You check your email, download a harmless looking Word document attachment, open it – and next thing you know, your computer has been infected with dangerous malware. It starts spreading to other documents. Maybe it steals your address book and attacks your friends. Or maybe it encrypts your files and demands a ransom to give them back. What happened? You were attacked by a macro virus (a.k.a. macro malware).

Let’s take a closer look at macro viruses – and how you can stay safe from them.

To begin with, what’s a macro? It’s a small program that runs within a bigger program to automate a task on a user’s behalf – typically a complex or time-consuming task that would be annoying to perform manually, or hard to perform accurately and consistently.

Macros are written in a programming language designed to work within their broader environment. So, for example, macros for Microsoft Office are currently written in Visual Basic for Applications (VBA), a variation of Microsoft’s popular Visual Basic programming language that was created specifically for Office. VBA works within most Office programs, including Access, Excel, Outlook, PowerPoint, Project, Publisher, Visio, and Word. It also works in most recent versions of Office for both Windows and Macintosh, and according to Microsoft, the majority of existing VBA macros will also work in the cloud-based Office 365.

Sophisticated macros are written directly in the VBA language, but individuals can also automate simple tasks by recording the steps and allowing Office to translate their recording into working VBA code.

Since macros are programs written in a programming language, they can potentially be compromised by malware authors just like any other program. Microsoft Office VBA macros are an especially attractive target because Office is used by so many people – Microsoft claims 1.2 billion users. There’s another reason, too: when Microsoft first introduced macros, it was extremely careless about security, and it’s been playing catchup ever since. For a while, it looked like the threat of macro viruses was fading, but they recently made a comeback: in the summer of 2018, one researcher found that nearly half of all malware loaders were being embedded as Office macro viruses.

The best way to stay safe from macro viruses is not to run them. So, in recent versions of Office, Microsoft has changed its default settings: now, if you open a file containing a VBA macro, the file will open but the macro will be disabled. By default, you’re shown a message informing you of this and giving you the option to enable the macros in that file if you’re confident they are safe. (Of course, that assumes you’re sure the file came from a source you can completely trust – or maybe you wrote the macro yourself.)

It’s a good idea to check this setting – and if you don’t have reasons to use macros, you might want to instruct your Office program to keep them disabled without even telling you. The steps vary a bit between Office versions and programs, but here’s how you do it in any Office 2016 program. Choose File, click Options, and click Trust Center. Click Trust Center Settings, choose the Macro Settings tab, click Disable All Macros Without Notification, and choose OK. (Note that changing the setting in one Office application doesn’t change it in all of them.)

If you’re using an older version of Office, it might run macros automatically, so you’d really better check. (Versions of Office older than Office 2010 aren’t supported by Microsoft anymore, so you might consider upgrading.)

You might imagine that if macros don’t run by default, the problem is solved. Unfortunately, macro virus authors are surprisingly good at coaxing people into turning on the macros in their documents. First, they convince you the document is important: supposedly it’s an invoice, a letter from the IRS, or something equally urgent. Then, they tell you the file’s “protected” and you need to run macros to view it. You agree, and zap – they’ve got you.

Don’t ever fall victim to that. Just close and delete the file.

There’s no substitute for being smart, but it isn’t enough. A 2017 security report identified several ways an attacker can potentially deliver malware via Office documents even without macros. And at least one of these attacks (based on ancient “Dynamic Data Exchange” techniques) has been seen in the wild.

What Are Macro Viruses?

A **macro virus** is a type of computer virus that is written in the same macro language that is used for software applications, most often office application software like Microsoft Word and Excel. The macros are automatically activated when documents are opened because the macro language is embedded in the documents. This is also the same way macro viruses workopening and closing a document. Macro viruses are among the more difficult viruses to detect; learn more about them below.

Macro Viruses: What They Do And How To Spot Them

The very first macro virus was the Concept Virus in July 1995, targeting Microsoft Word files. Macro viruses became the dominant virus from that point through the end of the decade. On March 26, 1999, the Melissa Virus started spreading via email and infected tens of thousands of computers within hours. Both of these instances caused Microsoft to begin turning off macros by default in Office applications, beginning with Office 2000. This is why criminals must trick the user into opening the document, since macros will no longer run without opening up the document first.

Macro viruses can be programmed to do almost anything on a PC; thus, they can do any or all of the following items:

* Create new files
* Move text
* Send files to another location on the computer or through the default email system
* Corrupt data on a hard drive or the hard drive itself
* Format the hard drive
* Insert pictures into documents

Oftentimes, the creators of these macro viruses will use them to transport malware and viruses onto the computer, thus enabling the cybercriminal to gain access to sensitive information, such as login information for financial accounts and other sites, etc.

If a person opens a document containing a macro virus, instantly, all other files on that computer become infected. Text files may look different because there could be added or missing words due to the macro virus. The macro virus will likely attempt to email itself to the first fifty or more people in the person’s contact list in an effort to spread itself further; if any of them open the document attached to the email, they will also be infected in the same way as the first victim was.

It’s important to note that because the macro virus is centered around an application rather than an operating system, it can infect any computer user, even those running MacOS or Linux. Any computer that can run office application software and open such files can be infected by a macro virus.

The symptoms of a macro virus infection usually include the slowdown of one’s computer. In addition, a macro virus will often ask the computer user for a password on a file that normally doesn’t require one to gain access. Virtually every file that is saved on an infected computer is saved as a template file. An infected computer will often display unusual error messages, ones that are not typical of regular error messages. Any or all of these instances most likely means that the user’s computer has been infected by a macro virus.

Macro Virus Prevention

Preventing a macro virus from getting onto a computer is the best course of action. One should have good antivirus and anti-malware programs and keep them updated. They should be run regularly to detect macro viruses and avoid possible activation. One’s operating system should be updated regularly to patch vulnerabilities that a macro virus could take advantage of. When downloading files, be sure to use digital signatures, which identify download sources so that a user knows what he/she is downloading and that the program is not a risk to run.

Getting Rid of a Macro Virus

It is possible to get rid of a macro virus without professional assistance or a good antivirus and/or anti-malware program, but to do so, one must know what files to look for that are associated with the macro virus. As suggested by M. David Stone in PC Mag in 2001, one should click on Tools-Macro-Macros for each file in Normal.dot and the Startup folder and be on the lookout for the following file names:

* AutoExec
* AutoOpen
* AutoClose
* FileExit
* FileNew
* FileOpen
* FileSave
* FileSaveAs
* ToolsMacro

The first three in that list run automatically, while the others are common names for viruses. If the user did create legitimate macros with those exact file names, he/she will have to use the Edit command to look inside the files and see if they have been changed and/or compromised in any way. If they haven’t, the user is probably virus-free.

Additionally, the user should use the “Alt-Ctrl-Delete” combination to bring up Task Manager and identify any suspicious-looking processes under the “Processes” tab. Those processes must be terminated with the “Terminate” button. Then, the user must search his/her computer using the “Start” button and “Search Programs and Files” button. The user must identify the infected Macro files and delete them manually.

As mentioned above, a good and updated antivirus or anti-malware program can often detect theses macros and remove them from within the program. By following the information above, one can know the dangers of macro viruses, identify the signs of one, and remove it before it can do damage and spread to others.

**Macro viruses add their code to the macros associated with documents, spreadsheets and other data files.** The first macro virus, called Concept, appeared in July 1995 and macro viruses (mostly infecting Word documents) subsequently became the dominant type of virus until the turn of the century, when Microsoft disabled macros by default in Office (versions since Office 2000): since then, cybercriminals have had to try and trick their victims into enabling macros before their infected macro is able to run.

**How Macro Viruses Spread**

Macro viruses are most commonly found embedded in documents or inserted as malicious code into word-processing programs. They may come from documents attached to emails, or the code may be downloaded after clicking on "phishing" links in banner ads or URLs. They are difficult to detect, as they do not operate until an infected macro is run, at which time they perform a series of commands. A macro virus is similar to a Trojan virus, since it may appear benign and users may not immediately notice any ill effects. Unlike Trojans, however, macro viruses can replicate themselves and infect other computers.

**Risks**

The main risk of macro viruses is their ability to spread quickly. Once an infected macro is run, all other documents on a user's computer become infected. Some of these viruses cause abnormalities in text documents, such as missing or inserted words, while others access email accounts and send out copies of infected files to all of a user's contacts, who in turn open and access these files because they come from a trusted source.

These viruses can also be designed to erase or compromise stored data. In addition, it's important to note that macro viruses are cross-platform; they can infect both Windows and Mac computers using the same code. Any program that uses macros can operate as a host, and any copy of an infected program — sent via email, stored on disk or on a USB drive — will contain the virus.

To remove these viruses, users should rely on security software that provides specific macro virus detection and removal tools. Regular scans will clean any infected documents and ensure no new computer viruses are downloaded.

**Types of Macro Viruses**

Macro viruses can be found in several different forms. Although some people consider them to be a relic of the late 1990s, they have in fact made a resurgence in recent years, forcing users to be extra vigilant.

* **Concept Virus**  
  Concept was the first macro virus, appearing in July 1995 and targeted Microsoft Word. Macro viruses subsequently became the dominant type of virus.
* **Melissa Virus**  
  Melissa made history as the first macro virus with email worm trait and started spreading via email on March 26, 1999 infecting tens of thousands within hours. It was one of the most serious epidemics in Internet history.