Applications utility, troubleshooting, a

KT2001 Upgrade and remove applications from computers

Uninstall

What Does Uninstall Mean?

Uninstall is the process of removing or deleting an application or software from electronic devices such as a personal computer, laptop, smartphone, cellphone, etc. Uninstall helps in removing applications or programs that are not functioning or working properly, are outdated or are not being used anymore. It can also help if extra disk space is needed. However, uninstall, if done improperly, can result in performance issues and problems for the electronic device.

Techopedia Explains Uninstall

Typically, an application includes an uninstall program that can be used to remove the application if the need arises. In fact, this is the recommended way of removing a program or application from a device, as it removes all the configurations, registry information and other files, including the files generated by the program or application to ensure that no conflicts, if any, will occur in the future. In some cases, searching for the application file by means of a file browser can help in uninstalling the application. However, an uninstaller may still be needed to remove all the files, including the orphan files that were not deleted by a manual uninstall.

For electronic devices such as smartphones and tablets, app removers are available that perform a similar functionality to that of an uninstaller. For most operating systems, commands are available at the kernel level for uninstalling applications or programs. The commands and the method of removal vary according to the operating system and, sometimes, to the type of applications. If the program is installed on a Windows operating system, the user can uninstall it from the Control Panel using the "Uninstall a program" option. If this procedure does not work, the user can use the Windows system-restore-

point feature to uninstall an application, which brings the system to its state prior to the installation of the program.

KT2002 New installs through disc or internet download

Installing software on your Windows PC

Your computer allows you to do some really amazing things. Digital photo editing, sophisticated computer gaming, video streaming—all of these things are possible because of different types of **software**. Developers are always creating new software applications, which allow you to do even more with your computer.

Installing from a CD-ROM

From the mid-1990s through the late 2000s, the most common way to get new software was to purchase a CD-ROM. You could then insert the disc, and the computer would walk you through the installation.

Now, almost all software has moved away from this model. Many new computers no longer include a CD-ROM for this reason. However, if you do need to install software from a CD-ROM, simply insert the disc into your computer, then follow the instructions.

Installing software from the Web

Today, the most common way to get new software is to **download it** from the Internet. Applications like Microsoft Office and Adobe Photoshop can now be purchased and downloaded right to your computer. You can also install free software this way. For example, if you wanted to install the Google Chrome web browser, you can visit **this page** and click the Download button.

The installation file will be saved to your computer in **.exe format**. Pronounced **dot e-x-e**, this is the standard extension for installation files on Windows computers. You can follow the steps below to install an application from an .exe file.

Locate and download an **.exe** file.

Locate and **double-click** the .exe file. (It will usually be in your **Downloads** folder.)

A dialog box will appear. Follow the instructions to install the software.

The software will be installed. You can now open the application from the **Start menu** (Windows 7) or the **Start Screen** (Windows 8).

Tips for finding software

In our experience, the easiest way to find new software is to **search the Web**. For example, if you were looking for a way to edit some personal photos on your computer, you could run a Google search for **free photo-editing software**. If you're not exactly sure what kind of software you're looking for, try describing the tasks you want to complete. For example, if you wanted a way to create to-do lists and organize your appointments, you might search for something like **free calendar organizer software**.

The Windows Store

If you're using Windows 8, you can download and install software from the **Windows Store**. The Windows Store is meant to simplify the process of locating and installing software from third-party developers—when you find an app in the Windows store, you won't have to do any extra work to install it.

KT2003 Common processes for downloading and removing software

How to safely download and install software

Unless you're planning to purchase all of your software on CDs (something you likely won't be able to do in the near future anyway), you're eventually going to have download new software directly from websites hosting those files. That could mean downloading software directly from the company or developers. But your downloading escapades will come with the inevitable dance around sometimes suspicious-looking websites, followed by the knot you get in your stomach that maybe, just maybe, you could be downloading a nasty piece of malware.

Is it possible to safely download and install software you find online? Of course! But sometimes it takes a little bit of common sense mixed with a touch of uncommon

knowledge to get the best and safest results. Let's lay out a few helpful tips to follow while trying to weave around sketchy websites and less-than-reputable downloads.

First, check the website address

We've written rather extensively on the differences between secured and unsecured websites, so we won't rehash the whole spiel here. Simply put: before downloading software from a website, check the website address. Look either for an **HTTPS** at the beginning of the address, or in the situations where your browser doesn't always display the hypertext transfer protocol, look for a **lock symbol**. Websites with an **HTTPS** or **lock symbol** (often both) are **secured through SSL/TLS encryption and have purchased a certificate to verify this fact**.

This means they are, for all intents and purposes, far more difficult to hack. The files you download from those pages are far less likely to have been hijacked and less likely to be a safety concern. Websites without SSL/TLS encryption or without the requisite certificates to prove they utilize that type of security cannot guarantee you anything, even if they say they can.

For example, one would think CNET's Download.com would be a secure, reputable place to download some new software. After all, it's Download.com. But wait:

There's no lock symbol and not HTTPS.

But then, sometimes websites choose to only secure specific pages. Perhaps CNET only saves the certification for where it's needed?

Not quite. Even an antivirus software's download page on CNET's website has no SSL/TLS secured certification:

Does that mean you can't trust Download.com? Not necessarily. But it doesn't exactly confer trust in Download.com either. Despite the mostly official source (CNET has been around for on the internet for over 2 decades), the site's lack of obtaining SSL/TLS certification is at the least somewhat confusing, considering the data protection concerns that exist on the web. They're not alone in this, to be frank, as the larger share of software hosting sites we've listed at the end of this article also lack SSL/TLS certificates.

CNET's Download.com might have highly secure servers hosting their files. We just don't know. They haven't bothered to purchase the certificate to verify that for us, and we could not find any information on their website detailing what security measures they employ for hosted files. We're left to wonder whether the site is or is not secure, among some other questionable practices they use (more on that later).

Meanwhile, a somewhat smaller, mostly unknown site, Free Software Directory, is fully secured:

Look, we get it. SSL certificates aren't exactly cheap to purchase. Even the lowest level SSL certificate, "Secure Site" can cost several hundred dollars a year, if not more. But if a not-for-profit website like Free Software Directory can afford to verify its security for consumers, surely a big, for-profit site like Download.com, and any other file-hosting websites for that matter can afford to do so as well.

Next, just use your eyes

This might seem a bit trite to say, but let your gut do the talking when you've hopped onto a website. Does it look and feel suspicious? Do you feel like your computer is catching viruses just by being connected to the web page? If so, you might want to consider moving away from that website as fast as possible. That is, of course, if your built-in web browser or antivirus software hasn't already alerted you to the fact that the website is not safe or secure. On that end…

Use active virus and malware scanners

There's almost no substitute for active virus and malware scanners. Not only can they scan your files before you install them, many will actually prevent you from downloading files that contain viruses and malware in them. This is a boon to you, and one of your best defenses against this kind of thing.

If you're a Windows user, you might also want to consider turning on Windows Defender. Windows Defender is Microsoft's built-in active malware scanner. It will actively block any attempt to download suspicious files.

If you don't trust the site, look for the software elsewhere

Simple, right? Sometimes, it's easier to try to locate the same program hosted on a more secure website. However, there will be times where that's simply not possible. Some programs are so rare or uncommon that the only websites that do host them are exactly the ones you want to steer clear of. In those cases, it may still be in your best interest to use those websites but to employ a few methods to avoid getting duped into downloading the malware or files and programs you don't actually want.

Check that the download link is really the link you're looking for

Let's come back to Download.com. Earlier, we mentioned that Download.com employs a few tricks we don't particularly like. One of them is including very large advertisements on download pages that will occasionally look like download links. This is a common practice among many software hosting sites, and it's not exactly a good one. On Download.com, that looks like this:

Instead of just giving you an obvious download link, CNET's site places two advertisements right beside the actual download link. In CNET's defense, you won't see this occur with the advertisements all the time. Sometimes the ads are mostly unrelated, and it's easy to identify which link is the correct one almost immediately.

However, the use of such ads is somewhat misleading. This method is used to build advertising revenue through more clicks, playing on the fact that the human eye tends to scan websites quickly. Many people will instinctively click the first link that looks like the right download button without thinking about it first. While you may not end up downloading unwanted software or malware if you click on such a link at Download.com, this has been known to occur with many other websites that utilize this same revenue tactic.

It's even worse on the website FileHippo. Where would you instinctively click first on this page?

That's right — you'd probably click the extremely large, in-your-face, official looking "START DOWNLOAD" button. FileHippo can get by with this because, well, it says "Advertisement" over the button. If you click that instead of the much less ambiguous real download link on the top right, that's your fault.

Not every website lacking SSL/TLS certificates does this. The website TechSpot doesn't offer misleading download links, for example:

The download link you see on this website is the download link you want. You don't get any misleading advertisements moving your eyes to other directions to trick you into hitting a link and downloading a file you don't want.

In most cases, you can check the download link by hovering over what looks like the download, then checking the bottom of your browser. For example, when we hover over the download link on TechSpot, this is what we get at the bottom of the screen:

Here, we are on the BitDefender download page for TechSpot. Positively, the download link is to BitDefender. Some websites do not bring up the actual link when you hover, although you can still right-click the link, select “Copy Address” and paste the link into your address bar or a word processor to see what the link actually says.

Avoid download programs and installers

Repeat after me: I do not need a downloader or installer to install a program. Keep saying that to yourself. That way, when you run into a website that attempts to make you download a program with an installer or a download program, you’ll remember to avoid that site altogether and find that file hosted somewhere else.

These types of programs are often referred to as “**potentially unwanted programs**”, or PUPs. To be clear, you don’t need a download program or installer simply because every operating system you might use is designed to unpack that software file and install it, while the program itself should have installation methods built into the software. Download programs and installers are essentially extraneous pieces of software that often pair the program you want into a piece of unneeded software, commonly adware.

Know the difference between freeware, shareware, trialware, open source, and commercial software

Here are some simple definitions for you:

Freeware: any software that is completely free. You do not have to purchase it to use it.

Shareware: any software that is designed for limited, evaluation use, after which you must pay for the software to continue using it.

Trialware: a modern iteration of shareware. You can use the terms interchangeably.

Open source: any program that has openly published source code, which is available for free, and which is often continuously in development by the community.

Commercial software: any software that you must purchase in order to use.

On that end, **free downloads** are not the same as **free software.** If a website tells you that you can download a program for free, be wary. Almost all software is available to download for free. Nobody makes you pay for the action of downloading. Pay attention to that tricky wording.

Installing software safely

Once you've found a reputable site to download your software and you've hit the download button, you're still going to have to install the program. Here are a few quick tips for when you're at the final stage.

Make sure your active malware or virus scanner has scanned the file

If this was not done, or you lack an active scanner, some programs do let you scan the file after downloading, but before installation. Some will even allow you to single out specific programs to scan by right clicking on the file name or icon.

During installation, always choose the "Custom" installation process

Many programs will come with multiple installation options. Instead of going for the "Quick" install option, instead, choose the "Custom" option. This will let you pick and choose which features you want to be installed. Sometimes, you may find that pieces of software come packed with additional software you don't actually want and that may actually be malware. Examine the list of options when doing a "Custom" install and uncheck anything you don't want.

Avoid giving out your email address during installation if you can

Some programs will ask for your email address once the download is nearly complete. In some cases, this is to sign up for an account with the website or service, yet far too often it's just so that the company behind the software can spam your email. If the software requires no account, it's best to avoid providing your contact information.

Of course, there are exceptions to this rule. **Free software** which requires no registration keys to install and use certainly don't need to have your email address. However, for **paid software** that requires a registration key to operate, such as the latest game or a high-quality piece of creative software, like Adobe Photoshop, it's in your best interest to register.

The main reason is **data loss**. If your computer crashes, or you lose all of your data, you may be forced to reinstall the program. Some programs have one-time use registration keys that are randomly generated upon purchase. Registration can help you avoid having to repurchase an expensive piece of software.

Trusty and untrustworthy software sites

Not sure which sites you should trust the most? Here's a list of websites that host software programs. We've broken them up into three categories: SSL/TLS Certified and Trustworthy, Not Certified but Trustworthy and Not Recommended.

In this case, we've listed a site as "trustworthy" if does not include SSL/TLS, but it avoids using sneaky and distracting ads. Any site listed as "Not Recommended" is purely based on our opinion that the site in question is not recommended due a lack of advertising its security methods through SSL/TLS certificates, or that it often uses distracting advertisements. This in no way means those sites are prone to hosting malware, nor that you will find malware on those sites.

KT2004 Troubleshooting

Unable to Install Apps or Software on Windows? Here's What to Do

If you're unable to install software on Windows 10 or Windows 11, here's how to fix common app installation problems.

Wondering why you can't install any apps on Windows 10 or Windows 11? It's frustrating when software installers won't run, throw an error code, or seem to work properly but then fail.

Below are fixes to try when software won't install correctly in Windows.

1. Reboot Your Computer

This is a common troubleshooting step, but it's important for a reason. The reason that software won't install on your computer could be due to a temporary glitch. Before you jump into more focused fixes, you should reboot to get back to a clean state.

If you still can't install software after a reboot, continue troubleshooting further with the next steps.

2. Check App Installer Settings in Windows

Windows 10 and Windows 11 allow you to install traditional desktop apps, as well as apps from the Microsoft Store. Certain settings will restrict you to only installing Store apps, so you should check those first.

To do this, head to **Settings > Apps > Apps & features**. At the top, you'll see a **Choose where to get apps** section. If the dropdown is set to **The Microsoft Store only (recommended)** then you won't be able to install apps from anywhere else. This prevents you from installing traditional Windows desktop software.

Change this to **Anywhere** (or **Anywhere, but let me know if there's a comparable app in the Microsoft Store** if you want) and Windows won't block you from installing software anymore

If you're on an older version of Windows 10, you should also check a similar setting in **Settings > Update & Security > For developers**. Here, under **Use developer features**, make sure that you have **Sideload apps** selected. Picking **Microsoft Store apps** can prevent you from installing regular software.

On modern versions of Windows 10 and on Windows 11, you won't see these three options. Instead, you'll see a single **Developer Mode** slider (on Windows 11, this is under **Settings > Privacy & security > Developer Mode**). You don't need to enable this to install regular apps, so you can leave it disabled. It doesn't hurt to enable it while you're troubleshooting, but you can turn it back off once everything is working.

If you're trying to install an app that requires you to toggle this setting, make sure you trust it. Installing random apps from unknown sources could be dangerous.

Finally, if you're in Windows 10 S Mode or Windows 11 S Mode, you can only install apps from the Microsoft Store. Thankfully, it's easy to switch out of S Mode at no charge. To do this, open the Microsoft Store app, search for "Switch out of S mode," and proceed through the download like you would with other apps.

3. Free Up Disk Space on Your PC

If you're extremely low on disk space, you may not be able to install new software. While this is rarely an issue for small apps, installing heavy-duty tools, such as Microsoft Office or Adobe products, will require several gigabytes.

Follow our **guide to freeing up space in Windows**, then try installing the software again.

4. Run the Installer as an Administrator

Thanks to **User Account Control (UAC) in Windows**, your account only uses its admin privileges when necessary. Since most software requires admin rights to install, you'll usually see a UAC prompt when you try to install a new app.

If you're only installing an app for your current account, it might not need administrator permissions. But installing software that applies to all users will require admin approval. Make sure you don't have UAC turned off, or prompts to give admin permissions might fail to appear.

Occasionally, approving a UAC prompt won't work right. You might see an error that the installer can't write to a certain folder, or it might refuse to run at all. In these cases, you should run the installer as an admin manually.

To do this, close the installer dialog if it's open, then right-click on the installer file and choose **Run as administrator**. After granting admin rights, try the installer again and see if it succeeds.

In case you don't have admin rights on your current machine, ask someone who manages the computer or check our **guide to getting admin rights on your computer** for more help.

5. Check the App's 64-Bit Compatibility

A lot of software offers both 32-bit and 64-bit flavors. 64-bit software is only compatible with 64-bit versions of Windows. However, 32-bit apps will run on both 32-bit Windows and 64-bit Windows, since 64-bit Windows is backward-compatible.

Most of the time, the software will automatically pick the right version to install on your system, or will just install as 32-bit if that's the only option available. If you have a modern computer, it's likely 64-bit, meaning this isn't a problem. But if you're not sure, you should **find out if you have 64-bit Windows**.

Once you know which version of Windows you have, keep an eye out on software download pages and make sure to download the version that's compatible with your system. **x86** refers to 32-bit, while **x64** means 64-bit. Don't download 64-bit software on a 32-bit system, as it won't run.

6. Run Program Troubleshooters

Windows 10 and 11 include several built-in troubleshooting tools that try to detect and fix common problems. They don't always work well, but they're worth a try when Windows won't install programs for some reason.

To access the troubleshooter that deals with installing software on Windows 10, head to **Settings > Update & Security > Troubleshoot** and click **Additional troubleshooters**. Here, run the **Program Compatibility Troubleshooter** and see if it fixes any problems. You can also run the **Windows Store Apps** tool if you're having trouble installing a Store app.

On Windows 11, these utilities are under **Settings > System > Troubleshoot > Other troubleshooters**.

If this doesn't work, you should try the **Program Install and Uninstall troubleshooter**, available to download separately from Microsoft.

7. Uninstall Previous Software Versions

Most of the time, installing an app update (even if it's a new major version) goes smoothly. But sometimes, having an old version of a program installed can cause issues when you try to install the latest release.

KT2005 Optimisation

Optimization (computer science)

In computing, **optimization** is the process of modifying a system to make some features of it work more efficiently or use fewer resources. For instance, a computer program may be optimized so that it runs faster, or to run with less memory requirements or other resources (see Space-time tradeoff), or to consume less energy. This is a branch of software engineering.

The optimization can have sense at different levels, from the lowest (development of circuits, writing of machine code designed especially for the architecture) up to the highest levels of making of implementation, use or design of algorithms.

The optimization is generally recommended to leave until the end of the process of development, since the premature optimization can introduce new errors (generally more difficult to detect for being of algorithmic nature).

The optimized system may be a single computer program, a collection of computers or even an entire network such as the Internet.

Internal Assessment Criteria and Weight

• IAC2001 Procedures for installing and removing utilities are described

(Weight 2%)

Previous Next

Content List: