

You are in: >

> Revealing Facts

Home

News Feed **XML**

Free Web Design

Quotation

Add Your URL

Hosting

Domain Names

Job Search

Submit an Article

Directory

FAQ

Forum

Get our Logo

Webmaster Tools

Contact Us

Returns Policy

Search DMOZ

Articles & Tutorials

Latest Articles

ASP

Beginner's

C#

CSS

Topical

Databases

Design Tips

Dreamweaver

Flash

Net History

Hosting

HTML/XHTML

Revealing Facts

Posted on Wed 06 October 2004 by: **S's Ramage**

Free Web Design Quota



Ads by Google
Data Protection Act
View BT's white paper about using CRM tools to support compliance
www.bt.com/html/whitep.htm

White-Collar Crime Charge
When the FBI Comes Calling, 100% White-Collar Federal Defense
www.federalcrimes.com

Spam Laws Compliance
Ensure staff read and accept company policies on spam laws
www.policymanager.com

Act Data Protection
Practical help/advice to businesses Access to objective info & support
www.businesslinks.gov.uk

of web design companies registered in our database. Request a quote today and do all the hard work of find the best quotations from a range of web designers.

By Sally Ramage Dabyydeen, BA(Hons), MBA, LL.M, MCMI, FFA.

The Computer and Internet Crime Conference 2004 which took place in London the 30th and 31st March was a very necessary and timely conference. Ed G Agent of the FBI and now at the US Embassy, gave a presentation, the open address made by the Assistant Commissioner of the Metropolitan Police Tari Ghaffar.

Cybercrime such as internal and external hacking, spam and computer virus widely acknowledged. Hacking is a growing problem for businesses which confidential client and customer details electronically. External hackers can confidential information, deface websites and steal financial company information. Often, white collar crime is carried out by internal hackers but a larger proportion through an outside source of security breaches. Employees can steal intellectual property from their employers. Intellectual property theft includes theft of e address books, proposal documents used as marketing tools of solicitors, client databases and contact information. An indication on how serious the problem white collar crime has become is the recent issue of "The Lawyer" which

JavaScript

Legal

Marketing

Networks

Perl

Photoshop

PHP

SEO

Security

Usability

XML

Other Resources

PHP Manual

PEAR Manual

SEO Tools

concentrated on the war on fraud and featured so many expert witnesses on collar crime.

In what way are hackers' activities illegal? In the UK, it is a Data Protection offence to send unsolicited e-mails. There is a new European Commission Directive introduced in 2003 which makes it a criminal offence to send unsolicited e-mails in the UK, this EC Directive has been implemented by the Privacy and Electronic Communications Regulations 2003. Will these regulations deter the sending spam? Only if the source of the spam can be pin-pointed. Spam is particularly sinister. At present spammers have created virtual countries' websites and banks even. Spammers can blackmail companies. Current anti-spam device filter spam. Spam also damage businesses by taking up valuable business time dealing with them and also because they can carry malicious viruses which even more major disruption to businesses. Viruses in a business's computer are very costly in terms of data recovery, slow-down in productivity, necessary software upgrades as well as loss of business, not to mention the lowering of morale and the damage to the business reputation. Internet filtering and e-monitoring software, anti-virus software, backing-up of data, and systems policies are steps to controlling any potential damage. Staff policies must be in place. The consequences of e-mail misuse must be set down in company policy. If staff, for example, use e-mail to circulate ridicule about other staff members would amount to gross misconduct and dismissal. Such e-mails would amount to intrusions into employee privacy as per Article 8 of the European Convention on Human Rights.

When things go wrong, electronic documents, spread-sheets and e-mails are relevant material for litigation. More and more in court cases, evidence is found exclusively in electronic format. Forensic technology therefore needs to be a large part of the investigation. Forensic technology can recover, for example deleted material. Forensic techniques can recover multiple versions of the same document from traces left on electronic media. Small differences between altered versions can be used to build up a picture of what changes were made when. The time-line of document creation and differing versions can be used to corroborate or disprove the chronology of events. Electronic evidence must the provenance of the material and the entire history of electronic material collated to produce robust evidence in court. The evidence must be collected the UK evidence laws. Metadata is hidden within electronic files, examples of are entries in e-mails, dates embedded in documents and links to other files case of e-mails, a full audit trail does exist and can be retrieved.

