



## February 2008 Update

### Summary

European Safer Internet Day highlighted the dangers of the Internet and safe usage tips. Resources provided by various organisations, such as Get Safe Online, may be helpful to promote good practise in the work or home environment. GovCertUK welcomes the emphasis on best practise and encourages all users to re-familiarise themselves with current advice.

Some readers will be aware of recent press reports about website defacements. GovCertUK recommend separating web hosting from the rest of an organisation's infrastructure, configuring multiple backup links and providers and working with upstream providers to block malicious activity.

### Trends and alerts

Many IT security firms have published studies demonstrating the massive increase in online malicious programs (often called "malware") in 2007. GovCertUK advises following CESG best practice, as published on the CESG websites and the IA Bookstore. This includes prompt patching, using anti-virus software, enabling a software firewall or installing a firewall device and disabling unused browser functionality such as JavaScript and ActiveX.

GovCertUK does not recommend investigating suspect software. Should you be concerned that your network has been subject to malicious attack, please submit sample material following procedures published on our website at <http://www.govcertuk.gov.uk/reporting-an-incident.shtml>.

Recent research activities by certain vulnerability researchers have identified potential security issues in the Mifare (classic) RFID smart card technology. This type of smart card technology is used extensively around the world for transport and access entry systems. There are a number of mitigations that can be put in place if you are using similar systems for your own security infrastructure. Interested parties should in the first instance contact their card system supplier for further information. Your local WARP operator or the GovCertUK enquiries line can provide general advice.

A number of software vendors have released important security updates this month and GovCertUK recommend that system administrators, after resilience testing, apply the relevant patches to their environments wherever possible. The GovCertUK Summary of Microsoft Advisories for February is available for download at [http://www.govcertuk.gov.uk/patch\\_advisories.shtml](http://www.govcertuk.gov.uk/patch_advisories.shtml).

## February news

The upcoming GovCertUK training day on 10<sup>th</sup> March 2008 includes a number of interesting presentations by our experts, with contributions from other organisations. Delegates should have received confirmation of their attendance, though should there be any other queries please contact us via the enquiries line: [enquiries@govcertuk.gov.uk](mailto:enquiries@govcertuk.gov.uk). If you are unable to attend this session there will be another training event in six months' time.

In response to sensitive personal data management issues, CESA has issued the Good Data Handling Guidance Information Pack, which brings together various advisories and Good Practice Guides. This can be found on the CESA IA Bookstore CD or the CESA GSi website. If not a GSi user or Bookstore recipient, please contact your local IT Security Officer or WARP administrator for further details.

## Contact us

We welcome any queries about this report. Please contact us via one of the following means:

Email	<a href="mailto:enquiries@govcertuk.gov.uk">enquiries@govcertuk.gov.uk</a>
Telephone	01242 709311
Fax	01242 709113
Postal address	GovCertUK A2f P.O. Box 144 Cheltenham Gloucestershire GL51 0EX