#Email

##Overview

This document provides you with guidance for safe and secure use of email within the Ministry of Justice (MoJ).

In general, always use email in an [acceptable way](acceptable-use.md).

In particular:

* Never circulate messages or material that contains obscene, profane, inflammatory, threatening, harassing (racially, sexually or otherwise), and disruptive, or otherwise offensive language.
* Don’t use email or other messaging systems for trivial debates or exchanges with an individual or group of people.
* Don’t use MoJ email or other messaging systems for anything other than appropriate business purposes.
* Don’t make statements that defame, slander or lower the reputation of the MoJ, any person or organisation.
* Don’t forward email [chain letters](#chain-letters) to your contacts. Instead, report them to [security@justice.gov.uk](mailto:security@justice.gov.uk).
* Avoid excessive use of email. Be aware of unsuitable attachments, for example video clips, images, or executable files.
* Avoid sending email to large numbers of recipients. Ask yourself if it really makes sense to “Reply All”?
* Keep your operating systems up to date to prevent susceptibility to viruses.
* Scan email attachments to detect viruses and other malware.

Be aware that the MoJ monitors the use of electronic communications and web-browsing. Your manager can request reports detailing your activity if they suspect inappropriate use of email or web-browsing facilities.

[Ask](#contacts-for-getting-help) if you want further information.

##Monitoring

The MoJ monitors all email for security purposes.

Specifically, communications may be monitored without notice and on a continual basis for a number of reasons including compliance with legal obligations, effective maintenance of IT systems, preventing or detecting unauthorised use or criminal activities (including cyber-intrusion), monitoring of service or performance standards, providing evidence of business transactions, and checking adherence to policies, procedures, and contracts.

In general, the MoJ monitors telephone usage, network, email and Internet traffic data (including sender, receiver, subject, attachments to an e-mail, numbers called, duration of calls, domain names of websites visited, duration of visits, and files uploaded or downloaded from the Internet) at a network level.

##Email threats

Although email is a powerful business tool, it has problems. In this guidance, we describe some of the problems, and how you can avoid them.

Email threats often use familiar email addresses to disguise attacks, or to pose as valid emails. Email threats are becoming more frequent and pose one of the biggest problems for MoJ systems and services.

There are many possible threats, including:

* Viruses: These can be spread between computers in emails or their attachments. They can make PCs, software or documents unusable.
* Spam: This is unsolicited mail sent in bulk. Clicking on links in spam email may send users to phishing websites or sites hosting malware. Often email spam mimics the addresses of people you know.
* Phishing: These are emails disguised to look like a legitimate company or bank to illegitimately obtain personal information. They usually ask you to verify your personal information or account details. Often links will direct you to a fake website, made to look like the real thing.
* Social engineering: In the context of security, social engineering refers to manipulating people to do something or divulge confidential information. For example, you might get a call from someone pretending to be from a software supplier, claiming that a virus has been found on your PC; they demand personal details before they can remove the virus.
* Spoofing: A spoofed email is where the sender (in this case, a criminal) purposely alters part of the email to make it look as though it was from someone else. Commonly, the sender’s name/address and the body of the message are made to look as though it was from a legitimate source. It is commonly used to trick the recipient into providing confidential information such as passwords, or to market an online service dishonestly, or to sell a bogus product. Check the real sender of any email you receive if you ever have any doubt or uncertainty. If the sending address is one you don’t recognise, do not click on any link contained within the email.

The MoJ scans approximately 14 million messages a month for threats (figures from November 2020). Of these, we might expect to find 1.4 million “spam” messages, 150,000 “phishing” messages, and about 1,000 malware messages (including viruses). Unfortunately, not every virus or spam email will be identified and blocked. The good news is that there are some simple steps you can take to reduce the threat:

* If you are not expecting the email, do not reply to it.
* If you are at all suspicious, do not divulge your details or any sensitive information.
* Avoid opening potential scam emails.
* Don’t open unexpected attachments or click on strange links in emails, even if the email appears to be from someone you know. Check the style and content; if it isn’t consistent with previous emails, it could be a scam.
* Do not reveal personal or other sensitive information in response to automatic email requests.
* Avoid sharing your business email address on the internet. These might be collected and used by automatic ‘harvesting’ software programs.
* Never use your MoJ email address to register for non-work related sites.

If you think you’ve received a scam email, or a virus, [report it immediately](reporting-an-incident.md). Do not click on any link or forward it to anyone. Only delete it from your inbox when you have been told to do so.

##Further reading from the NCSC

[Email security and anti-spoofing](https://www.ncsc.gov.uk/guidance/email-security-and-anti-spoofing)

##Other email problems

##Auto-forward

Auto-forwarding is where you get your email system to send emails automatically to another account. This might seem very useful, especially if for some reason you can’t access your normal business email account, for example while you are away on holiday.

But auto-forwarding is very risky.

You can’t be certain that the forwarded emails are safe to send to the new account. For example, the new account might have weaker technical security, making it easier for a hacker to break in and read your email.

You might also be auto-forwarding emails sent to you from outside the MoJ; perhaps from another government department or commercial organisation.

When an email is sent to you, you are responsible for ensuring that everything in the email is handled correctly. This means looking after it to the standard required for that information. You mustn’t send that information to another email address, where the required security standards might not be met.

Never use auto-forwarding to forward emails from your MoJ business email address to another non-MoJ email address. In particular, never forward email from your MoJ business email address to a personal email address.

**Note:** An external email service is any service that is outside the gov.uk domain.

There might be occasions when you have a genuine business need to auto-forward email to another email account, where the new address has the same or higher security standards. An example is forwarding from an MoJ business email address to another MoJ business email address. If you have business need for this, [ask](#contacts-for-getting-help) for help.

##Chain letters

These are letters sent to several people who are asked to send copies to several others. They sometimes threaten that bad things will happen if the letter is not forwarded. Chain letters are a hoax.

Chain letters usually do not have the name and contact information of the original sender so it is impossible to check on their authenticity.

Legitimate warnings and solicitations will always have complete contact information from the person sending the message.

Newer chain letters may have a name and contact information but that person either does not exist or is not responsible for the hoax message.

Warnings without the name of the person sending the original notice, or warnings with names, addresses and phone numbers that do not actually exist, are probably hoaxes.

Don’t circulate warnings yourself; real warnings about viruses and other network problems are issued for everyone by MoJ technical services.

**Note:** When in doubt, don’t send it out.

##Scams

Scams are “get rich quick” schemes. They make claims such as promising your bank account will soon be stuffed full of cash if follow the detailed instructions in the letter or email. In reality, it is an illegal plan for making money.

A typical scam includes the names and addresses of several individuals whom you may or may not know. You are instructed to send a certain amount of money to the person at the top of the list, and then remove that name and add yours to the bottom.

You are then supposed to mail copies of the letter or email to a few more individuals who will hopefully repeat the entire process. The letter promises that if they follow the same procedure, your name will gradually move to the top of the list and you’ll receive money.

Other high-tech scams using IT also exist. They might be sent over the internet, or may require the copying and mailing of computer disks rather than paper. Regardless of the technology used to advance the scheme, the end result is still the same.

Scams are a bad investment. You certainly won’t get rich. You will receive little or no money. The few pounds you may get will probably not be as much as you spend making and mailing copies of the letter if hard copy.

By their very nature, scams are harassing. Sending such mails using MoJ facilities is prohibited. The misuse of computer resources to harass other individuals or groups is unacceptable. Any person tempted to forward an email scam should familiarise themselves with the HR intranet pages, particularly the section regarding disciplinary action and electronic communications.

**Note:** Scams also clog up the system and reduce the efficiency of our servers.

##How to recognise a scam

From the older printed letters, to the newer electronic kind, scams follow a similar pattern, with three recognisable parts:

* A hook: this to catch your interest and get you to read the rest of the letter. Hooks used to be “Make Money Fast” or “Get Rich” or similar statements related to making money for little or no work. Electronic chain letters also use the “free money” type of hooks, but have added hooks like “Danger!” and “Virus Alert” or “A Little Girl is dying”. These tie into our fear for the survival of our computers or into our sympathy for some poor unfortunate person.
* A threat: when you are hooked, you read on to the threat. Most threats used to warn you about the terrible things that will happen if you do not maintain the chain. Others play on greed or sympathy to get you to pass the letter on. The threat often contains official or technical sounding language to get you to believe it is real.
* A request: some older chain letters ask you to send money to the top ten names on the letter and then pass it on. The electronic ones simply admonish you to “Distribute this letter to as many people as possible.” They never mention clogging the internet or the fact that the message is a fake; they only want you to pass it on to others.

If it sounds too good to be true, then it is!

##Bogus calls

There are a range of scams that can target you at home or at work. Callers usually say they are from IT Support, and tell you that they have detected a virus on your machine that needs to be removed. The bogus caller will then either:

* Direct you to a website, in the hope you will download malicious software.
* Try and obtain details from you about your computer, or the MoJ network.

In all genuine situations, the MoJ service desk will provide you with an incident reference number if there is a real problem with your machine.

If you receive a call from someone claiming to be from the service desk, always ensure you ask them for the incident reference number. Then disconnect the call, and call service desk yourself, directly. If the original call was genuine, when you provide the incident reference number, they will be able to help you.

In general:

* Treat all unsolicited calls as suspicious.
* If possible, note the details and incoming telephone number of the caller.
* Do not go to any external site if directed from an unsolicited call.
* Never give any information about your computer to the caller.
* Check if the call is genuine with your IT Service desk. [Report the call](reporting-an-incident.md) as a security incident if it is not. Use a different phone from that used to take the original call.

##Hoaxes

Hoax letters are designed to trick you into believing, or accepting as genuine, something false and often preposterous: the messages they contain are usually untrue.

Hoax messages try to get you to pass them on to everyone you know using several different methods of social engineering. Most of the hoax messages play on your need to help other people. Who wouldn’t want to warn there friends about some terrible virus that is destroying people’s systems? Or help this poor little girl who is about to die from cancer?.

Chain letters and hoax messages have the same purpose but use a slightly different method of coercing you into passing them on. Chain letters, like their printed ancestors, generally offer luck or money if you send them on (scams). They play on your fear of bad luck and the knowledge that it is easy for you to send them on. Scams play on people’s greed and are illegal no matter what they say in the letter.

##The risk and cost of hoaxes

The cost and risk associated with hoaxes may not seem to be that high. If, however, you consider the cost of everyone within the MoJ receiving one hoax message, spending two minutes reading it and another two minutes forwarding it on or discarding it, the cost can be significant.

Handling these messages may also make our mail servers slow down to a crawl or crash.

Spammers (bulk mailers of unsolicited mail) may harvest email addresses from hoaxes and chain letters. Many of these letters contain hundreds of legitimate addresses, which is what the spammers want. There are also rumours that spammers are deliberately starting hoaxes and chain letters to gather email addresses.

##How to recognise a hoax

A request to “send this to everyone you know” (or some variant) should raise a red flag. The warning is probably a hoax. It’s unlikely a real warning message from a credible source will tell you to send it to everyone you know.

If the warning uses technical language, most people, including technologically savvy individuals, tend to believe the warning is real.

There may be credibility by association. If the janitor at a large technological organisation sends a warning to someone outside of that organisation, people on the outside tend to believe the warning because the company should know about those things. Even though the person sending the warning may not have a clue what he is talking about, the prestige of the company backs the warning, making it appear real.

These make it very difficult to be certain a warning is a hoax. Check to see if the claims are real, and if the person sending out the warning is a real person. Ask yourself if they are someone who would know what they are talking about.

##Type of hoaxes

##Scam chains

Mail messages that appear to be from a legitimate company but that are scams and cons, for example [Advance fee scams](https://en.wikipedia.org/wiki/Advance-fee_scam).

##Giveaways

Stories about giveaways by large companies. If you only send this on, some big company will send you a lot of money, clothes, a free vacation, etc., etc. You would have to wait forever for any of these to pay off.

##Malicious warnings (virus hoaxes)

These are warnings about Trojans, viruses, and other malicious code, that have no basis in fact.

Virus hoaxes have flooded the internet with thousands of viruses worldwide. Paranoia in the internet community fuels such hoaxes. An example of this is the [“Good Times” virus hoax](https://en.wikipedia.org/wiki/Goodtimes_virus), which started in 1994 and is still circulating the internet today. Instead of spreading from one computer to another by itself, Good Times relies on people to pass it along.

##Sympathy letters and requests to help someone

Requests for help or sympathy for someone who has had a problem or accident.

##Urban myths

Warnings and stories about bad things happening to people and animals that never really happened.

##Inconsequential warnings

Out of date warnings and warnings about real things that are not really much of a problem.

##True legends

Real stories and messages that are not hoaxes but are still making the rounds of the internet.

##Traditional chain letters

Traditional chain letters that threaten bad luck if you don’t send them on or request that you send money to the top “x” people on the list before sending it on.

##Threat chains

Mail that threatens to hurt you, your computer, or someone else if you do not pass on the message.

##Scare chains

Mail messages that warn you about terrible things that happen to people (especially women).

##Jokes

Warning messages that it’s hard to imagine anyone would believe.

##Email and storing MoJ information

Data held by the MoJ should be managed in such a way that employees who require the data, for business reasons, can gain access to it. Managers should ensure that data is stored in an area that is easily accessible to those who require access. This includes MoJ information exchanged using email.

If you need further assistance or information about this process, [ask](#contacts-for-getting-help) for help.

##Accessing emails or information in an absent employee’s email account

Staff absences do occur and these can cause disruption to MoJ business where colleagues have no access to relevant departmental information. Staff are away for events such as annual leave, secondment or maternity leave, but they don’t make provision for colleagues to access departmental information.

When an absence occurs, there is no right to be able to access another employee’s account to obtain information. This is true, regardless of whether the absence is expected or unexpected, for example annual leave or illness.

Accessing another employee’s account, without their permission, might contravene data protection legislation.

Data protection legislation protects personal information which relates to identifiable, living individuals held on computers. It specifies that appropriate security measures must be in place to protect against unauthorised access to, loss or destruction of personal data. If you breach this principle you could render the MoJ liable to enforcement action by the Information Commissioner.

##Avoiding the problem

If you know you’re going to be away for any significant amount of time, you can make life easier for everyone, including yourself, by following these simple steps:

1. Make provision for someone to have access to your work email account during your absence. If you don’t know how to do this, [contact your IT Helpdesk](#Xbb07d12fea49fbb5b3e8df93e92f1bfa0e2d2a2).
2. Create a “handover” package, containing information about the tasks that will, or might, need attention during your absence.
3. Make sure the package has contact details for everyone who might need to help progress or update the status of the tasks.
4. Create an “Out Of Office” notification in your email system; include clear details of who to contact in your absence.

##Authorised access to user email accounts

You must not access the email accounts of any other users, unless you are authorised to do so as required by your role. Access is authorised on a case by case basis only, and will typically be aligned to the following circumstances:

* During a criminal investigation by a law enforcement agency.
* During an employee investigation relating to misconduct or a security incident, for example IT misuse.
* Upon the death or unexpected exit of an employee, for example for the retrieval of key information and closing down an account.

Ideally, access will have been organised in advance of an absence. But this is not always the case; sometimes there are unexpected or unusual circumstances. Gaining access in such situations will require substantial escalation to [management and Data Privacy and Security teams](#contacts-for-getting-help).

##Contacts for getting help

In practice, all sorts of things can go wrong with email from time-to-time. Don’t be afraid to [report a problem or ask for help](#Xbb07d12fea49fbb5b3e8df93e92f1bfa0e2d2a2); you’ll be creating a better and safer work environment.

For general assistance on MoJ security matters, email [security@justice.gov.uk](mailto:security@justice.gov.uk).

For Cyber Security assistance or consulting, email [CyberConsultancy@digital.justice.gov.uk](mailto:CyberConsultancy@digital.justice.gov.uk).

Suppliers to the MoJ should primarily contact your usual MoJ points of contact.

##General enquiries, including theft and loss

**Technology Service Desk** - including DOM1/Quantum, and Digital & Technology Digital Service Desk. Use one of the following two methods for contacting service desk:

* Tel: 0800 917 5148
* [MoJ Service Portal](https://mojprod.service-now.com/moj_sp)

**Note:** The previous itservicedesk@justice.gov.uk and servicedesk@digital.justice.gov.uk email addresses are no longer being monitored.

**Note:** Use of the Digital & Technology Digital Service Desk Slack channel (#digitalservicedesk) is being withdrawn, and should be avoided.

**HMPPS Information & security:**

* Email: [informationmgmtsecurity@justice.gov.uk](mailto:informationmgmtsecurity@justice.gov.uk)
* Tel: 0203 334 0324

##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).