

INFORMATION SECURITY: E-MAIL CHECKLIST

The following is a series of practical actions you can take to reduce the risk of harm being caused to your business by your e-mail service.

- If you connect directly to the Internet (using a dial-in modem, ISDN or broadband) from your desktop or laptop machine, it is sensible to install 'personal firewall' software. You should ensure that any network connection (such as an e-mail server) has an appropriate firewall installed.
- Ensure all e-mail servers have appropriate virus-defence software and make sure it is set to check e-mail messages (both incoming and outgoing). It is sensible to use an external virus-scanning service or perhaps a separate mail gateway.
- Consider utilising junk mail filters in your client software (e.g. Microsoft Outlook) or buying a gateway spam (junk mail) filter product. Your Internet Service Provider (ISP) may provide spam filtering services.
- Check with your system software vendors (such as Microsoft) if you need to update security software. This is normally done online. Regularly apply appropriate security patches to mail servers.
- Similarly, regularly update gateway/server virus checkers.
- Perform periodic checks on any event logs stored on your systems for anything unusual or suspicious.
- Produce, publish and circulate an e-mail policy. Ensure it covers what sort of personal use is acceptable (if any) and what content is prohibited (e.g. chain letters, jokes, pornography etc.). Other potential content may relate to the size of file attachments, management of numbers of stored emails, unchecked mailing lists, and the policy on replying to e-mails from unknown or suspect sources etc.
- Archive to CDs all older e-mail from local stores and servers. If there is any sensitive information, make sure it is appropriately protected.
- Set up e-mail signatures that include correct contact information.
- Include a disclaimer containing appropriate legal text. The following sample text may be used: 'This e-mail is sent in confidence for the attention of the addressee only. The contents are not to be disclosed to anyone other than the addressee. If you receive this message in error please preserve this confidentiality and immediately inform the sender of this error.'
- Periodically check for and delete unused e-mail addresses.
- Tidy up servers, deleting temporary files and ensuring servers have enough disc space for your future requirements.
- Periodically check the validity of your contact and address lists and update them appropriately.

Please refer to the section on [Hints and Tips for Email Policy](#) in our business advice pages (see below) for further information.

Further help and advice

General

BERR Information Security Health Check Tool

<http://www.securityhealthcheck.berr.gov.uk/>

BERR Information Security Home page

www.berr.gov.uk/sectors/infosec

BERR Information Security Business Advice pages

<http://www.berr.gov.uk/sectors/infosec/infosecadvice/page10059.html>

BERR Information Security Publications (available to order or download)

<http://www.berr.gov.uk/sectors/infosec/infosecdownloads/page9935.html>