Need help unlocking your digital life?

Communication toolkit for partners

NO MORE RANSOM!

INTRODUCTION

This toolkit contains a range of resources to help No More Ransom (NMR) official partners to promote the online portal through their corporate communication channels.

It includes:

1. Information about the initiative
2. Main functionalities – how does the portal work?
3. Key messages
4. Assets
5. Social media
6. Recommendations – how can partners support?

> The promotion of the NMR portal is to be done without commercial interests and it does not imply endorsement of the partners' products or services by the NMR founding members.

If you have any questions about NMR or these resources, please contact nomoreransom@europol.europa.eu

1/ ABOUT THE INITIATIVE

No More Ransom (NMR) is a non-commercial public-private partnership between law enforcement and industry leaders launched in July 2016. Its central governance is currently managed by the three founding members: Europol, the High Tech Crime Unit of the Netherlands' Police and McAfee.

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

- assist victims in the recovery of their encrypted files;
- raise awareness of the problem of ransomware in the public arena;
- provide direct links to national police agencies worldwide to encourage citizens to report the cases.

Official entities from all sectors bringing a unique skill set can join the project. There are two partnership levels:

- **Associate partner:** providing unique decryption tools or decryption keys.
- **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.

This toolkit applies to both levels.

The full list of partners can be consulted here: https://www.nomoreransom.org/en/partners.html

2/ MAIN FUNCTIONALITIES – HOW DOES THE PORTAL WORK?

THE CRYPTO SHERIFF

1. The victim uploads two encrypted files and the ransomware note.

2. The Crypto Sheriff matches the information against the list of available decryption tools.

3. If there is a positive hit, the link to the tool is provided. The victim only needs to follow the instructions to unlock their files.

4. If no tool is available, the victim is advised to continue checking in the future, as new tools are added on a regular basis.

List of available tools:
https://www.nomoreransom.org/en/decryption-tools.html

PREVENTION ADVICE

Basic tips aiming to educate the public about how to avoid their devices becoming infected with ransomware in the first place.

List of tips:
https://www.nomoreransom.org/en/prevention-advice.html

REPORT A CRIME

For those people that do become a victim, the portal offers direct links to report to the law enforcement authorities of the countries that support the NMR initiative.

List of available police websites:
https://www.nomoreransom.org/en/report-a-crime.html

MULTI-LANGUAGE

The portal was initially launched in English. Since then, it has been translated to more than 30 languages. Visitors are prompted to select their preferred language when they access the resources.

3/ KEY MESSAGES

- 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 general advice is not to pay the ransom. There is no guarantee that the victim will receive the decryption key in return. By sending the money, victims will be financing the criminals and encouraging them to continue their illegal activities.
- Law enforcement and industry partners have joined forces to disrupt criminal businesses with ransomware connections. NMR showcases the value of non-commercial public-private cooperation.
- 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, NMR provides users with a third choice they did not have before.
- It is much easier to avoid the ransomware threat than it is to deal with an infected system. Follow the NMR prevention advice.
- Ransomware is a crime. Always report it to the competent national authorities. This will help to catch the criminals and prevent other users from becoming infected.

!

- The NMR portal is not used to collect, process or store personal data. The encrypted files uploaded by the victim get deleted from the system as soon as the Crypto Sheriff finalises the assessment. The NMR portal does not and cannot access the content of the uploaded files.

4/ ASSETS

Logo

CMYK: 74 68 66 88
RGB: 7 7 7
HEX: 070707

Black version

CMYK: 0 0 0 0
RGB: 255 255 255
HEX: ffffff

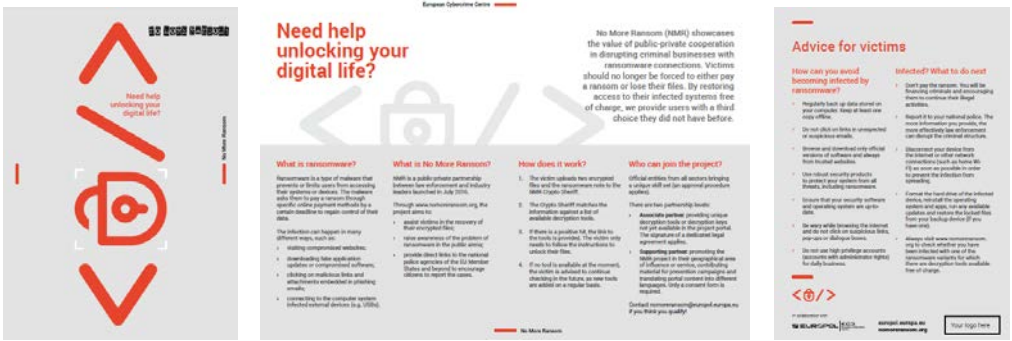
White version, dark backgrounds

To preserve the integrity of the NMR logo, always maintain a minimum clear space around it. This clear space isolates the logo from other competing graphic elements such as other logos, photography or background patterns that may divert attention.

For co-branding with the logo of a NMR partner make sure all logos have equal and balanced visual weight and align them with each other horizontally.

! The proportions of the NMR logo must be kept intact at all times.

Flyer



NMR partners are strongly encouraged to distribute the NMR flyer as they see fit.

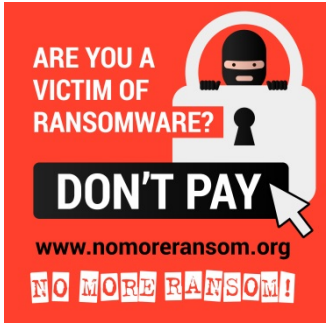
The colours and fonts can be adjusted to the partner's corporate style. Only the NMR logo and the overall design are to remain in its original specifications.

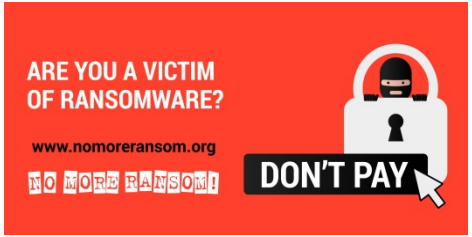
The partner's logo can be added in the designated area on the back cover.

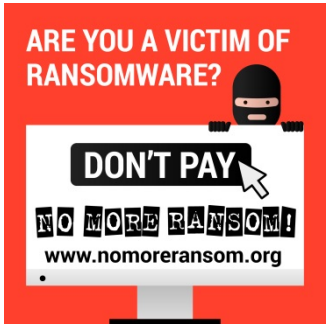
The flyer can be translated at the partner's discretion.

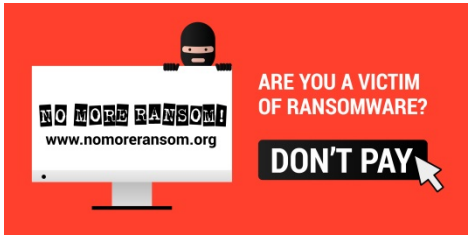
4/ ASSETS

Website button









NMR partners are strongly encouraged to display the NMR web button on their corporate website.

The button is to be hyperlinked to www.nomoreransom.org

It is advised to place the button preferably in the website Home; or alternatively, in a ransomware related page.

The button is available in two different designs and formats, which can be used at the partner's discretion.

Colours and fonts can be adjusted to the partner's corporate style, only the NMR logo and the overall design are to remain in their original specifications.

The sentence 'Are you a victim of ransomware?' can be translated at the partner's discretion.

5/ SOCIAL MEDIA – GENERAL GUIDELINES

- If possible, always include the official hashtags: #NoMoreRansom and #DontPay
- If possible, link to the NMR portal or relevant section within https://nomoreransom.org
- We have prepared a wide range of messages that can be used on any social media platform: Twitter, Facebook, Instagram, LinkedIn, etc.
- The messages cover different aspects of the initiative. The examples can be used as they are, or amended as needed, in order to suit your style and/or communications guidelines.
- Alternatively, please feel free to write your own messages.
- The content is provided in English, but you are welcome to translate/adjust it to your national language.

Follow Europol's Twitter accounts (@EC3Europol and @Europol) for regular updates on new tools, partners and languages and amplify the news among your own audience!

5/ SOCIAL MEDIA – MESSAGES

- Pay No More! Victims of #ransomware can recover their files for free thanks to the #NoMoreRansom initiative.

  Visit https://www.nomoreransom.org

- 'WARNING! Your personal files are encrypted. You can't get them back unless you pay a ransom'. If this happens to you… #DontPay! We can help you unlock your digital life.

  Visit https://www.nomoreransom.org to access free decryption tools and more. #NoMoreRansom

- Protect your devices and your files from #ransomware by following simple #prevention advice.

  Avoid becoming a victim, follow the #NoMoreRansom tips: https://www.nomoreransom.org/en/prevention-advice.html

- What can you find in the #NoMoreRansom portal?

  - Free decryption tools
  - Prevention tips
  - Reporting links to national law enforcement

  Visit https://www.nomoreransom.org, available in more than 30 languages!

- Have you fallen victim to #ransomware?

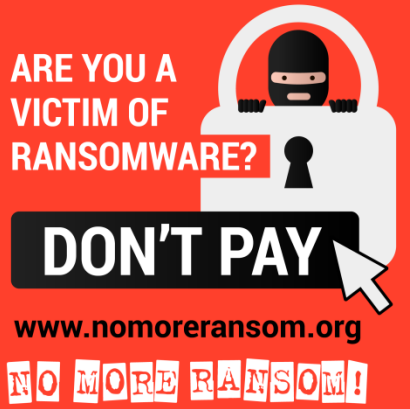
  REPORT IT! the #NoMoreRansom portal gives you direct lines to #lawenforcement worldwide: https://www.nomoreransom.org/en/report-a-crime.html

  #DontPay

6/ RECOMMENDATIONS – HOW CAN PARTNERS SUPPORT?

We encourage you to support NMR in the following ways:

- Sharing the official press releases issued on a regular basis by Europol;
- Adding the NMR button to your corporate website;
- Sharing the suggested messages on social media and/or creating your own ones;
- Helping to promote the portal's existence through any other corporate means available, such as blogs, intranet, customers' distribution lists, display of information (e.g. print out copies of the flyer) in local branches, etc.



In cooperation with

EUROPOL | EC3 European Cybercrime Centre