Malware Protection Guide: Defensive Layer 1

# Malware Protection Guide: Defensive Layer 1

**Parent topic:** [Malware Protection Guide - Overview](malware-protection-guide-introduction.html)

## Introduction

This guide explains the types of controls that need to be implemented to form the first of three layers of defence. Layer 1 reduces the likelihood that malicious content will reach the Ministry of Justice (MoJ) network through implementing the controls outlined in this guide. This guide is a sub-page to the [Malware Protection Guide](malware-protection-guide-introduction.html).

### Who is this for?

This Malware Protection information is mainly intended for in-house MoJ Digital and Technology staff who are responsible for implementing controls throughout technical design, development, system integration and operation. This includes DevOps, Software Developers, Technical Architects, and Service Owners. It also includes Incident Managers from the Event, Problem, Incident, CSI and Knowledge (EPICK) Team.

Other MoJ bodies, agencies, contractors, or IT suppliers and partners who in any way design, develop or supply services (including processing, transmitting and storing data) for, or on behalf of the MoJ, will also find this information helpful.

## Defensive Layer 1: Preventing malicious code from being delivered to devices

|  |
| --- |
| Do |
| ✔ Ensure that all public facing URLs that are assigned to services owned or managed on behalf of the MoJ are protected by enrolling them in the [NCSC Web Check](https://www.ncsc.gov.uk/information/web-check) service. Contact [security@justice.gov.uk](mailto:security@justice.gov.uk) to add URLs to this service. |
| ✔ Use of the [Protective Domain Naming Service subscription](public-sector-dns.html) service should be configured for end users. As a Central Government department, systems owned or managed on behalf of the MoJ are permitted to use the service for free. Contact [security@justice.gov.uk](mailto:security@justice.gov.uk) to be included in this service. |
| ✔ Ensure that if you are developing a system or application where any element is outsourced, such as hosting a service in the cloud, you must understand and record security related responsibilities of the MoJ, of the cloud service provider and any other supplier. For guidance on what responsibilities to consider, see the [NCSC guidance on Cloud Security](https://www.ncsc.gov.uk/collection/cloud-security) or [ISO27017](https://www.iso.org/standard/43757.html). These provide guidelines for information security controls applicable to the provision and use of cloud services. |
| ✔ Ensure that if you are managing an email system, all inbound emails to the MoJ are scanned for malware. For Microsoft systems this is provided by Office 365 which quarantines any suspected malware. |
| ✔ Avoid the need for removable media by using existing approved online collaboration services where possible, for example Office 365. Where removable media has to be used, it must be scanned by approved Anti-virus before and during use. |
| ✔ All web traffic must be routed through a proxy which logs and monitors internet access. This reduces the chance of malicious sites infecting end user devices. The proxy is configured in agreement with the security team. Email must also be routed through email scanning services. Direct Internet access should only be configured for update services, and by exception only. |
| ✔ Allow the installation of applications only from approved stores. |
| ✔ Systems must be able to be updated and must be kept up-to-date with OS and application upgrades and patches. Where possible, software updates should be configured to update automatically. See the [Vulnerability Scanning and Patch Management Guide](vulnerability-scanning.html) for further information. |
| ✔ A formal process must be developed and documented to ensure all firewall configuration changes are approved before being implemented. |
| ✔ Be aware of the risks of '[watering hole attacks](https://en.wikipedia.org/wiki/Watering_hole_attack)' that use GitHub or other open source code repositories. These attacks place malware into popular sites. Avoid trusting code, components, or other resources from popular sites. See the Access Control Guide for further information. |
| ✔ When developing a new system. ensure that it's properly scoped to understand what, if any, appropriate anti-malware software is required. You must also ensure that if the eventual system has anti-malware software, that it is configured to minimise the impact of scans on system or application performance. Contact the [Operational Security Team (OST)](#contact-details) for further information on how to do this. |
| ✔ Ensure that if you are responsible for patching or installing security updates of an in-house developed system or application follow the processes and requirements set out in the [Vulnerability Scanning and Patch Management Guide](vulnerability-scanning.html). The success of these updates should be validated using automated vulnerability scanning services. |
| ✔ Use hardened devices including approved and assured Gold Builds. Further information can be found in the Technical Controls guidance; contact the [Cyber Assistance Team](#contact-details) for help with this. |

|  |
| --- |
| Don't |
| ✖ Allow externally obtained (from outside the MoJ) executable software to run. This includes auto-running macros. |
| ✖ Try to circumvent any security controls such as safe browsing lists or removable media controls; they are in place to protect the MoJ from malware. |
| ✖ Connect any devices not procured and/or managed by the MoJ to trusted networks. Devices connected to MoJ trusted networks must be under MoJ management. |

## Contact details

* Contact the Cyber Assistance Team for advice on protecting against malware – [CyberConsultancy@digital.justice.gov.uk](mailto:CyberConsultancy@digital.justice.gov.uk)
* Contact the Technology Service Desk to report suspected malware:Telephone: 0800 917 5148.
* Contact the Operational Security Team (OST) - [Operationalsecurityteam@justice.gov.uk](mailto:Operationalsecurityteam@justice.gov.uk)