#Ransomware

Ransomware is a type of malicious software created or used by cybercriminals. It prevents people or businesses from accessing their own data. The software takes hold of the data, holding it “hostage”, until a ransom payment is made to release it.

##Preventing Ransomware from taking hold of information

* Store all your information in official Ministry of Justice (MoJ) systems. This is general best practice, and also minimises the risk of the data being accessed by the hackers.
* Use a secure antivirus and firewall software. All official MoJ systems have these installed as standard.
* Use a trustworthy VPN when accessing public networks through wifi, for example when working remotely in a coffee shop. All official MoJ systems have a suitable VPN installed as standard.
* Ensure your laptop computer is updated regularly. All official MoJ systems do this for you automatically, as standard.
* Use multi-factor authentication (MFA) methods. Most MoJ systems support MFA, but you might have to enable it yourself.
* Do not provide any personal information to unknown contacts.
* Avoid unsecure apps or websites.

##Things to look out for if you suspect you have become victim to a ransomware attack

* Unable to open documents.
* Suspicious file names. Files encrypted by ransomware tend to end with .crypted or .cryptor, rather than the more typical names such as .docx, .pdf, or .jpeg.
* An unrecognised pop-up screen prevents access to your computer.

##What to do if you think a ransomware attack is affecting your system

In the event of a ransomware attack, or if you have suspicions one may be taking place, the first thing to do is to [contact your local IT Helpdesk](#incidents-and-contact-details).

With your help, the IT team attempt to determine which systems have been impacted, and can isolate them immediately. You might be asked to disconnect all your devices from the network or wifi connection, to prevent a further spread of attacks throughout the business.

##Incidents and contact details

**Note:** If you work for an agency or ALB, refer to your local incident reporting guidance.

For help with incidents, including theft and loss, contact:

* **DOM1/Quantum - Technology Service Desk**
* Tel: 0800 917 5148
* **Note:** The previous itservicedesk@justice.gov.uk email address is no longer being monitored.
* **Digital and Technology - Digital Service Desk**
  + Email: [servicedesk@digital.justice.gov.uk](mailto:servicedesk@digital.justice.gov.uk)
  + Slack: #digitalservicedesk
* **HMPPS Information and security**
  + Email: [informationmgmtsecurity@justice.gov.uk](mailto:informationmgmtsecurity@justice.gov.uk)
  + Tel: 0203 334 0324

For non-technology incidents, contact the MoJ Group Security Team: [mojgroupsecurity@justice.gov.uk](mailto:mojgroupsecurity@justice.gov.uk)

Contact the Privacy Team for information on Data Protection Impact Assessments: [privacy@justice.gov.uk](mailto:privacy@justice.gov.uk)

If you are not sure who to contact, ask the Operational Security Team:

* Email: [OperationalSecurityTeam@justice.gov.uk](mailto:OperationalSecurityTeam@justice.gov.uk)
* Slack: #security

For any further questions relating to security, contact: [security@justice.gov.uk](mailto:security@justice.gov.uk), or for security advice, contact the Cyber Assistance Team [CyberConsultancy@digital.justice.gov.uk](mailto:CyberConsultancy@digital.justice.gov.uk).

##Feedback

If you have any questions or comments about this guidance, such as suggestions for improvements, please contact: [IT policy content](mailto:itpolicycontent@digital.justice.gov.uk).