

Don't Invite Malicious Software to Install Itself on Your PC!

This article shows you:

- The way malware can hide in innocent-looking programs
- How to check a program for malware before installing it
- The safest approach to installing a new program

Why would you invite malicious software to install itself on your PC? Well, you certainly wouldn't do it knowingly – nobody wants a malware infection! But you might do it in the belief that you're installing something trustworthy and safe. In this article, I'll show you how easily this can happen, and I'll explain the steps you should take to ensure the software you install really is what you think it is!



Contents:

The Dangers of Installing Free Software.....	M 037/2
Safety Step 1: Research the Program Online.....	M 037/5
Safety Step 2: Verify Software with 'VirusTotal'	M 037/6
Safety Step 3: Install Without an Internet Connection.....	M 037/8
Safety Step 4: Check the Licence Terms First.....	M 037/9
Safety Step 5: Always Choose a 'Custom' Installation	M 037/11
Safety Step 6: Read Every Step Carefully!	M 037/12

The Dangers of Installing Free Software

Free software is easy to find... Everywhere you turn on the World Wide Web, you'll find offers of free software to download. Some of that software is excellent and utterly trustworthy. Where would we be without free web browsers like Mozilla Firefox and Google Chrome, free photo-editing programs like Paint.NET, and free security software such as AVG AntiVirus (to name just a tiny handful)?

... but is it safe? Unfortunately, though, a lot of free software is very different from those famous examples. Unless you're careful, you can find that you've installed something that's extremely annoying, and perhaps dangerous and costly too.



Why am I picking on free software? Quite simply, if a software company makes its money by selling software, it relies on keeping a good reputation. If word gets out that a program it sells does undesirable things to its customers' computers, sales would quickly dry up!

While I certainly recommend applying some caution to anything at all you install on your computer, it's free software that presents the greatest risk by far.

The risks of free software fall into two main categories:

Risk1: rogue 'security' software

Free software isn't always what it appears You arrive at the website of a company that makes an excellent-sounding free security program for your PC. Or at least, the website makes it sound excellent. The program claims to scan your PC for viruses and malware, and clean and speed-up your PC. It seems to have won awards and received glowing reviews, and its web page carries a reassuring graphic that says 'Guaranteed 100% Spyware Free!'.

However, when you've downloaded and installed it, what do you find? After making a show of scanning your PC, the program reports a bewildering list of virus infections and other problems it's found. What it can't do, unfortunately, is fix them. You need to pay for its 'Premium edition' to do that.

While you're wondering whether to stump up the rather-high price it asks for this 'Premium edition', yet more errors and warnings are appearing. After a while, they're appearing so thick and fast that you can barely close one before the next appears.

This is what's known as 'scareware'. It isn't scanning your PC at all, it's simply designed to scare you into believing your PC is in a mess so that you'll pay for that 'Premium edition'. From here, you'll do one of two things:

- Perhaps you'll believe all these warnings and pay for that 'Premium edition' to have all these errors fixed. This expensive purchase does nothing useful either: since the errors were all fictitious, there's nothing to fix! However, it will quickly discover other problems which, it says, can only be fixed by buying some other program. You're in an endless cycle of buying one program after another that does absolutely nothing (until you finally realise you've been had and set about trying to get rid of this scareware infection).
- Perhaps you'll realise what this program is really doing straight away and you'll thus avoid being conned into paying. However, that still leaves you with the job of removing this scareware from your PC, and that's unlikely to be easy. The company purposely makes this 'scareware' difficult to remove so that, eventually, you might just pay up in the hope that all these warnings will then stop. (They won't: as far as the company is concerned, if you paid once, why wouldn't you pay again?)

*Scareware
frightens you into
paying...*

*... perhaps
several times!*

*It's notoriously
hard to remove*

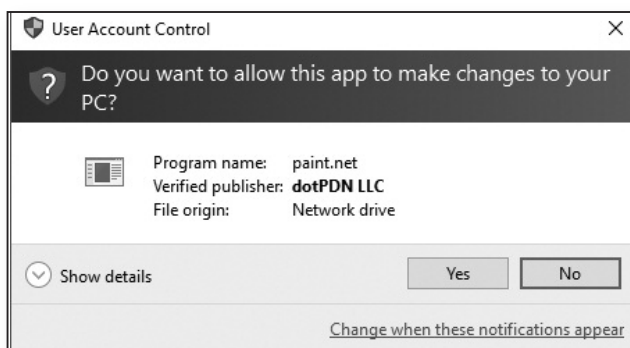
Risk 2: bundled adware, spyware and unwanted changes to your settings

- A good program...* Perhaps the free program you've found really is a good one: it does what it claims to do and does it well, and you've heard good things about it. However, as with any software, before you can use it, you have to install it. This leads to our second risk.
- ... with unpleasant extras* Rather than charging customers for a program, the company can earn money by bundling other companies' software with it. These added extras are installed at the same time as the main program itself – possibly without your knowledge. And while the company's own program may indeed be safe and useful, these bundled extras might give you all sorts of trouble!
- Some are very annoying* One common type of bundled addition is software that makes changes to your web browser: it adds extra toolbars, it changes your home page and search page, and it stuffs extra advertisements into the web pages you visit. It might take things further still, changing your desktop wallpaper to display a sequence of advertisements or displaying pop-up ads at intervals while you work.
- Some could be very dangerous* That's all certainly very annoying, but it's the least-dangerous aspect of this software bundling. These extras could just as easily be spyware: programs which hide on your PC and spy on the websites you visit, the passwords you type to sign into them, the credit card details you type when buying something, and the personal details stored in files on your computer.
- Choose and install your software carefully!* **Summary:** free software can be superb, and some of the very best and most popular programs really are completely free. However, it's vital to remember that on the Internet things are not always what they seem! Don't take chances: pay attention to the 6 Safety Steps below to avoid unwittingly installing malware on your computer.

Safety Step 1: Research the Program Online

I'm sure you've noticed that whenever you start to install a new program you've downloaded, you have to run through a couple of security checks. The first tells you that this program came from another computer and asks if you're sure you want to run it; the second, headed 'User Account Control', asks if you're willing to let this program make changes to your computer.

Are you sure the program is safe to install?



Essentially, what Windows is asking is whether you trust this program – are you certain it's safe? If you allow the installation to begin, it will have permission to do more-or-less whatever it likes on your PC.

Therefore, it's important to do some research about a program before you download it. Visit a good search engine such as Google (www.google.co.uk) or Bing (www.bing.com) and search for the program by name.

Do some research before downloading

When looking through the search results, ignore any links that point to the program maker's own website: you know that's going to paint a glowing picture of the program, whether deserved or not! Instead, look out for recent reviews of the program and discussion forums where users of the program have talked about it. And, in particular, watch out for any links in the

search results that seem to suggest there may be something risky or undesirable about the program.



This should only take you a few minutes, but it could save you an awful lot of trouble if the program does turn out to be undesirable in some way. In addition, of course, you may find helpful tips in using the program, or a recommendation of a better program to consider (and research!).

Whatever you do, NEVER download a program based solely on what its own maker says about it!

Safety Step 2: Verify Software with 'VirusTotal'

Is this a safe place to download from?




The Internet is awash with 'download sites' – websites which gather together all sorts of free programs from all sorts of companies and allow you to browse through them and download what you like. The trouble is, you can't be sure that these copies of the programs haven't been modified in some possibly-malicious way.

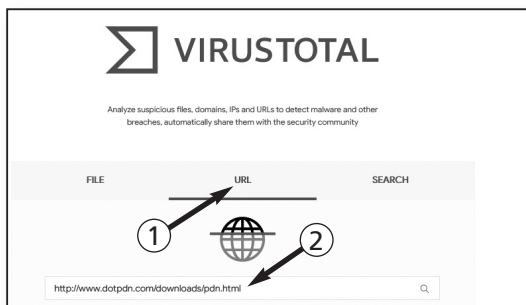
Therefore, once you've researched a program and satisfied yourself that it should be safe to install, aim to download it directly from the website of the company that makes it.

Try to download directly from the program's maker

If you can't do that for some reason, or if you're not sure you really have found the right website, run some extra checks. A terrific online service named 'VirusTotal' can scan both the web page and the program itself using (at the time of writing) 93 different malware scanners to let you know whether the web page and its software are safe.

Start your favourite web browser (or open a new tab in your browser) and follow these steps:

1. Type the address www.virustotal.com and press **Enter**.
2. In the simple web page that opens, click the **URL** tab  . Then, in the box below , type or paste the URL (address) of the web page from which you're planning to download your new program.

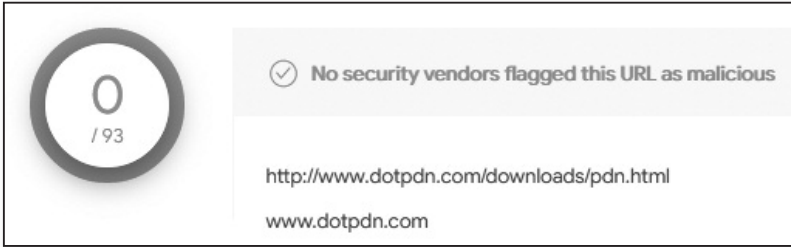


Rather than trying to type the address into this box, it's quicker and easier to copy-and-paste it. Switch back to the browser tab containing the program's web page, click in the address box to highlight the address of the page and then press **Ctrl+C** to copy it to the clipboard. Then switch back to the tab containing the VirusTotal page, click in the box and press **Ctrl+V** to paste that address into the box.

3. Press **Enter**. After a short wait, you'll quite likely see a panel showing the results of VirusTotal's scan of that web page. Alternatively, you might arrive at a page showing the results from all 93 of those scanners in a list. Either way, what matters is the 'Detection ratio' noted in the pop-up panel or at the top of the list. As you can see in the screenshot below, the page I've scanned has a 'Detection ratio' of **0/93**: in other words, none of VirusTotal's 93 malware scanners has found anything suspicious on the page and that's exactly what you're hoping to see.



Check the 'Detection ratio' for this web page



Now scan the program before installing it

4. If the scan of the web page revealed it to be safe, you can return to that page and download your program.
5. When the download is complete, use VirusTotal again to scan the program before installing it. On the VirusTotal web page, switch to the **File** tab, click the **Choose File** button and select the program you've just downloaded and saved to your PC, then click the **Confirm upload!** button. A copy of this file will be uploaded to VirusTotal and scanned.
6. As before, look at the 'Detection ratio', where you'll again be hoping to see that none of those malware scanners detected anything suspicious in the file.



If anything suspicious was detected, you can examine the results to see what it was. It's worth noting that some scanners could detect a 'false positive' – in other words, they see a risk that isn't actually there. However, if more than a small handful of scanners have detected a problem, it's wise to believe it and delete the file from your PC rather than going ahead with the installation.

Safety Step 3: Install Without an Internet Connection

Before you begin installing the free program you've downloaded, there's one more step that's well worth

taking in order to help prevent infections: to disconnect your computer from the Internet.

Why? Well, in some cases, the malware or adware isn't actually included in the file you've downloaded. Instead, the setup program connects to the Internet during the installation routine and downloads it. (Of course, that could be one reason why VirusTotal's scanners didn't find anything suspicious in the file!)

By disconnecting from the Internet, you make it impossible for this to happen. In some cases, even if the installation routine would normally have installed something undesirable, it will simply move past that section of the routine and just install your program.

The drawback to this tip is that sometimes an installer does need to connect to the Internet for perfectly innocent reasons – to check for updates or to fetch additional system files required by your new program, for instance. Thus, for one reason or another, you may reach a point at which the installation refuses to continue without an Internet connection.

Nevertheless, it's worth trying to follow this tip and see what happens. If error messages appear, use these to try to determine why the installation needs an Internet connection and decide whether or not to continue.



Remove the chance of downloading malware

Safety Step 4: Check the Licence Terms First

At the beginning of a program's installation routine, you'll usually be shown the licence terms and be asked to confirm your agreement to them. Although they can be painfully tedious to read, it's well worth having a look through them to see if anything suspicious catches your eye.

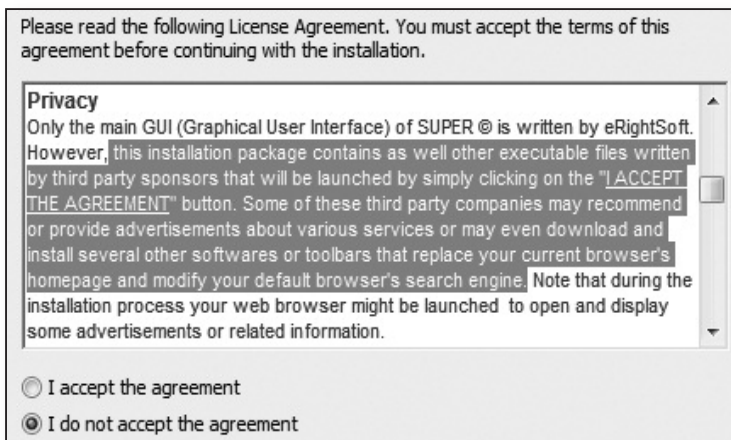
Tedious, but worthwhile!

Some software companies use these licence terms to excuse the actions of any extra software they've bundled with their program. If there are complaints or threats of legal action, they can say: 'We told you about this in the licence agreement, and you accepted it.'

Valuable clues that unwanted extras are included

One such example is pictured below, from a program named 'SUPER'. As you can see in the text I've highlighted, this program intends to install other programs from third parties, with the possibility of adware and browser toolbars arriving on your PC and changes being made to your browser's settings.

It's quite possible that if you accepted this agreement without reading it and continued with the installation, there would be no further mention of any of this in the steps that followed: you'd simply find that all these unwelcome extras had suddenly appeared!



The legality of these licence agreements is questionable. Certainly, though, no-one could get away with installing spyware or other malicious software on your PC simply by telling you about it here. For this reason, of course, if true malware is being bundled with a

program (or if the program itself has malicious intent), you won't see any advance warning of it! This tip and those below are chiefly aimed at avoiding adware and similar annoyances.

Safety Step 5: Always Choose a 'Custom' Installation

Once you've moved past the licence terms, whatever they revealed, you may arrive at a step which gives you a choice between a 'Typical' (or 'Express' or 'Complete') installation and a 'Custom' installation. If so, always choose the 'Custom' option.

A choice of installation methods

Choose the installation method you prefer, and then click Next.

Express

This is the recommended choice for most users. This installs using the default options, or the same options that were specified during a previous installation.

Custom

Allows you to change the installation directory, and options related to file type associations and update checking.

With a 'Typical' installation, many of the steps are hidden from you. Rather than having to click your way through a sequence of steps before reaching the final 'Install' button, you're taken straight to the point at which the program is installed.

Many steps are hidden

However, you want to see those steps! One of them may be a page which offers to install one of those 'bundled extras', and if you don't see that step, you don't get the option to refuse it!

By choosing the 'Custom' option, you're guaranteed to see every available option about what will be installed and how. It may take you half-a-minute longer, but it could save you many hours of frustration!

Choose 'Custom' to see what's really going on!

Safety Step 6: Read Every Step Carefully!

*It's easy: just click **Next*** In general, every program's installation happens in the same way. Once you've started the process and accepted the licence terms, you begin a sequence of steps offering a variety of options about what is installed, where and how. In the same place in each of these steps, there's a **Next** button, and after clicking that button a few times, you arrive at a step containing an **Install** button instead.

Don't rush through these steps When you've become used to this process, it's very tempting just to place your mouse pointer over that first **Next** button and then just click-click-click until you find you've clicked the **Install** button and your program is being installed.

Look out for those unwanted extras! Resist that temptation! Take your time and read the options being presented in each step. In many of the steps there'll be nothing to change, but you may well arrive at a page in which some 'optional extra' is offered and the option is ticked. If you skip past without reading it or removing the tick, you're not in a good position to complain about the trouble it's caused you afterwards!

