Malware Protection Guide - Overview

# Malware Protection Guide - Overview

* [**Malware Protection Guide: Defensive Layer 1**](malware-protection-guidance-defensive-layer-1.html)
* [**Malware Protection Guide: Defensive Layer 2**](malware-protection-guidance-defensive-layer-2.html)
* [**Malware Protection Guide: Defensive Layer 3**](malware-protection-guidance-defensive-layer-3.html)

## Introduction

This guide introduces the information which explains your responsibilities in helping the Ministry of Justice (MoJ) to prevent, detect and recover from malware. The MoJ has a three layer defence approach aligning with the National Cyber Security Centre (NCSC) guidance to mitigate the risks posed by malware. If one layer of defence is compromised then malware should be blocked or detected by the next layer.

## Detailed information

For further guidance around implementing the three lines of defence to protect the MoJ from Malware, see the guides below.

* [Malware Protection Guidance - Defensive Layer 1](malware-protection-guidance-defensive-layer-1.html): Preventing malicious code from being delivered to devices - This section explains the preventative measures which should be taken to prevent malware from entering the MoJ's systems.
* [Malware Protection Guidance - Defensive Layer 2](malware-protection-guidance-defensive-layer-2.html): Preventing malicious code from being executed on devices - This section explains the controls which should be implemented to prevent malicious code from executing on the MoJ's systems if it evades Layer 1.
* [Malware Protection Guidance - Defensive Layer 3](malware-protection-guidance-defensive-layer-3.html): Increasing resilience to infection and enabling rapid response should an infection occur - This section explains how to minimise the impact of a successful malware intrusion through backing up information and limiting malware's ability to spread if the first two layers fail.

## Assessing the malware risk

Malware can affect different systems in very different ways depending on how they store, process and execute files and potentially attacker-supplied content. Each system needs to be assessed to understand the potential threat from malware to it, and to design appropriate controls for that situation. The MoJ Assurance Framework provides information on how this may be achieved. Contact the [Cyber Assistance Team](#contact-details) for help regarding the Assurance Framework.

## Who is this for?

The Malware Protection information is aimed at two audiences:

1. The 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.
2. Any other MoJ body, agency, contractors, 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.

## Contact details

* Contact the Cyber Assistance Team by email: [CyberConsultancy@digital.justice.gov.uk](mailto:CyberConsultancy@digital.justice.gov.uk)
* Contact the Technology Service Desk to report suspected malware:Telephone: 0800 917 5148.