# What is a Trojan Horse?

When you hear the term '*Trogan Horse'*, do you think back to Greece and that epic horse that is one of history's most famous tricks?

*Trojan malware* takes its name from the classical story of the *Trojan Horse*, because it imitates the technique to infect computers. *A Trojan* will hide within a seemingly harmless program, or will try to trick you into installing it.


*Trojans* do not replicate by infecting other files or computers. Instead, they survive by going unnoticed. They may sit quietly in your computer, collecting information or setting up holes in your security, or they may just take over your computer and lock you out.

Due to *Trojans* being so versatile and with their ability to go unnoticed, their popularity has exploded and unfortunately for us, they have become the malware of choice for many online criminals.

Some of the more common actions that *Trojans* take are:

- **Creating 'backdoors':** *Trojans* typically makes changes to your security system, so that more malware or even a hacker can get in.
- **Spying:** Some *Trojans* are essentially *Spyware*; designed to wait until you access your online accounts or enter your credit card details. Then, they send your passwords and other data on for criminals to use.
- **Turning your computer into a zombie!** Sometimes, a hacker isn't interested in you, but just wants to use your computer, in a network under his or her control.

- **Send costly SMS messages:** Even smartphones get *Trojans*. The most common way for criminals to make money, is by using them to make your phone send costly SMS messages to premium numbers.

## What does a Trojan Horse look like?

Well, that's just it: *Trojans* can look like just about anything. The computer game you downloaded, a free song that you downloaded and even an advertisement might try to install something on your computer.

Some *Trojans* are specifically designed to trick you into using them. They can use misleading language or try to convince you they are a legitimate application. Tricking you this way is called *social engineering*, because the criminals designed a situation to make you act against your interest.

## How do I protect myself against Trojans?

1. Realise that you are an attractive target to hackers. Don't ever say *"It won't happen to me."*
2. Practice good password management. Use a strong mix of characters and don't use the same password for multiple sites. Don't share your password with others, don't write it down and don't write it on a post-it note attached to your monitor, *ever!*
3. Never leave your devices unattended. If you need to leave your computer, phone or tablet for any length of time, no matter how short, lock it up so no one can use it while you're gone. If you keep sensitive information on a flash drive or external hard drive, make sure to lock it up as well.
4. Always be careful when clicking on attachments or links in email. If it's unexpected or suspicious for any reason, don't click on it. Double check the URL of the website the link takes you to. ***Think you can spot a phoney website? Try this Phishing Quiz*.**
5. Sensitive browsing, such as internet banking, should only be done on a device that belongs to you and on a network, that you trust. Whether it's a friend's phone, a public computer or a cafe's free Wi-Fi—your data could be copied or stolen.
6. Back up your data regularly and make sure your anti-virus software is always up to date.
7. Be conscientious of what you plug in to your computer. Malware can be spread through infected flash drives, external hard drives, and even smartphones.
8. Watch what you're sharing on social networks. Criminals can befriend you and easily gain access to a shocking amount of information; where you went to school, where you work, when you are on holiday—that could help them gain access to more valuable data.
9. Be wary of social engineering, where someone attempts to gain information from you through manipulation. If someone calls or emails you asking for sensitive information, it's okay to say no. You can always call the company directly to verify credentials before giving out any information. Never openly give information out if you don't feel comfortable with who you are speaking to.

10. Be sure to monitor your accounts for any suspicious activity. If you see something unfamiliar, contact your in-house IT department or Managed Service Provider straight away. That's what they are there for!

Please feel free to call our helpful and knowledgeable team on 01843 572600 if you would like any advice about cyber security. You can also email us at hello@365itsupport.co.uk – we are always happy to help and provide advice for your IT requirements.

bcs
business computer solutions