

# Malware

‘Malware’, short for ‘malicious software’, is used by criminals to disrupt computer operations and access confidential information. Malware can be installed into your computer through clicking a link in an email, opening an attachment to an email, or by downloading software from a malicious source.

## Trojans

Trojan programs are a type of malware that enter your computer on the back of other software. They act as back doors to the computer, granting a fraudster remote access. Once inside your device, a trojan can give a stranger access to your personal details by taking screenshots or capturing keystrokes.

When logging into online banking websites, an unexpected screen might appear, delaying you or asking you to repeatedly input data. While you are delayed by these, a fraudster could be setting up another payment elsewhere, waiting for you to unwittingly authorise it by inputting your PIN.

Trojans are hard to detect as they remain passive when not in use. Firewalls and anti-virus software help to defend against trojans, but can’t guarantee your protection. You should always be cautious of ‘pop-ups’ on your screen requesting that you put your card into the reader, input your PIN, or allow a download.

## Ransomware

Ransomware enables a fraudster to gain control of your system in order to encrypt your files, demanding a fee to unlock them. Without the decryption code, it is very unlikely that you will be able to access your files again.

---

**24% rise**  
in new ransomware samples  
in Q1 2016<sup>6</sup>  
**Over 5.5 million**  
samples of ransomware counted  
in Q1 2016<sup>7</sup>

---

Though in many cases the criminals will restore files when the ransom is paid, there is no guarantee this will be the case. Hackers have been known to share stolen private customer information free of charge on the web in order to punish a company for not paying their proposed ransom.

<sup>6,7,8</sup>McAfee, 2016.



Over  
**half a billion**  
malware samples  
were detected  
in Q1 2016<sup>8</sup>

---