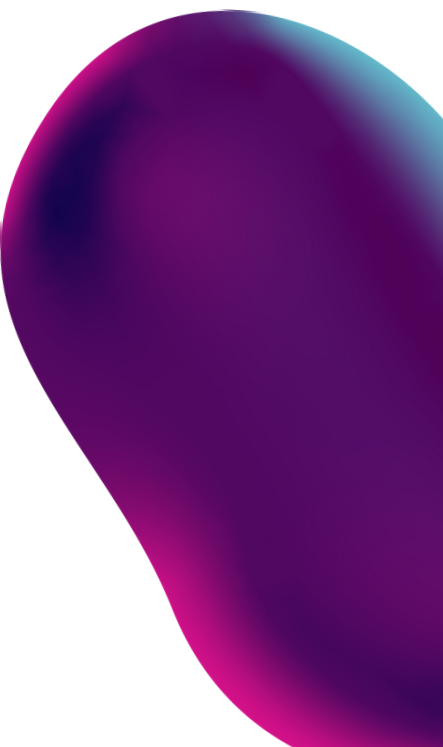
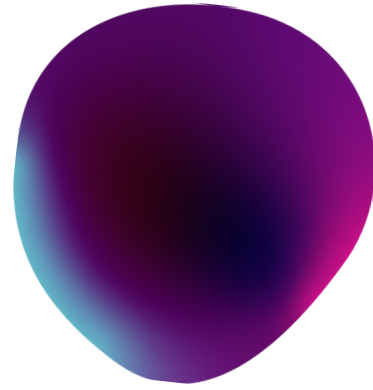


# The Future of Communication



The background features several abstract, organic shapes in shades of purple and blue. A large, irregular shape occupies the upper right quadrant, with a smaller, more circular shape positioned above it. In the bottom right corner, there is a smaller, elongated shape. The colors transition from a deep purple in the center of the shapes to a lighter blue at the edges.

**RANSOMWHERE**

# What is Ransomware?

Ransomware is a type of attack where threat actors take control of a target's assets and demand a ransom in exchange for the return of the asset's availability and confidentiality. The victim usually shortly after receives a blackmail note by pop-up, pressing the victim to pay a ransom (hence the name) to regain full access to system and files. There are three key elements in every ransomware attack: assets, actions and blackmail.



# How does it work?

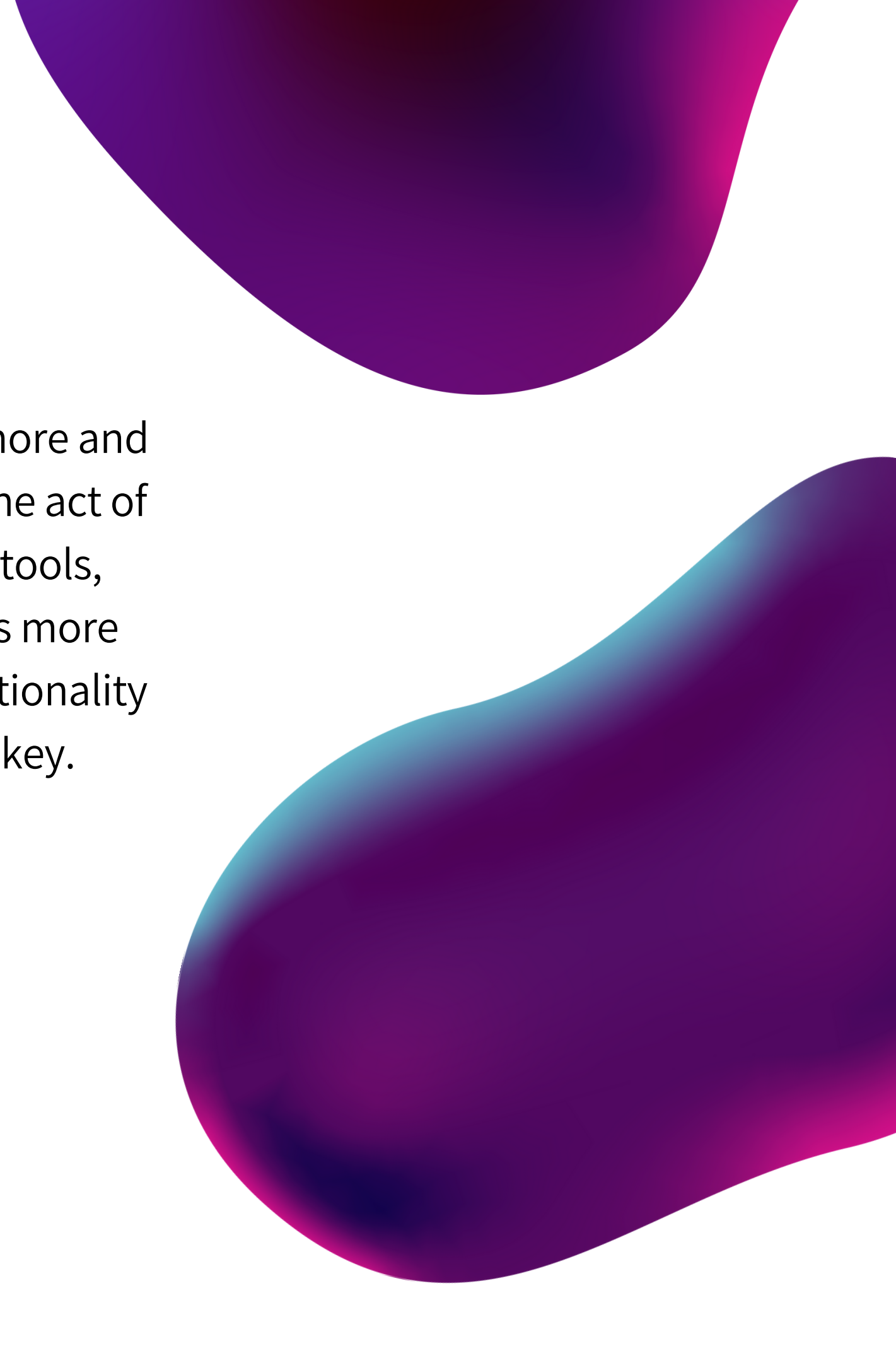
**Ransomware is a type of malware which prevents you from accessing your device and the data stored on it, usually by encrypting your files. A criminal group will then demand a ransom in exchange for decryption.**





# Use of ransomware

A user of a system infected with ransomware is usually confronted with an extortion message (in many cases a windows popup) asking the victim to pay a ransom fee to the attacker in order to regain access to their system and files. The already mentioned Cryptolocker accepts payments in the digital currency Bitcoins, which gives the attacker an additional layer of anonymity. In the case of Cryptolocker the victim, after payment, receives the key and the method to decrypt their files again and regain full access.



It is reported that criminals, their tools and their back office structure gets more and more sophisticated and (in a distorted way) more "user friendly". Not only the act of intrusion into a victims system is done with utmost precision and elaborate tools, but also the act of "supporting" the victim in restoring their systems receives more and more attention by the criminals. Some groups even offer helpdesk functionality for victims facing problems with bitcoins, payment or the application of the key.

# How to defend against ransomware

- Back up your data.
- Secure your backups.
- Use security software and keep it up to date.
- Practice safe surfing.
- Only use secure networks.
- Stay informed. Implement a security awareness program.



## Source

<https://www.trellix.com/en-us/security-awareness/ransomware/what-is-ransomware.html>  
Enisa.europa.eu