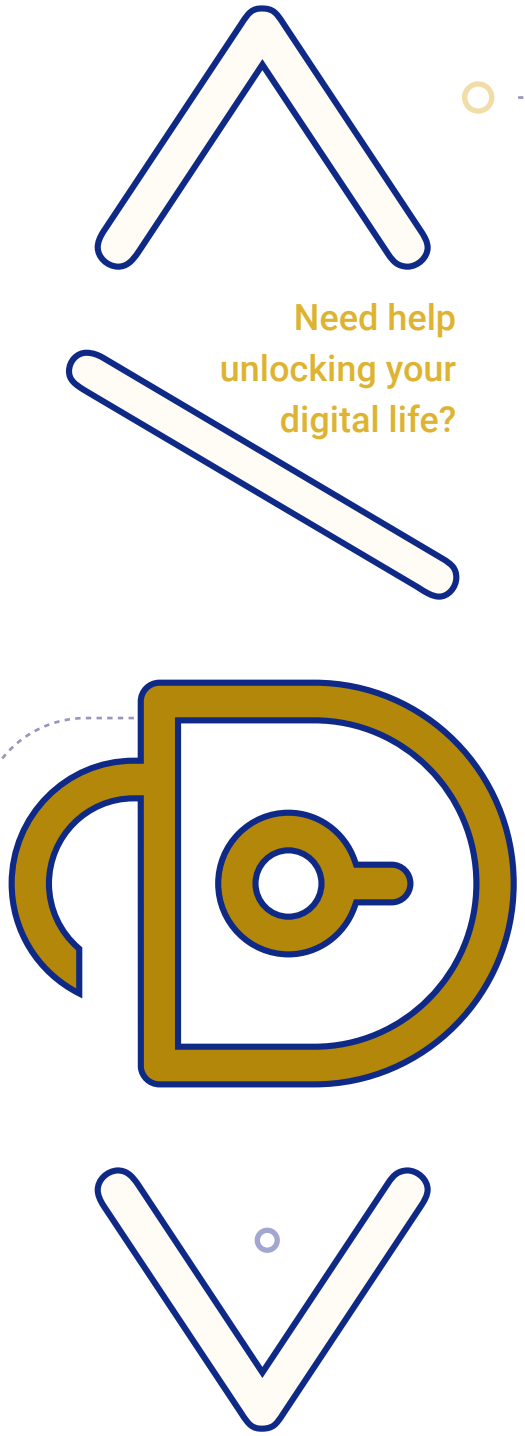
NO MORE RANSOM



Need help unlocking your digital life?

No More Ransom

# Need help unlocking your digital life?

**No More Ransom (NMR) showcases the value of public-private cooperation in disrupting criminal businesses with ransomware connections. Victims should no longer be forced to either pay a ransom or lose their files. By restoring access to their infected systems free of charge, we provide users with a third choice they did not have before.**

## What is ransomware?

Ransomware is a type of malware that prevents or limits users from accessing their systems or devices. The malware asks them to pay a ransom through specific online payment methods by a certain deadline to regain control of their data.

The infection can happen in many different ways, such as:

- visiting compromised websites;
- downloading fake application updates or compromised software;
- clicking on malicious links and attachments embedded in phishing emails;
- connecting infected external devices (e.g. USBs) to the computer system.

## What is No More Ransom?

NMR is a public-private partnership between law enforcement and industry leaders launched in July 2016.

Through www.nomoreransom.org, the project aims to:

- assist victims in the recovery of their encrypted files;
- raise awareness of the ransomware threat in the public arena;
- provide direct links to the national police agencies of the EU Member States and beyond to encourage citizens to report the attacks.

## How does it work?

1. The victim uploads two encrypted files and the ransomware note to the NMR Crypto Sheriff.
2. The Crypto Sheriff matches the information against a list of available decryption tools.
3. If there is a positive hit, the link to the tools is provided. The victim only needs to follow the instructions to unlock their files.
4. If no tool is available at the moment, the victim is advised to continue checking in the future, as new tools are added on a regular basis.

## Who can join the project?

Official entities from all sectors bringing a unique skill set (an approval procedure applies).

There are two partnership levels:

- **Associate partner:** providing unique decryption tools or decryption keys not yet available in the project portal. The signature of a dedicated legal agreement applies.
- **Supporting partner:** promoting the NMR project in their geographical area of influence or service, contributing material for prevention campaigns and translating portal content into different languages. Only a consent form is required.

# Advice for victims

## How can you avoid becoming infected with ransomware?

- Regularly back up data stored on your computer. Keep at least one copy offline.
- Do not click on links in unexpected or suspicious emails.
- Browse and download only official versions of software and always from trusted websites.
- Use robust security products to protect your system from all threats, including ransomware.
- Ensure that your security software and operating system are up-to-date.
- Be wary while browsing the internet and do not click on suspicious links, pop-ups or dialogue boxes.
- Do not use high privilege accounts (accounts with administrator rights) for daily business.

## Infected?

- Always visit www.nomoreransom.org to check whether you have been infected with one of the ransomware variants for which there are decryption tools available free of charge.
- Don't pay the ransom. You will be financing criminals and encouraging them to continue their illegal activities.
- Report it to your national police. The more information you provide, the more effectively law enforcement can disrupt the criminal enterprise.
- Disconnect your device from the internet or other network connections (such as home Wi-Fi) as soon as possible in order to prevent the infection from spreading.
- Format the hard drive of the infected device, reinstall the operating system and apps, run any available updates and restore the locked files from your backup device (if you have one).