

Ransomware

Ransomware (Erpressersoftware) hört sich nicht nur furchterregend an. Hacker verwenden diese Technik, um Sie aus Ihrem eigenen Gerät auszusperrern und gegen ein Lösegeld wieder hineinzulassen. Ransomware kann Sie in eine sehr unangenehme Lage bringen und sollte unbedingt vermieden werden.

Was ist Ransomware?

Ransomware (auch Scareware oder Erpressersoftware genannt) schränkt den Zugriff auf Ihr Computersystem ein, und verlangt die Zahlung eines Lösegelds, damit die Einschränkung wieder behoben wird. Die gefährlichsten Ransomware-Angriffe gingen von [WannaCry](#), [Petya](#), Cerber, CryptoLocker und Locky aus.

Woher stammt Ransomware

Ransomware wird von Betrügern erstellt, die sich sehr gut mit Computer-Programmierung auskennen. Ransomware kann über einen E-Mail-Anhang oder den Browser auf Ihren PC gelangen, falls Sie eine mit dieser Malware verseuchte Website besuchen. Die Software kann auch über das Netzwerk auf Ihren PC zugreifen.

Wie erkennt man Ransomware?

Man sieht sofort, wenn Ihr Gerät mit einer Ransomware infiziert ist, da Sie vermutlich gar nicht auf Ihren Computer zugreifen können.

Wie entfernt man Ransomware?

Verwenden Sie hierfür das Tool zur Ransomware-Entfernung Ihrer Virenschutz-Software, das eventuelle Ransomware-Versuche auf Ihrem Computer aufspüren und entfernen sollte.

Wie lässt sich gegen Ransomware vorbeugen?

- Achten Sie darauf, dass jede Software auf Ihrem Computer aktualisiert wurde, auch das Betriebssystem, der Browser und eventuelle Toolbar-Plugins, die Sie verwenden.
- Achten Sie auch darauf, dass Ihre Virenschutz-Software und der Firewall-Schutz aktuell sind.