virtual and physical memory analysis tool.
* **VolumeID** - Allows you to change the IDs of FAT and NTFS disks.
* **WhoIs** - Performs a registration record for the specified domain name or IP address.
* **WinObj** - Displays information of the NT Object Manager's name space.
* **ZoomIt** - A screen zoom and annotation tool for technical presentations.

As you can see from this list, there are some very powerful tools in this suite. Let's examine one of the most useful tools in this toolkit, Process Explorer.

**Step 2: Open Process Explorer**

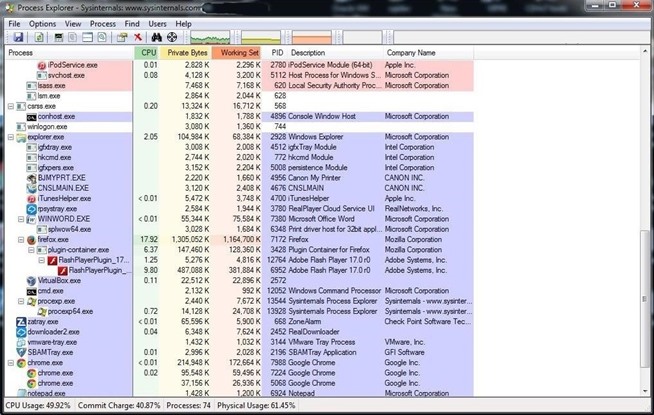
In terms of digital forensics, Process Explorer can be one of the most useful Sysinternals tools. Simply click on the procexp icon in the SysinternalsSuite folder to get started.

Process Explorer lists each and every process and its child processes, its CPU use, private bytes, working set, PID, description, and company. If we suspect a malware infection, we can often find evidence of it in the Process Explorer as you can see below.

[](http://img.wonderhowto.com/img/original/04/96/63568853399767/0/635688533997670496.jpg)

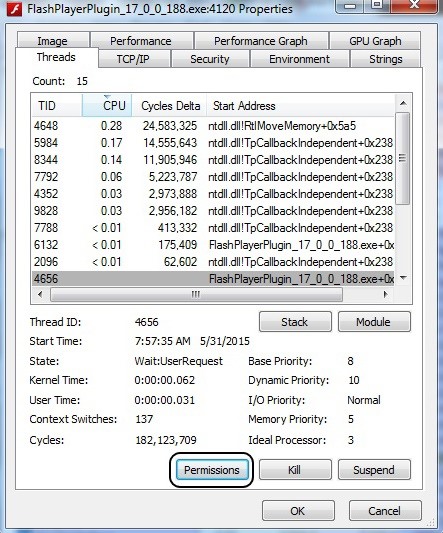
**Step 3: Use Process Monitor to Examine a Process**

Let's examine one process a bit closer. About two-thirds of the way down the following screenshot, you will see the Flash plug-in process which I suspect has been compromised.

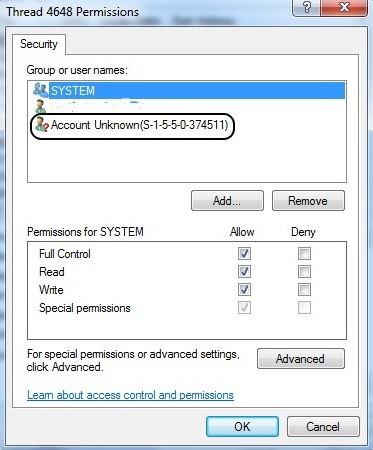
[](http://img.wonderhowto.com/img/original/36/77/63568853503626/0/635688535036263677.jpg)

If you have read my other articles here on Null Byte, you know that I think [Adobe Flash Player](http://null-byte.wonderhowto.com/how-to/hack-like-pro-hacking-windows-xp-through-windows-8-using-adobe-flash-player-0155228/) is probably the worst application for security—and the best application for us hackers. Almost daily, new vulnerabilities and exploits are found in Flash Player.

Let's double-click on it and open its properties. As you can see in the screenshot below, this window reveals numerous properties of the selected process.

[](http://img.wonderhowto.com/img/original/13/79/63568853747095/0/635688537470951379.jpg)

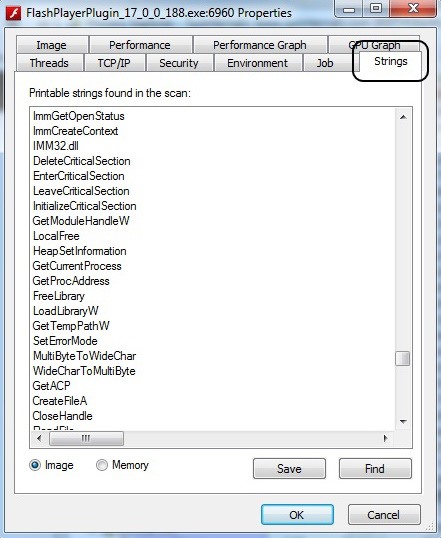
Now, we can click on Permissions to see who has permissions of this process. Notice in the screenshot below that besides System and the user (which I have obscured), an Unknown Account has permissions to use this process. Very suspicious! This would seem to warrant further investigation.

[](http://img.wonderhowto.com/img/original/17/23/63568853811220/0/635688538112201723.jpg)

**Step 4: Check Strings**

Among the many bits of information we can glean from the process, we can extract any ASCII strings embedded in this process. Often, we can find key information about the process including any comments the developers left. Remember that when the FBI released the evidence against North Korea in the [Sony hacking case](http://null-byte.wonderhowto.com/how-to/advice-from-real-hacker-why-im-skeptical-north-korea-hacked-sony-0159332/), they cited comments within the malware code. This is one way they can extract those "strings."

While in the properties window of Flash, we can simply click on the Strings tab to see any ASCII text within the process.

[](http://img.wonderhowto.com/img/original/29/18/63568853887923/0/635688538879232918.jpg)

The Sysinternals suite of tools can be a very powerful for examining the inner workings of a Windows system and its processes. It's worth investing the time of any digital forensic investigator, hacker, or system administrator in understanding these extraordinarily useful tools. In future tutorials, we will work some of the other Sysinternals tools, so keep coming back, my aspiring hackers!

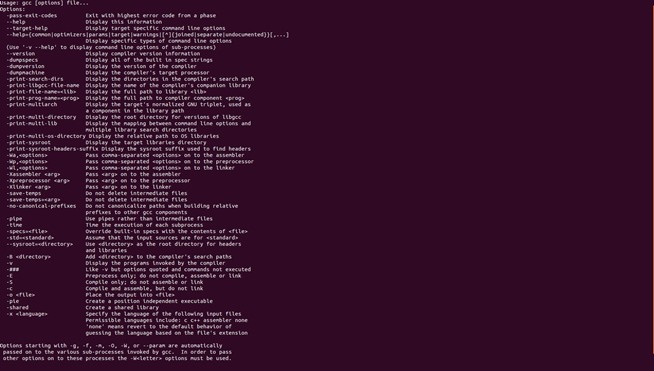
Hello my fellow hackers! Since i am new here, i'd first like to introduce myself: i am Phoenix750, a 15 year old passionated hacker who likes to share everything he knows with other people of my kind. I have been reading null byte for quite some time now, but only could register today. I truely love how this community respects newcomers, But even after reading a lot of tutorials on here, i never came accross a good programming tutorial (except the scripting tutorials, but scripting isn't programming. I'll talk about that later). There are forum questions about it, but not really a decent series of tutorials. **So i decided to write them to help the newcomers!** So, with my introduction out of the way, let's get started!

**What You Will Need Before We Begin**

1. **A Linux operating system.** i am going to use Ubuntu in these series. you can use any other Linux distro or even Windows if you know how to setup the GNU/GCC compiler for that operating system. but i still recommend Ubuntu because GCC comes preinstalled on it. I will only talk about the install instructions for Ubuntu (thoughh they should be the same for Kali aswell).
2. **The GNU/GCC compiler.** this is the compiler that we will use to build our programs. if you do not know what a compiler is, a compiler is simply said a program that turns our programming code (C, C++, Java...) into machine code (1's and 0's). to Check if you have GCC installed, just type the following in a terminal:

**gcc --help**

this should produce an output like this:

[](http://img.wonderhowto.com/img/original/03/28/63568632858142/0/635686328581420328.jpg)

If you have a "command not found" error, then you must type this in your terminal, and it should begin installing.

**apt-get update && apt-get install gcc -y**

1. **A text editor.** this can be any text editor, but i will use the default one in Ubuntu.

**Why Programming Is Important for Hackers to Know.**

Programming is an important skill that every self respecting hacker should master. here are some good examples of why it is important:

* **Building your own malware.** When you program your own malware, there is no signature for it registered, thus making it pretty much impossible for AV software to detect.
* **Knowing how programs work will help you exploit them.** though most exploit development is done in the assembly language in debuggers, knowing how a program works will help you exploit it faster.
* **Hacking tools are mostly open source.** most hacking tools are open source, which means everyone can access the source code of said program. when you know how to program in the language the program is written, you can edit it and make it even better!
* **Making your own exploits.** Though i recommend ruby & the Metasploit Framework for this purpose, ruby is still quite slow compared to C or C++. if you need your exploit to be fast, you can write it in C/C++.

i chose to make a series about C/C++ because C++ is a powerful language and is used in a lot of programs, like games. C is less powerfull but is still quite a low-level language, which means it interacts closely with the CPU. embedded devices are usually programmed in C aswell, from traffic lights to your microwave, will most likely run on some kind of software that is written in C.

**What Will We Be Doing in This Series?**

# [The Novice Guide to Teaching Yourself How to Program (Learning Resources Included)](http://null-byte.wonderhowto.com/how-to/novice-guide-teaching-yourself-program-learning-resources-included-0131969/)

Today's post is a small go-to guide for beginner programmers in Null Byte. With many of our community members picking up programming from our [Community Bytes](http://null-byte.wonderhowto.com/blog/goodnight-byte-hackthissite-walkthrough-part-5-legal-hacker-training-0132051_146288/), it only makes sense to lay out a one-stop guide for your reference. Hopefully this guide will help you make an educated and thoughtful choice on what programming languages you want to learn, and how you want to learn said languages.

The question has come up [in the forums](http://null-byte.wonderhowto.com/forum/languages-learn-1728/) already. What programming languages should I learn? Well, a good friend of Null Byte once said that a programmer should learn a compiled language, an interpreted or high-level language, a scripting language, and machine code.

If you are very new to all of this, I bet you're asking, *"What do these types of languages even mean and why should I learn so many?"*. To answer that, I'll need to explain what each kind of language really is, and list examples of each. From there, I will guide you to great resources to learn the languages that pique your interest.

**I Want to Learn How to Hack! Why Is There So Much Programming?**

Hacking and programming are nearly one in the same. Don't get me wrong, there is a lot more to hacking than just code. However, when you learn how to code, you are taking the computer and making it do what *you* want. You are learning what makes it tick. Only then, when you understand how things work, you will have found that you have already become a hacker.

**Note:** If you need to make a programming environment for yourself, check out this [great guide](http://null-byte.wonderhowto.com/blog/coding-basics-guide-choosing-your-optimal-text-editor-ide-0131745/) from Null Byte.

**Types of Languages & Free Resources to Learn**

**Binary**

The mother of computer languages, binary is as simple as it gets (in terms of logic, not actual simplicity). The 1's and 0's that make up binary represent a boolean integer for *on* and *off*. These are grouped into octets called *bytes*. Each byte can be up to 256 different combinations (0-255). These are assigned registers and values, and are interpreted by computer programs.

**Binary Resources**

* Here is a simple [binary tutorial](http://www.math.grin.edu/%7Erebelsky/Courses/152/97F/Readings/student-binary). It will provide all you need to understand the basics. It's far simpler than you may think.

**Machine Code**

Machine code (or assembly) is code that speaks directly to the hardware. Each processor type has an [instruction set](http://en.wikipedia.org/wiki/Instruction_set) that it uses to understand commands given to it. This results in code that can be executed with nearly 0 latenecy. Programs execute as fast as your processor capabilities allow when you program machine code using [assembly](http://en.wikipedia.org/wiki/Assembly_language).

**Machine Code Resources**

* A great book to read, especially if you are new to programming and assembly, is [Programming from the Ground Up](http://www.exactas.org/modules/UpDownload/store_folder/1_-_COMPUTACION/Jonathan%20Bartlett%20-%20Programming%20From%20The%20Ground%20Up.pdf). This book will help you understand how computers work, as well as their processors. Then it takes you into coding in ASM assembly.

**Compiled Languages**

Compiled languages are languages that are written in a code syntax, such as C/C++. They are run through a compiler, which turns them into machine code executables. This may make you wonder why we even use assembly. Well, an elite hacker who is a mentor of mine has always taught me that the compiler takes shortcuts—and for perfect, fast, clean code, you must code it yourself and "outsmart" the compiler.

**C/C++**

Considered a mid-level languate, C/C++ is probably the most popular programming language and usually the most favored among skilled coders. It is very fast, but can be hard to understand. You probably shouldn't start with this.

**C/C++ Resources**

* A great beginner book that is up-to-date is [*C Programming: A Modern Approach - Second Edition*](http://www.amazon.com/C-Programming-Modern-Approach-2nd/dp/0393979504)*.*
* Also, commonly considered to be one of the greatest programming books ever written, check out [The C Programming Language](http://pelusa.fis.cinvestav.mx/tmatos/LaSumA/LaSumA2_archivos/Supercomputo/The_C_Programming_Language.pdf). It was written by the creator of the C programming language (RIP, Dennis Ritchie).
* Videos from [LearnToProgramDotTV](http://www.youtube.com/user/LearnToProgramDotTV).

**Haskell**

Haskell is strange, but the people who learn it tend to be very amazing programmers. It is a [purely functional](http://en.wikipedia.org/wiki/Purely_functional) language, which means that in general, functions in Haskell do not have [side effects](http://en.wikipedia.org/wiki/Side_effect_%28computer_science%29). There is a distinct type for representing side effects, [orthogonal](http://en.wikipedia.org/wiki/Orthogonal#Computer_science) to the type of functions. A pure function may return a side effect, which is subsequently executed, modeling the impure functions of other languages.

**Haskell Resources**

* There is a [beautiful answer](http://stackoverflow.com/questions/1012573/how-to-learn-haskell) on this Stack overflow page on how to go about learning Haskell.

**Java**

Java is a great language. Comparable in ways to C/C++, Java uses its own interpreter and compiler that runs across all operating systems to execute its byte code. This mean it is completely portable. Java is also a very fast and lower-level language, so it's great to have in your arsenal. Many jobs hire programmers with experience in Java.

**Java Resources**

* [Java from the Ground Up](http://www.javaworld.com/javaworld/jw-03-2000/jw-0331-java101.html) offers a huge variety of tutorials on Java. Great for beginners.
* [JavaVideoTutes](http://www.javavideotutes.com/) has many great videos, for those who learn better via video.

**Interpreted Languages**

Interpreted languages are languages that are commonly scripted and then run through an interpreter. The interpreter processes the script as machine code. This allows code to be short and elegant, but takes up a lot more precious resources.

**Python**

My personal favorite, Python is a fast, simple, clean and user-friendly programming language that focuses on user readability. This makes learning Python easy and very fun.

**Python Resources**

* [How to Think Like a Computer Scientist, Python](http://greenteapress.com/thinkpython/thinkCSpy.pdf) is a great book to get started in Python. It gives you analytical tips on tackling tough programming problems. Even a little bit of artificial intelligence is taught at the end where you make a program that *actually* learns!
* [TheNewBoston](http://thenewboston.org/) has tons of great vTutorials that will walk you through learning Python.
* [Learning Python](http://nqnwebs.com/IMG/pdf/OReilly-Learning-Python-4th-Edition-Oct-2009.pdf) takes you from the beginning of learning Python, to the elite. It is a very long, but complete book to becoming a sage with Python.
* [DiveIntoPython](http://www.diveintopython.net/) is a pre-exposed programmers tutorial for Python. If you can trudge through it and understand it as a beginner, this is by far the best way to learn the language. The book teaches perfect coding habits and syntax, right up-to-par with the Python standards.

**Perl**

Perl is similar to Python in many ways. Its syntax is slighty more difficult, and it is less powerful than Python in some areas. For that, I reccommend only learning it to read and hack other coders' Perl scripts.

**Perl Resources**

* The [Perl website](http://learn.perl.org/) has a free book and loads of other resources right there, which also happen to be some of the best.
* [Learning Perl](http://chapman.christscollege.com/oreilley/%20Learning%20Perl%203rd%20Edition.pdf) is an extensive book and Perl's counterpart to its *Learning Python* cousin.

**PHP**

PHP is an important language on the internet. Nearly every website uses this language to perform scripted tasks, such as parsing information from a database. It can also be used to code fun things like IRC bots! Learning PHP is essential to learn if you want to be a hacker, because most websites on the internet use PHP, and to exploit it, we must learn it.

**Resources**

* [The official PHP documentation](http://php.net/manual/en/index.php) is the best place to learn PHP, in my opinion. Learning from something like the PHP bible can be far too overwhelming, and a lot of the information provided could be irrelevant to beginners, or make little to no sense.

**Ruby**

Ruby is a [dynamic](http://en.wikipedia.org/wiki/Dynamic_programming_language), [reflective](http://en.wikipedia.org/wiki/Reflection_%28computer_science%29), general purpose [object-oriented programming language](http://en.wikipedia.org/wiki/Object-oriented_programming_language). It is a popular language to learn and was also used to code the [Metasploit](http://metasploit.com/) framework and many of its payloads.

**Resources**

* The [Ruby Learning](http://rubylearning.com/) site has some great information that you can use to learn to code in Ruby, but it costs money. However, the best choice in my opinion, would be [Learn Ruby the Hard Way](http://ruby.learncodethehardway.org/). This is an awesome, free learning resource to go from programming newbie, to Ruby-ninja.

**Shell**

Learn BASH/ plain and simple. Windows users rarely need to use the terminal. However, Mac and Linux users can benefit on a large scale if we all got together and learned the terminal. This can make repetitive takes a cinch with a script! If you have a webhost, it is likely they will run Linux, so why not make your life easier and just learn it now?

**Resources**

* The best guide to BASH and just managing your computer from the terminal would probably have to be [The Rute User Tutorial](http://www.linux-books.us/gnoppix_0001.php). I really can't stress how great this book is, so please do not forget to pick it up if you plan on learning shell commands.

If you have any questions about programming, ping me, or any of the other helpful people on Null Byte!

**Get Involved!**

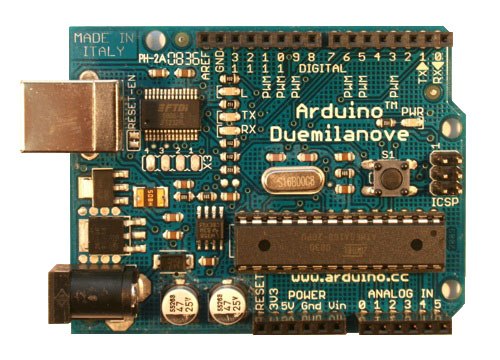
In this article, I'll be explaining the basics of how microcontrollers work, physically and virtually. First off, microcontrollers are no simple thing, so don't be discouraged if you find it mind-boggling! The world of microcontrollers is fascinating, engaging, and an awesome hobby; it never gets boring. I'll be focusing more on I/O and analog based microcontrollers, such as those running [*Arduino*](http://en.wikipedia.org/wiki/Arduino)*,* and using Atmel chips as examples (these are most commonly available, and easy to program).

[](http://img.wonderhowto.com/img/original/21/31/63471558750049/0/634715587500492131.jpg)

A common ATmega328 microcontroller, used in the Arduino unit depicted below.

**What Is a Microcontroller?**

A microcontroller is a silicone-based computer chip (or [*integrated circuit*](http://en.wikipedia.org/wiki/Integrated_circuit)), that is programmed with a set of instructions. These instructions can range from as simple as blinking an LED, to dealing with mass amounts of data from a serial connection. The size of the microcontroller generally depends on the amount of pins and [*flash memory*](http://en.wikipedia.org/wiki/Flash_memory). For beginners, I'd recommend purchasing the [Arduino Duemilanove](http://arduino.cc/en/Main/arduinoBoardDuemilanove), as it is inexpensive ($30) and very easy to use.

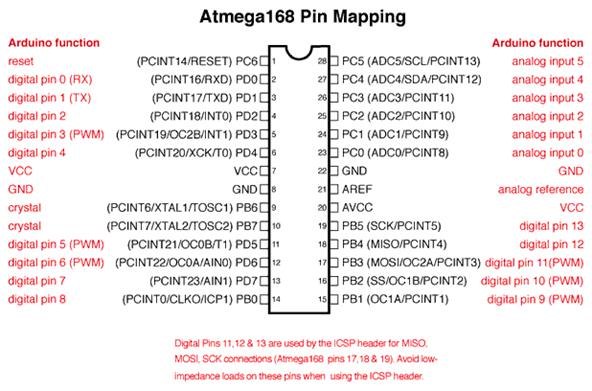
[](http://img.wonderhowto.com/img/original/54/86/63471432459797/0/634714324597975486.jpg)

Advanced microcontroller users typically write their programs in C, then compile the finished script to a hex (hexadecimal) format. Finally, using a serial cable and AVR (or similar) programming software, users write or flash the data onto the chip itself through the SCK, MOSI, MISO, and RESET pins of the microcontroller (referred to as the SPI, or [Serial Peripheral Interface Bus](http://en.wikipedia.org/wiki/Serial_Peripheral_Interface_Bus)).

In the case of Arduino, the ATmega chip on the board itself contains a "bootloader", which understands and programs data through the [UART](http://en.wikipedia.org/wiki/Universal_asynchronous_receiver/transmitter), which is basically a telephone line between the computer and the board, the bootloader being the interpreter and recorder. The little silver rectangle (rounded edges) is a [quartz crystal oscillator](http://en.wikipedia.org/wiki/Crystal_oscillator), which generates a frequency (in this case, 16 MHz). For accurate and precise serial communication, an external oscillator is practical.

[](http://img.wonderhowto.com/img/original/20/43/63471433060882/0/634714330608822043.jpg)

AVR microcontrollers without a bootloader must be programmed through the SPI, as described above. All microcontrollers (at least, those with datasheets) have a pinout schematic and pin description. For example, below is the pinout and description for the ATmega328 described above.

[](http://img.wonderhowto.com/img/original/69/36/63471558795897/0/634715587958976936.jpg)

The VCC is the positive power input (5V) and GND is the negative (or ground). Pins 17, 18, and 19 are used by the SPI to program the chip, if it does not have a bootloader. Digital pins are capable of both I and O interfaces, in other words, they can either output power (ex. light an LED), or receive power (ex. identify if a switch is at a high or low state/on or off).

Analog pins are more complicated, as they collect multiple forms of data over a large span of voltage readings. For example, analog pins can determine "digital" specific voltage being inputted.

The AREF pin (21, analog reference) is used as the max value, or highest value measured, represented by the digital value 1023. Any values in between 0 and the reference voltage are represented with values between 0 and 1023.

**Warnings**

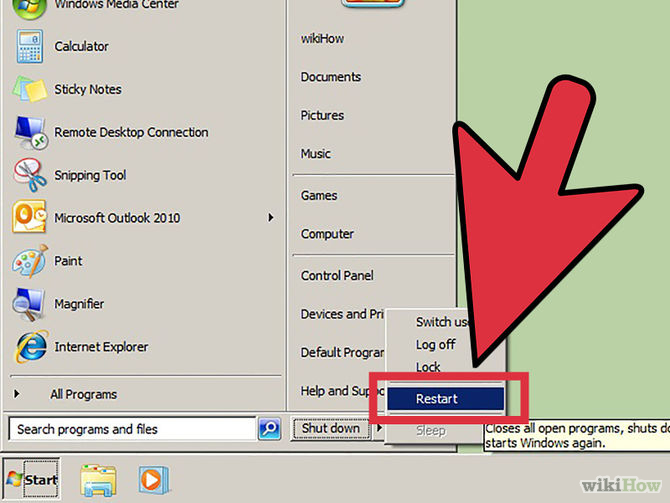
* Microcontrollers can fry very easily! Ensure that you NEVER insert/attach with incorrect polarity, or to incorrect pins.
* Microcontrollers are sensitive to static electricity, always employ static-protection (grounded wristband).
* Microcontrollers are FRAGILE! Treat them with care.

Now,[head on over to part two](http://fear-of-lightning.wonderhowto.com/how-to/hardware-hackers-introduction-microcontrollers-part-two-does-arduino-think-0141262/), which digs deeper into the mysteries of microcontroller programming!

# [How to Crack a Windows 7 Password](http://www.wikihow.com/Crack-a-Windows-7-Password)

Windows 7 is a very secure and powerful operating system for your home computer, which allows you to create a password to secure your user account. But, what if you forget it, and you don't have a Reset Disk, password cracking program or anything else which would help you retrieve it? Well, follow those simple steps below and you will have your password reset in no time!

## Steps

1. [](http://www.wikihow.com/Crack-a-Windows-7-Password#/Image:Crack-a-Windows-7-Password-Step-1-Version-3.jpg)

1

**Start (or restart) your computer.** You can do this by clicking the reset button in the Windows 7 Login Prompt or pressing the On/Off button on your computer.

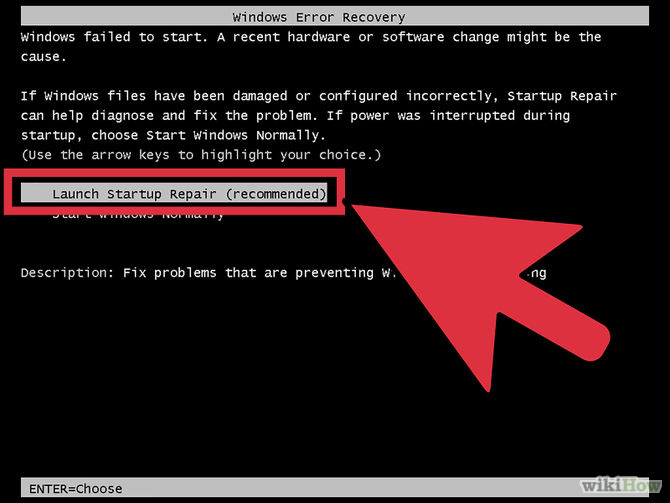
Ad

1. 2

**Make Windows 7 have a hard shutdown.** Complete this step by pressing the On/Off button on your computer while the "Starting Windows" screen is active.

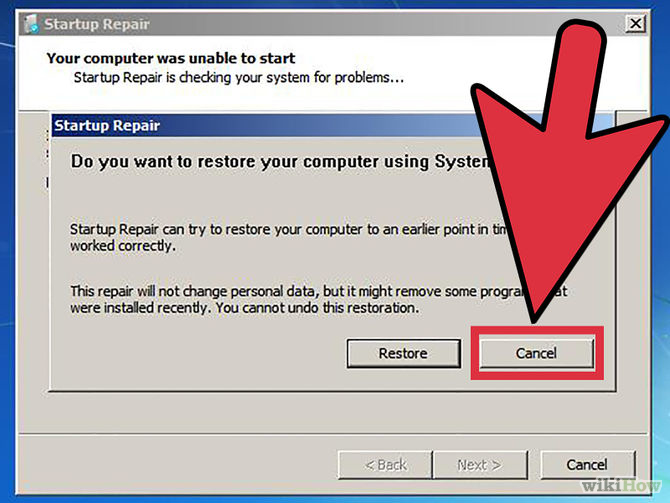
1. 3

**Start your computer again.** Same, complete this task by pressing the On/Off button on your computer.

1. [](http://www.wikihow.com/Crack-a-Windows-7-Password#/Image:Crack-a-Windows-7-Password-Step-4-Version-4.jpg)

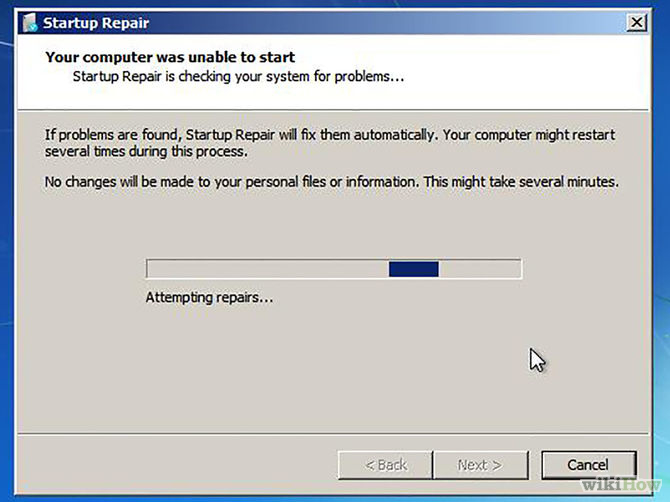
4

**Select the "Launch Start up Repair" option.** If you completed steps 1, 2 and 3 correctly, you will be given to options on how to start your computer: normally or using the Start up Repair. You should select the Start up Repair option.

1. [](http://www.wikihow.com/Crack-a-Windows-7-Password#/Image:Crack-a-Windows-7-Password-Step-5-Version-4.jpg)

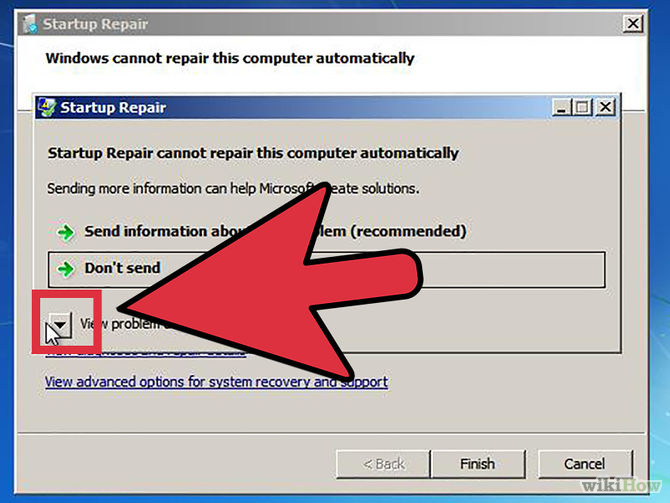
5

**Cancel the "Do you want to use System Restore?**" prompt. After you've launched Start up Repair, a prompt will pop up on your screen. You will want to select "Cancel".

1. [](http://www.wikihow.com/Crack-a-Windows-7-Password#/Image:Crack-a-Windows-7-Password-Step-6-Version-4.jpg)

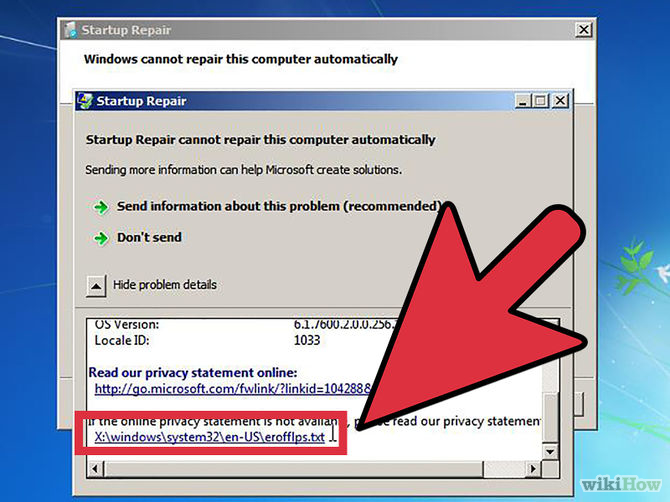
6

**Wait until Windows has finished repairing your computer.** After completing Step 5, you will have to wait. The repairing process will not harm any of your personal files.

1. [](http://www.wikihow.com/Crack-a-Windows-7-Password#/Image:Crack-a-Windows-7-Password-Step-7-Version-4.jpg)

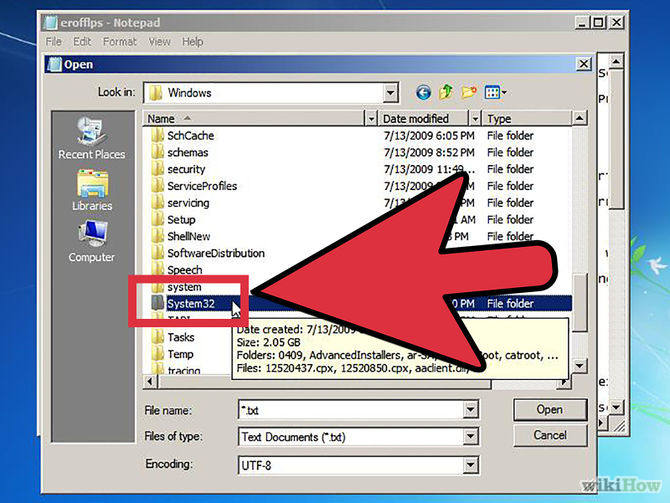
7

**Click the arrow in the bottom-left corner of the window.** After waiting, a window saying "Start up Repair could not repair your computer." You will see an arrow pointing downwards in the bottom left corner (Problem Details).

1. [](http://www.wikihow.com/Crack-a-Windows-7-Password#/Image:Crack-a-Windows-7-Password-Step-8-Version-4.jpg)

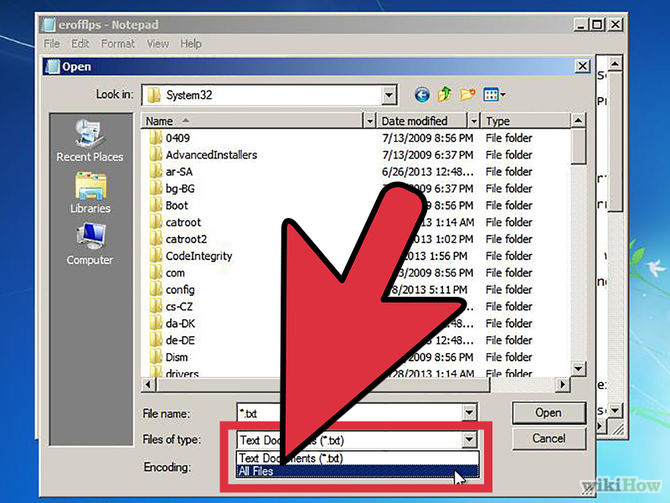
8

**Scroll down and click the last link.** After Step 7, a window will pop up displaying the Problem Details. Scroll down until you see links. Ignore the first one, click the second one.

1. [](http://www.wikihow.com/Crack-a-Windows-7-Password#/Image:Crack-a-Windows-7-Password-Step-9-Version-4.jpg)

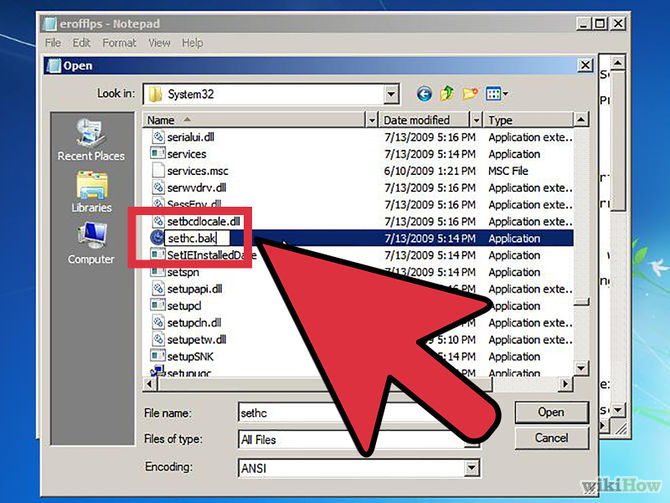
9

**File > Open > Computer > Local Disk > Windows > System32.** After completing Step 8, Notepad will open up. You will want to follow the route displayed in bold.

1. [](http://www.wikihow.com/Crack-a-Windows-7-Password#/Image:Crack-a-Windows-7-Password-Step-10-Version-4.jpg)

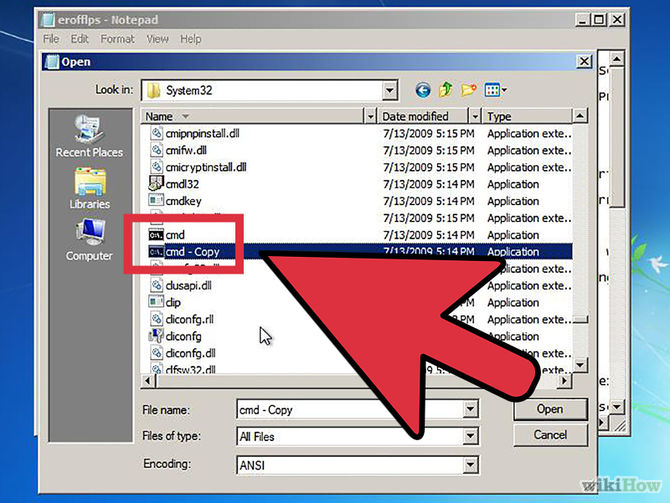
10

**Switch from Text Documents (\*.txt) to All Files.** You can do this by simply clicking the drop-down menu, displayed as Text Documents (\*.txt) and select All Files.

1. [](http://www.wikihow.com/Crack-a-Windows-7-Password#/Image:Crack-a-Windows-7-Password-Step-11-Version-4.jpg)

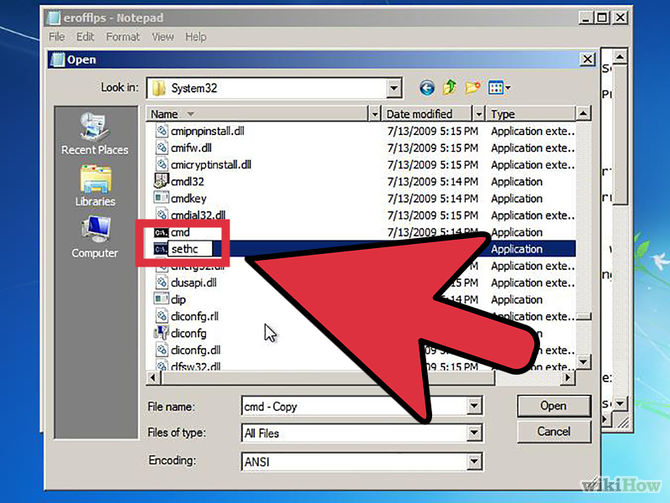
11

**Find the application named sethc and rename it to sethc-bak.** Sethc is the application for the Sticky Keys program. You have to rename it to sethc-bak as a backup file. This won't do any harm to your computer or personal files.

1. [](http://www.wikihow.com/Crack-a-Windows-7-Password#/Image:Crack-a-Windows-7-Password-Step-12-Version-4.jpg)

12

**Find the application named cmd and copy & paste it into the folder System32 (the one you're in right now).** Cmd is the application known as Command Prompt. After this, you will have a file named cmd - Copy in the System32 folder.

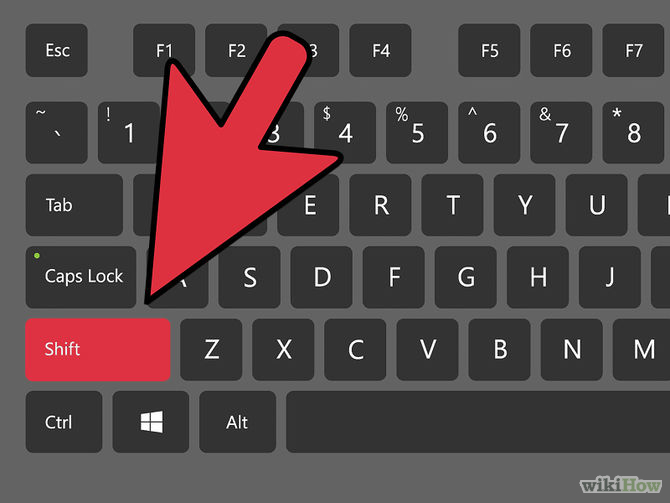
1. [](http://www.wikihow.com/Crack-a-Windows-7-Password#/Image:Crack-a-Windows-7-Password-Step-13-Version-4.jpg)

13

**Rename cmd - Copy to sethc.** To be able to access cmd without permission from Windows, you will need to trick Windows thinking it is Sticky Keys.

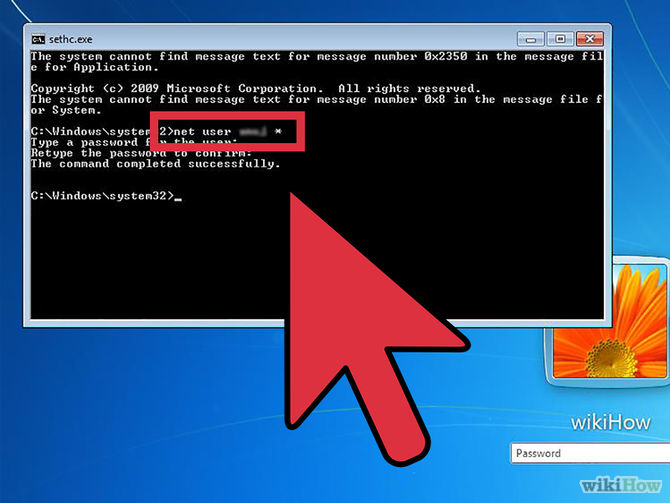
14

**Close all opened windows and select "Finish".** You're done! Now you just need to close out of all the opened windows and restart your computer.

1. [](http://www.wikihow.com/Crack-a-Windows-7-Password#/Image:Crack-a-Windows-7-Password-Step-15-Version-4.jpg)

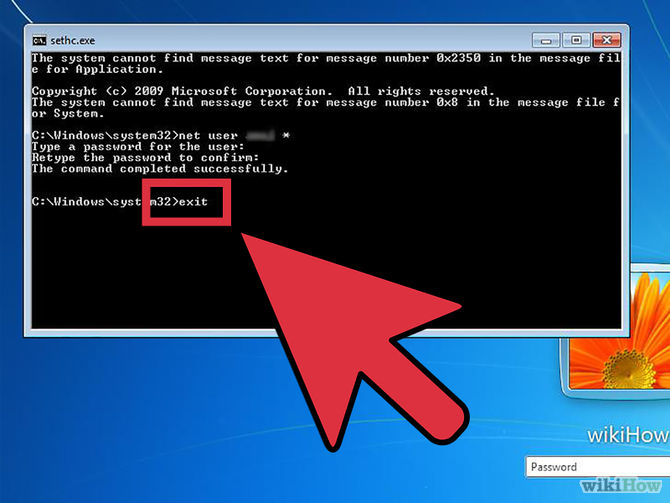
15

**Hit Shift 5 times.** After successfully restarting your computer, hit Shift on your keyboard 5 times. Command Prompt with administrator privileges opens up!

1. [](http://www.wikihow.com/Crack-a-Windows-7-Password#/Image:Crack-a-Windows-7-Password-Step-16-Version-4.jpg)

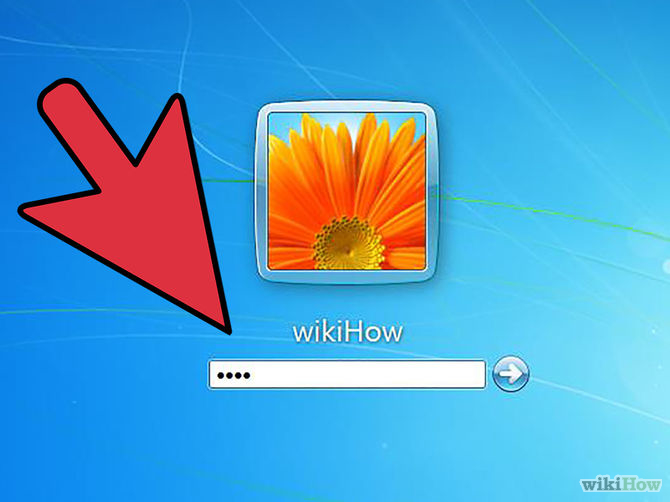
16

**net user [username] \*.** Enter this code into the command prompt to change the [username]'s password. You will not be able to see the new entered password, so enter it wisely.

1. [](http://www.wikihow.com/Crack-a-Windows-7-Password#/Image:Crack-a-Windows-7-Password-Step-17-Version-4.jpg)

17

**Close Command Prompt.** After you've successfully changed the user's password, you can now close cmd.

1. [](http://www.wikihow.com/Crack-a-Windows-7-Password#/Image:Crack-a-Windows-7-Password-Step-18-Version-4.jpg)

18

**Enter the password you've just set for the user.** After you've entered the password - you're in! This is all you need to do!

### How to Hack Windows 7 Administrator or User Password?

We have already written several windows 7 password recovery tips on this blog. Today we will tell you how to [**hack Windows 7 password**](http://youtu.be/PcamZKfsm2A) if locked out of computer? Yes, there are kinds of Windows 7 password hacker ways with which you can get pass windows 7 login screen even when you forgot windows 7 login password.



### Hack Windows 7 Password without Software

There are 2 types of account on Win 7 by default. There is local account or Windows live or hotmail account. The former stores the login on PC, while the latter connects to the online hotmail or live email id. Here I would like to show you [**Windows 7 password reset**](http://resetwindows7passwords.blogspot.com/) with default Windows 7 administrator account.

#### Tip 1: Hack Windows 7 Login Password with Default Windows 7 Administrator Account

First you need to boot Win 7 in safe mode as it is disabled in normal mode. When you are in safe mode, this default Windows admin account enabled to login Win 7 with a blank password. The you can remove the forgotten user account under users in control panel. Below is step by step guide for you:  
  
1. Press on the F8 key while you start Windows 7 until your PC displays the boot menu.  
2. Select Safe Mode option and press the Enter key  
3. Then a login box appears, click on Administrator in the username box and leave the password field as blank, click on OK to login.  
4. Now you can open Control Panel, then in User Accounts you can reset any user password easily.

#### Tip 2: Hack Password Windows 7 with Password Reset disk

It seems quite simple to hack Windows 7 password if you have Win 7 password reset disk. Assure that you have created it in advance. Otherwise, you change to hack Windows 7 password is over. Now you lost Windows 7 password, it is time for you to find it and use it. It is easy to [**reset Windows 7 password**](http://www.lostwindowspassword.com/article/reset-windows-7-password.html) with it, what you need to do is follow the step by step wizard to create a new login password to the current user.  
  
If the above **Windows 7 password hacker** methods don’t work at all for you, don’t worry. These windows 7 password hacker methods in the above list are helpful, but might be unsuitable for your case. In this condition, you can have a try Windows password reset tool designed for Win 7.

### Hack Forgotten Windows 7 Password with Software

One of the popular **Windows 7 password hacker tool** which is confirmed to replace your forgotten windows 7 password with blank so that you can login without entering any password, it is Windows Password Key. Besides hacking a local account password this tool will also show you how to break main user account password.  
  
Windows Password Key resets any Windows password, such as Windows 8/7/Vista/XP/2012/2011/2008/2003/2000. It can hack domain passwords as well. No matter how complicated your Windows 7 password, Windows Password Key can reset it within 4 minutes. It’s easy to use, whether for beginners or advanced users. And it comes with ready-only and non-destructive designs to make sure it has no data loss on your computer. You can go to its official website to for more information: [www.lostwindowspassword.com](http://www.lostwindowspassword.com/)  
  
  
  
After reading this article, you should have learned **how to hack Windows 7 password** when you forgot or lost the password. If not, read it again. By the way, you can also hack Windows 8/Vista/XP/2012/2011/2008/2003/2000 password as these methods.