

## Links to Information Security Websites

It is impossible to have a comprehensive and multilingual review of websites dealing with Information Security and this is merely a selection which many people found useful. The inclusion of vendors or other commercial entities does not constitute an endorsement of their products or services.

The websites on this page have been grouped in the following categories

- Security portals
- International fora
- Security standards and best practices
- Reference sites
- Security mailing lists
- Virus information and anti-virus software
- Alerts, incident tracking and reporting
- Virus hoaxes
- Vendor websites
- Security and encryption
- Activism and Hacktivism
- Cyberwar, Information warfare
- Auditing and e-fraud
- Cyberlaw

This list does not include pointers to hacker websites or to sources from which hacking tools can be obtained. These are however, numerous. Feedback on the desirability of including such websites would be appreciated. Should you want to contribute please <mailto:ed.gelbstein@wanadoo.fr>

### SECURITY PORTALS

This is a listing of only some of the sites that offer information and resources on information security. All are worthwhile.

<http://www.cerias.purdue.edu/coast/hotlist/>

<http://www.csoonline.com/> Website of the Chief Security Office journal

<http://www.infosyssec.org/>

<http://www.itsecurity.com/>

<http://packetstorm.securify.com/>

<http://secinf.net/>

<http://www.securityfocus.com/>

<http://security.itworld.com/>

<http://www.securityportal.com/>

<http://www.securitysearch.net/>

## **INTERNATIONAL FORA**

<http://www.oecd.org/dsti/sti/it/secur>

Documents and events relating to information security and privacy issues.

<http://www.iccwbo.org>

The Alliance against commercial cybercrime of the International Chamber of Commerce.

<http://www.uncjin.org>

The website of the United Nations Crime and Justice Information Network. It addresses cyberspace issues.

<http://www.odccp.org>

The website of the United Nations office for Drug Control and Crime Prevention

<http://www.coe.int/>

The Council of Europe Cybercrime convention issued in 2001 and adopted as a model by other countries

The text of the Convention can be found under Legal Affairs, fight against organized crime. There is no direct bookmark for downloading the document.

## **SECURITY STANDARDS AND BEST PRACTICES**

<http://www.diffuse.org/secure.html#help>

The Diffuse project provides reference and guidance information on available and emerging standards and specifications that facilitate the electronic exchange of information, including a comprehensive listing of information security standards. A good starting point.

<http://www.iso.ch/cate/d33441.html>

ISO/IEC 17799:2000 Information technology -- Code of practice for information security management.

See also:

<http://www.bsi-global.com/group.xhtml> for BS 7799-2:1999 Information security management -- Specification for information security management systems.

<http://www.standards.com.au/> for AS/NZS 4444-2:1999 Information security management -- Specification for information security management systems.

<http://www.sas70.com>

The website dedicated to the Statement on Auditing Standards Number 70 developed by the American Institute of Certified Public Accountants (AICPA)

<http://csrc.nist.gov>

The website of the Computer Security Resource Centre of the USA's National Institute for Standards and Technology. It links to the standard NIST 800-37

<http://www.itu.int/>

The International Telecommunications Union produces recommendations that are developed and published as standards by the International Standards Organization (ISO) and the International Electrotechnical Commission (IEC). These include the X.509

standard for digital certificates and the X.800 series of standards for electronic commerce related activities

<http://www.ietf.org>

The Internet Engineering Task Force is the major international forum for the discussion and development of Internet-related technical standards – the pages “IETF Security Area” were under construction in mid April 2002.

<http://csrc.nist.gov/publications/>

The Computer Security Resource Center is maintained by the US Government National Institute of Standards and Technology. Good resource for US Government standards and other resources. This website also has links to the security standards activities of the Institution of Electrical and Electronic Engineers (IEEE), the European Computer Manufacturers Association (ECMA), also working on the development of security related standards as well as to the work of other bodies.

<http://www.radium.ncsc.mil/tpep/>

US Government Commercial Product Evaluations, with links to the “Common Criteria” (*Common Criteria Information Technology Security Evaluation CCITSE*), the “Rainbow Series” (*Trusted Computer System Evaluation Criteria TCSEC*) and the Evaluated Products List.

<http://www.caspr.org>

Work in progress to create a Common Body of Knowledge (CBK) through a series of Commonly Accepted Security Practices and Recommendations (CASPR). It is expected that this material will become available later in 2002.

<http://www.sans.org>

The System Administration and Networking Security Institute provides guidance, training and information on a broad range of information security matters.

<http://www.issa.org>

The Information Systems Security Association – a website primarily for information security professionals

<http://www.gocsi.com/>

The Computer Security Institute

<http://www.itil-itsm-world.com/security.htm>

The Information Technology Infrastructure Library (ITIL) originated in the UK Government’s Central Computing and Communications Agency and developed since into an autonomous business unit providing documentation, guidance, consultancy and other activities

<http://www.survive.com/>

Worldwide professional association for business continuity professionals.

## REFERENCE SITES

<http://www.cs.georgetown.edu/~denning/publications.html>

Professor Dorothy Denning's website, at Georgetown University, contains many documents and publications on cybercrime, encryption and related matters

<http://whatis.techtarget.com/>

An on-line encyclopædia specifically for IT-related definitions. It has a topic specific index for security, among other topics.

<http://www.cis.ohio-state.edu/hypertext/information/rfc.html>

An index, and key word search, of Internet Request For Comments (RFC) documents, which are the written definitions of the protocols and policies of the Internet.

Some interesting, general RFCs on Internet security are:

RFC 1281: Guidelines for the Secure Operation of the Internet / R. D. Pethia, S. Crocker and B. Y. Fraser. - November 1991

<http://www.cis.ohio-state.edu/htbin/rfc/rfc1281.html>

RFC2084: Considerations for Web Transaction Security / G. Bossert, S. Cooper, W. Drummond - January 1997

<http://www.cis.ohio-state.edu/htbin/rfc/rfc2084.html>

RFC 2196: Site Security Handbook / B. Fraser, Editor - September 1997

<http://www.cis.ohio-state.edu/htbin/rfc/INDEX.rfc.html>

RFC 2350: Expectations for Computer Security Incident Response / N. Brownlee, E. Guttman - June 1998

<http://www.cis.ohio-state.edu/htbin/rfc/rfc2350.html>

RFC 2504: Users' Security Handbook. . Guttman, L. Leong, G. Malkin. February 1999

<http://www.cis.ohio-state.edu/htbin/rfc/rfc2504.html>

RFC 2828: Internet Security Glossary. R. Shirey. May 2000

<http://www.cis.ohio-state.edu/htbin/rfc/rfc2828.html>

## SECURITY MAILING LISTS

The following web pages are the "home" for some of the security mailing lists available. From these web pages you can subscribe to these mailing lists, search through mailing list archives, or find out about the mailing list itself.

**BugTraq** <http://www.securityfocus.com/>

Home of the widely subscribed **BugTraq** mailing list, for announcements and detailed discussions of computer security vulnerabilities. And there are several other useful security-related mailing lists as well. The web site also has information on security basics, intrusion detection, incident response, and for Microsoft, Sun and Linux systems, as well as databases on vulnerabilities and viruses.

**CERT Advisory** [http://www.cert.org/contact\\_cert/certmaillist.html](http://www.cert.org/contact_cert/certmaillist.html)

A well-respected mailing list providing descriptions of serious security problems and their impact, along with instructions on how to obtain patches or details of workarounds. In addition, the web site has excellent resources for improving security practices and implementations. Highly recommended.

**Crypto-Gram Newsletter** <http://www.counterpane.com/crypto-gram.html>

An excellent monthly newsletter on computer security and cryptography.

**Executive Security Digest** <http://www.securityportal.com/topnews/>

A weekly executive-level summary of important information security news. Other interesting security mailing list are also available.

**Firewalls** <http://www.lists.gnac.net/firewalls/>

A mailing list for the discussion of Internet firewall security systems and related issues, including the design, construction, operation, maintenance, and philosophy of Internet firewall security systems. However, this is a very active mailing list and you will be inundated with postings.

**NTBugtraq** <http://www.ntbugtraq.com/>

NTBugtraq is a mailing list for the discussion of security exploits and security bugs in Microsoft Windows NT and its related applications.

**Security Alert Consensus** <http://www.sans.org/sansnews>

**SANS Newsbites** <http://www.sans.org/sansnews>

SANS (System Administration, Networking and Security) Institute provides the "Security Alert Consensus", which is a weekly summary of new security alerts and recommended countermeasures, and the "SANS Newsbites", which is a weekly summary of information security news. The web site also has some excellent information security resources.

## **VIRUS AND WORM INFORMATION**

The links below, sorted in alphabetical order, are for some of the anti-virus software vendors. This list is not exhaustive and the virus information databases on these web sites are useful. Their presence on this list does not constitute an endorsement of their products.

Computer Associates:

<http://ca.com/virusinfo/encyclopedia/>

F-Secure:

<http://www.europe.datafellows.com/v-descs/>

Network Associates:

<http://vil.nai.com/vil/default.asp>

Sophos:

<http://www.sophos.com/virusinfo/analyses/>

Symantic:

<http://www.symantec.com/avcenter/vinfodb.html>

Trend Micro

<http://www.antivirus.com/vinfo/virusencyclo/>

## **VIRUS HOAXES**

Note: The anti-viral software vendor sites (see above) all have useful information on virus hoaxes as well.

<http://hoaxbusters.ciac.org/>

US Department of Energy (US DOE) and Computer Incident Advisory Capability (CIAC) on Internet Hoaxes and chain letters.

<http://vmyths.com/>

A useful "independent" site on virus myths, misconceptions, and hoaxes by a self-proclaimed expert.

## **ALERTS, INCIDENT TRACKING AND REPORTING**

<http://www.cert.org>

The website of the Computer Emergency Response Team at Carnegie Mellon University, USA.

<http://www.attrition.org/>

A web site for the collection, dissemination and distribution of information about computer security. It is especially known as the largest mirror of web site defacements.

<http://cve.mitre.org/>

A web site with a database of standardised names for Common Vulnerabilities and Exposures in information systems. Becoming widely referenced in the industry when referring to recognised vulnerabilities.

<http://www.htcn.org/>

The High Tech Crimes Network – a somewhat complex home page leads into valuable information, training and testing facilities, conferences and technology issues.

## **MISCELLANEOUS**

This is not an exhaustive list of the various security sites available. However, the information provided on these web sites can be very useful.

<http://cnet.com/enterprise/0-9567.html?tag=dir>

A very informative web site with information technology and commerce related information. This is their security site.

<http://www.infosecuritymag.com/>

Information Security magazine is a recognised publication with news, analysis, insight and commentary on information security. The web site also offers an information security e-mail newsletter and an information security news web site.

<http://www.linuxsecurity.com/>

A great web site for offering information about security and the open source Linux operating system.

<http://www.zdnet.com/enterprise/filters/resources/0,10227,6007271,00.html>

A very informative web site for people who want to buy, use, or learn more about technology. This is their security site.

<http://www.epic.org>

The Electronic Privacy Information Centre, includes a survey of national policies with regards to the use of encryption.

<http://www.privacyinternational.org/>

As above, a website discussing personal privacy issues

## **VENDORS**

### **General**

<http://www.microsoft.com/security/>

Microsoft Corporation is the world's largest software producer and the number 1 company in the IT industry in terms of revenue and performance. This is their IT security web site.

<http://www.cisco.com/warp/public/779/largeent/issues/security/>

Cisco Systems is the world-wide leading maker of data networking equipment for the Internet, and the second largest company in the IT industry in terms of revenue and performance. This is their enterprise security web site.

<http://www.ibm.com/services/e-business/security.html>

IBM develops and manufactures computers, networking systems, software, and other IT devices. They are the third largest company in terms of revenue and performance in the IT industry. This is their security and privacy web site.

<http://www.oracle.com/ip/solve/security/index.html>

Oracle Corporation is a provider of software and services, primarily Internet enabled database, tools and application products. They are the fourth largest company in terms of revenue and performance in the IT industry. This is their database security web site.

<http://www.sun.com/products-n-solutions/software/security/index.html>

Sun Microsystems is a provider of Unix networked systems and are the fifth largest company (in terms of revenue and performance) in the IT industry. This is their computer security web site.

## **SECURITY AND ENCRYPTION**

<http://www.checkpoint.com/>

Check Point is a commercial provider of Firewall software and security solutions. They are the largest company in terms of revenue and performance in the security and encryption section of the IT industry.

<http://www.verisign.com/>

Verisign Incorporated is a commercial provider of Internet trust services including authentication, validation and payment needed to conduct secure electronic commerce and communications over the Internet. They are the second largest company in terms of revenue and performance in the security and encryption section of the IT industry.

<http://www.pgpi.com/>

Pretty Good Privacy International provides a number of encryption products on an international basis

<http://iss.net/>

ISS Group is a commercial provider of security software and management solutions. They are the fourth largest company in terms of revenue and performance in the security and encryption section of the IT industry. They have an excellent database ("X-Force") and other resources for computer threats and vulnerabilities.

<http://www.baltimore.com/>

One of the major vendors of security solutions for e-business

## **ACTIVITISM AND HACKTIVISM**

<http://www.gn.apc.org/pmhp/ehippies/>

The Electrohippies are not hackers per se. Instead they promote civil disobedience and electronic sit-ins (WTO was one of their targets) through denial of service attacks, etc

<http://www.thehacktivist.com/>

Website devoted to Electronic Civil Disobedience

<http://www.thing.net/~rdom/ecd/ecd.html>

Topics of Electronic Civil Disobedience

Hackers are remarkably well organised. Their activities, tools, etc. are reported through many websites. This list does not include any such sites.

Many companies offer security audit and certification services. Some pointers towards certification practices and international organizations are given in the section below.

## **CYBERWAR AND INFORMATION WARFARE**

<http://www.terrorism.com>

Website of the Terrorism Research Centre, an independent institute founded in 1996

<http://news.ists.dartmouth.edu>

The website of the Dartmouth College Institute for Security Technology studies

<http://www.acq.osd.mil/dsb>

The website of the Defense Science Board of the United States of America

<http://www.fas.org/irp/wwwinfo.html>

Information Warfare and Information Security resources on the web compiled by the Federation of American Scientists

<http://212.111.49.124>

Information Warfare Site

[www.intapactinc.com/infowarfare.html](http://www.intapactinc.com/infowarfare.html)

Interpact Inc., is a company specializing in Security Awareness Programmes. This website contains many useful resources on information insecurity, information warfare and related topics

[www.cs.georgetown.edu/~denning](http://www.cs.georgetown.edu/~denning)

Pages on cybercrime and information warfare by Professor Dorothy Denning

## **AUDITING AND E-FRAUD**

<http://www.isaca.org>

The Information Systems and Control Association and Foundation. The guidelines and framework for the Control Objectives for Information Technology (COBIT) can be downloaded from this website

<http://www.isc2.org/>

The International Information Systems Security Certification Consortium

<http://www.giac.org/>

The Global Information Assurance Certification related to the SANS institute mentioned above under standards and best practices

<http://www.securityauditor.net/>

Developers of a software product (COBRA) to support risk analysis, self-evaluation and compliance in the framework of ISO 17799

<http://www.auditnet.org/>

A website dealing primarily with audit matters, including security audits

<http://www.merchantfraudsquad.com/>

A not-for profit organization set up to assist merchants with fraud situations

<http://www.ifccfbi.gov/>

The website of the Internet Fraud Complaint Centre

<http://www.usdoj.gov/criminal/cybercrime/index.html>

Website of the Computer Crime and Intellectual Property Section of the Criminal Division of the U.S. Department of Justice. It has a good section on international matters

## CYBERLAW

There are many websites, the majority in academic circles dealing with emerging cyberlaw legislation. The selection below is suggested as a starting point

<http://www.isoc.org/internet/law/intsubs2.shtml>

Links on internet related legislation maintained by the Internet Society

<http://www.coe.int>

The website of the Council of Europe. Within this site, but without a direct link, is the Convention on Cybercrime signed in November 2001

<http://nsi.org/>

The website of the United States of America National Security Institute lists legislation proposed or approved by the U.S. Congress as well as counter-terrorism legislation covering cyberspace

<http://www.ll.georgetown.edu/intl/guides/cyberspace/index.html>

The law library at Georgetown University offers a research guide on cyberlaw prepared by the Department of Foreign and International Law

<http://www.temple.edu/lawschool/dpost/writings.html>

Professor David Post has written extensively on cyberlaw and is also one of the founders of the

<http://www.cli.org>

The Cyberspace Law Institute. At the time of revising these bookmarks, the site was under construction and contains some material expected to develop further

<http://www.asil.org>

The website of the American Society for International Law

<http://www.usdoj.gov/criminal/cybercrime/intl.html>

This U.S. website has extensive links dealing with international activities and legislation on cybercrime

<http://www.mossbyrett.of.no/info/legal.htm>

The website of the Chief Justice, Moss District, Norway, lists the status of penal legislation in 44 countries

<http://www.cdt.org/legislation/107th/wiretaps/>

The website of the Centre for Democracy and Technology has pages dealing with legislation affecting the Internet

<http://www.gahtan.com/cyberlaw/> and <http://www.gahtan.com/techlaw>

The website of a Canadian lawyer that posts "The Cyberlaw Encyclopedia"