Mitigating malware and ransomware attacks

How to defend organisations against malware or ransomware attacks.

This guidance helps private and public sector organisations deal with the effects of malware (which includes ransomware). It provides actions to help organisations prevent a malware infection, and also steps to take if you're already infected.

Following this guidance will reduce:

- the likelihood of becoming infected
- the spread of malware throughout your organisation
- the impact of the infection

> If you've already been infected with malware, please refer to our list of urgent steps to take

For advice on minimising potential harm smaller organisations should refer to the NCSC's Small Business Guide. For information about protecting your devices at home, please read our guidance especially written for individuals and families.

In this guidance

What are malware and ransomware?

Malware is malicious software, which - if able to run - can cause harm in many ways, including:

- causing a device to become locked or unusable
- stealing, deleting or encrypting data
- taking control of your devices to attack other organisations
- obtaining credentials which allow access to your organisation's systems or services that you use
- 'mining' cryptocurrency
- using services that may cost you money (e.g. premium rate phone calls).

Ransomware is a type of malware that prevents you from accessing your computer (or the data that is stored on it). The computer itself may become locked, or the data on it might be stolen, deleted or encrypted. Some ransomware will also try to spread to other machines on the network, such as the Wannacry malware that impacted the NHS in May 2017.

Usually you're asked to contact the attacker via an anonymous email address or follow instructions on an anonymous web page, to make payment. The payment is invariably demanded in a cryptocurrency such as Bitcoin, in order to unlock your computer, or access your data. However, even if you pay the ransom, there is no guarantee that you will get access to your computer, or your files.

Occasionally malware is *presented* as ransomware, but after the ransom is paid the files are not decrypted. This is known as wiper malware. **For these reasons, it's essential that you always have a recent offline backup of your most important files and data**.

Should you pay the ransom?

Law enforcement do not encourage, endorse, nor condone the payment of ransom demands. If you do pay the ransom:

- there is no guarantee that you will get access to your data or computer
- your computer will still be infected
- you will be paying criminal groups
- you're more likely to be targeted in the future

Attackers will also threaten to publish data if payment is not made. To counter this, organisations should take measures to minimise the impact of data exfiltration. The NCSC's guidance on Protecting bulk personal data and the Logging and protective monitoring guidance can help with this.

Using a defence in depth strategy

Since there's no way to **completely** protect your organisation against malware infection, you should adopt a 'defence-in-depth' approach. This means using layers of defence with several mitigations at each layer. You'll have more

opportunities to detect malware, and then stop it before it causes real harm to your organisation.

You should assume that some malware **will** infiltrate your organisation, so you can take steps to limit the impact this would cause, and speed up your response.

Actions to take

There are some actions you can take to help prepare your organisation from potential malware and ransomware attacks.

+ Show all

Action 1: make regular backups Show

Action 2: prevent malware from being delivered and spreading to devices Show

Action 3: prevent malware from running on devices Show

Action 4: prepare for an incident Hide

Malware attacks, in particular ransomware attacks, can be devastating for organisations because computer systems are no longer available to use, and in some cases data may never be recovered. If recovery is possible, it can take several weeks, but your corporate reputation and brand value could take a lot longer to recover. The following will help to ensure your organisation can recover quickly.

- Identify your critical assets and determine the impact to these if they were affected by a malware attack.
- Plan for an attack, even if you think it is unlikely. There are many examples of organisations that have been impacted by collateral malware, even though they were not the intended target.

- Develop an internal and external communication strategy. It is important that the right information reaches the right stakeholders in a timely fashion.
- Determine how you will respond to the ransom demand and the threat of your organisation's data being published.
- Ensure that incident management playbooks and supporting resources such as checklists and contact details are available if you do not have access to your computer systems.
- Identify your legal obligations regarding the reporting of incidents to regulators, and understand how to approach this.
- Exercise your incident management plan. This helps clarify the roles and responsibilities of staff and third parties, and to prioritise system recovery. For example, if a widespread ransomware attack meant a complete shutdown of the network was necessary, you would have to consider:

- how long it would take to restore the minimum required number of devices from images and re-configure for use
- how you would rebuild any virtual environments and physical servers
- what processes need to be followed to restore servers and files from your backup solution
- what processes need to be followed if onsite systems and cloud backup servers are unusable, and you need to rebuild from offline backups
- how you would continue to operate critical business services

- After an incident, revise your incident management plan to include lessons learnt to ensure that the same event cannot occur in the same way again.

The NCSC's free Exercise in a Box online tool, contains materials for setting up, planning, delivery, and post-exercise activity.

Steps to take if your organisation is already infected

If your organisation has already been infected with malware, these steps may help limit the impact:

1. Immediately disconnect the infected computers, laptops or tablets from all network connections, whether wired, wireless or mobile phone based.
2. In a very serious case, consider whether turning off your Wi-Fi, disabling any core network connections (including switches), and disconnecting from the internet might be necessary.
3. Reset credentials including passwords (especially for administrator and other system accounts) - but verify that you are not locking yourself out of systems that are needed for recovery.
4. Safely wipe the infected devices and reinstall the OS.
5. Before you restore from a backup, verify that it is free from any malware. You should only restore from a backup if you are **very** confident that the backup **and** the device you're connecting it to are clean.
6. Connect devices to a clean network in order to download, install and update the OS and all other software.
7. Install, update, and run antivirus software.
8. Reconnect to your network.
9. Monitor network traffic and run antivirus scans to identify if any infection remains.

The NCSC has jointly published an advisory: Technical Approaches to Uncovering and Remediating Malicious Activity, which provides more detailed information about remediation processes.

> **Note**
> Files encrypted by most ransomware typically have no way of being decrypted by anyone other than the attacker. However, the No More Ransom Project provides a collection of decryption tools and other resources from the main anti-malware vendors, which may help.

Further advice

There's plenty of further reading and services that can help you protect your organisation from malware and ransomware attacks.

- **Report**
  Cyber security incidents can be reported to the NCSC by visiting https://report.ncsc.gov.uk/. We also encourage reporting to the Action Fraud website.
- **Cyber Incident Response**
  The NCSC runs a commercial scheme called Cyber Incident Response, where certified companies provide support to affected organisations.
- **Cyber Essentials**
  You may also wish to consider the Cyber Essentials certification scheme (which covers a number of these mitigations), so your customers and partners can see that you have addressed these risks. Many of these mitigations also work well against other types of attack, such as phishing.
- **Additional guidance**
  Follow the NCSC guidance on protecting your organisation from phishing attacks. Larger organisations / enterprises should refer to the NCSC's Device Security Guidance.

PUBLISHED

13 February 2020

REVIEWED

9 September 2021

VERSION

/

3.0

WRITTEN FOR

Cyber security professionals

Large organisations

Public sector