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 is malware?
- Actions to take
- Steps to take if your organisation is already infected
- Further advice

What are malware and ransomware?

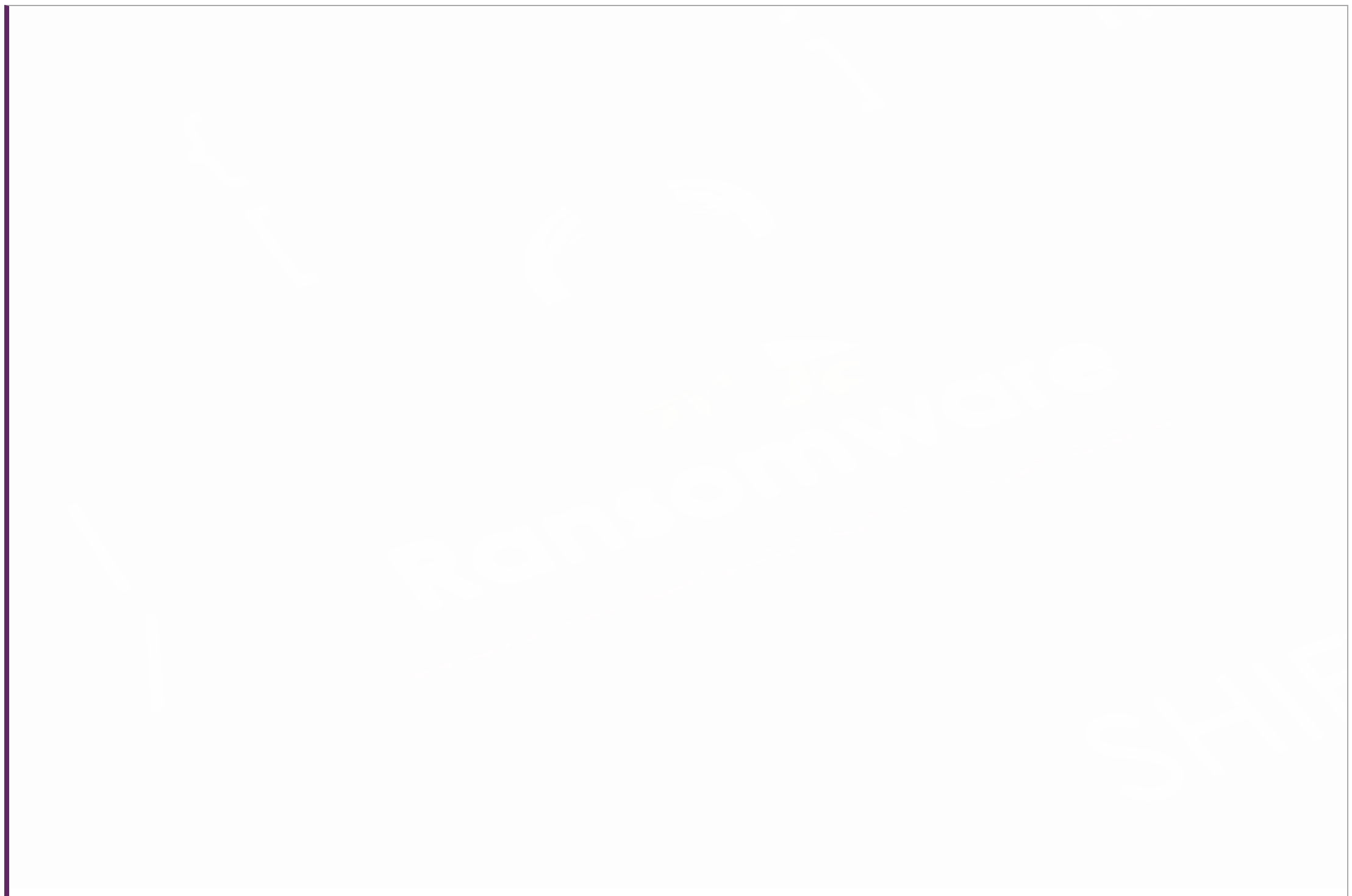
Malware is malicious software, which - if able to run - can cause harm in many ways, including:

- 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

Up-to-date backups are the most effective way of recovering from a ransomware attack, you should do the following.

- Make regular backups of your most important files - it will be different for every organisation - check that you know how to restore files from the backup, and regularly test that it is working as expected.
- Ensure you create offline backups that are kept separate, in a different location (ideally offsite), from your network and systems, or in a cloud service designed for this purpose, as ransomware actively targets backups to increase the likelihood of payment. Our blog on 'Offline backups in an online world' provides useful additional advice for organisations.
- Make multiple copies of files using different backup solutions and storage locations. You shouldn't rely on having two copies on a single removable drive, nor should you rely on multiple copies in a single cloud service.
- Make sure that the devices containing your backup (such as external hard drives and USB sticks) are **not** permanently connected to your network. Attackers will target connected backup devices and solutions to make recovery more difficult.
- You should ensure that your cloud service protects previous versions of the backup from being immediately deleted and allows you to restore to them. This will prevent both your live and backup data becoming inaccessible - cloud services often automatically synchronise immediately after your files have been replaced with encrypted copies.
- Ensure that backups are only connected to known clean devices before starting recovery.
- Scan backups for malware before you restore files. Ransomware may have infiltrated your network over a period of time, and replicated to backups before being discovered.
- Regularly patch products used for backup, so attackers cannot exploit any known vulnerabilities they might contain.

There have been cases where attackers have destroyed copied files or disrupted recovery processes before conducting ransomware attacks. Ideally, backup accounts and solutions should be protected using Privileged Access Workstations (PAW) and hardware firewalls to enforce IP allow listing. Multi-factor Authentication (MFA) should be enabled, and the MFA method should not be installed on the same device that is used for the administration of backups. Privileged Access Management (PAM) solutions remove the need for administrators to directly access high-value backup systems.

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

+ Show

You can reduce the likelihood of malicious content reaching your devices through a combination of:

- filtering to only allow file types you would expect to receive
- blocking websites that are known to be malicious
- actively inspecting content
- using signatures to block known malicious code

These are typically done by network services rather than users' devices. Examples include:

- mail filtering (in combination with spam filtering) which can block malicious emails and remove executable attachments. NCSC's Mail Check platform can also help eligible organisations with this. Please check your organisation's eligibility for Mail Check.
- intercepting proxies, which block known-malicious websites
- internet security gateways, which can inspect content in certain protocols (including some encrypted protocols) for known malware
- safe browsing lists within your web browsers which can prevent access to sites known to be hosting malicious content

Eligible organisations are encouraged to subscribe to the NCSC Protective Domain Name Service. This will prevent users from reaching known malicious sites. Please check your organisation's eligibility for PDNS.

Ransomware is increasingly being deployed by attackers who have gained access remotely via exposed services such as Remote Desktop Protocol (RDP), or unpatched remote access devices. To prevent this organisations should:

- disable RDP if it's not needed (if you're not sure if you're running RDP, we recommend you register with the NCSC's Early Warning service)
- enable MFA at all remote access points into the network, and enforce IP allow listing using hardware firewalls
- use a VPN that meets NCSC recommendations, for remote access to services; Software as a Service or other services exposed to the internet should use Single Sign-On (SSO) where access policies can be defined (for more information read our blogpost on protecting management interfaces)
- use the least privilege model for providing remote access - use low privilege accounts to authenticate, and provide an audited process to allow a user to escalate their privileges within the remote session where necessary
- patch known vulnerabilities in all remote access and external facing devices immediately (referring to our guidance on how to manage vulnerabilities within your organisation if necessary), and follow vendor remediation guidance including the installation of new patches as soon as they become available

Prevent malware spreading across your organisation by following NCSC guidance on preventing lateral movement. You should also:

- use MFA to authenticate users so that if malware steals credentials they can't easily be reused
- ensure obsolete platforms (Operating Systems (OS) and apps) are properly segregated from the rest of the network - refer to NCSC guidance on Obsolete Platforms for further details
- regularly review and remove user permissions that are no longer required, to limit the malware's ability to spread
- ensure system administrators avoid using their accounts for email and web browsing (to prevent malware being able to run with their high level of system privilege)
- practice good asset management, including keeping track of which versions of software are installed on your devices so that you can target security updates quickly
- keep devices and infrastructure patched, especially security-enforcing devices on the network boundary (such as firewalls and VPN products)

Action 3: prevent malware from running on devices

+ Show

A 'defence in depth' approach assumes that malware will reach your devices. You should therefore take steps to prevent malware from running. The measures required will vary for each device type, OS and version, but in general you should look to use device-level security features. Organisations should:

- centrally manage devices in order to only permit applications trusted by the enterprise to run on devices, using technologies including AppLocker, or from trusted app stores (or other trusted locations)
- consider whether enterprise antivirus or anti-malware products are necessary, and keep the software (and its definition files) up to date
- provide security education and awareness training to your people, for example NCSC's Top Tips for Staff
- disable or constrain scripting environments and macros, by:
    - enforcing PowerShell Constrained Language mode via a User Mode Code Integrity (UMCI) policy - you can use AppLocker as an interface to UMCI to automatically apply Constrained Language mode
    - protecting your systems from malicious Microsoft Office macros
- disable autorun for mounted media (prevent the use of removable media if it is not needed)

In addition, attackers can force their code to execute by exploiting vulnerabilities in the device. Prevent this by keeping devices well-configured and up to date. We recommend that you:

- install security updates as soon as they become available in order to fix exploitable bugs in your products
- enable automatic updates for OSs, applications, and firmware if you can
- use the latest versions of OSs and applications to take advantage of the latest security features
- configure host-based and network firewalls, disallowing inbound connections by default

The NCSC's Device Security Guidance provides advice on how to achieve this across a variety of platforms.

Action 4: prepare for an incident

+ Show

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 read our guidance on responding and recovering from disruptive cyber attacks.

GUIDANCE

Recovering from a highly disruptive cyber attack

Practical guidance for leaders and cyber teams, covering early response, recovery to minimum viable operations, and rebuild.

PART OF What to do when cyber attacks disrupt your organisation

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 Report 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