

Cyber Security Fact Sheet

Abstract: A compendium of facts, statistics, trivia, etc. that pertain to cyber security.

- 41 percent of people use the same password at every [password-controlled] site they visit¹.
- One new infected web page is discovered every 5 seconds².
- One new spam-related web page is discovered every 20 seconds³.
- 38% of all malware hosting occurs in the USA⁴.
- One in every 2500 email messages contains an infected attachment⁵.
- 97% of business email contains spam⁶.
- 353.8 billion spam text messages were sent to China's cell phone owners in the last year⁷.
- In the first half of 2008, the top hosting site for malware was Blogger [Blogspot dot com]⁸.
- 98% of data leakage incidents are due to accident or stupidity⁹.
- Trick to enhance web-site password security: always answer secret questions with lies!
- The largest blackout in North American history, which occurred in August 2003 and affected 50 million people over a 9300-square-mile area, is believed to have been precipitated by a cyber-intrusion by China's People's Liberation Army¹⁰.
- In fiscal year 2007 37,000 reported breaches of government and private systems occurred¹¹.
- If the 9/11 perpetrators had focused on a single U.S. bank through cyberattack and it had been successful, it would have had an order-of-magnitude greater impact on the U.S. economy¹².
- The Office of Management and Budget has directed Federal agencies to limit the total number of Internet "points of presence" to 50 by June 2008.
- In April 2000, a disgruntled job hunter hacked into a computerized municipal sewage management system and caused the discharge of millions of liters of raw sewage into parks, rivers, and even the grounds of a Hyatt Regency hotel¹³.
- In a survey of European IT executives and managers by Logica, organizations that suffered data breaches reveal that 60% of their customers are not informed of the breaches, and only 30% of organizations educate staff in IT security and information handling procedures on a regular basis¹⁴.

¹ Data security firm Sophos, Inc.

² *Security Threat Report, July 2008*; Sophos, Inc.

³ Ibid.

⁴ Ibid.

⁵ Ibid.

⁶ Ibid.

⁷ Ibid.

⁸ Ibid.

⁹ Network World, 9/11/07; <http://www.networkworld.com/news/2007/091107-data-leak-prevention.html>

¹⁰ *National Journal*, 5/31/08; http://www.nationaljournal.com/njmagazine/cs_20080531_6948.php

¹¹ Ibid.

¹² Ibid.

¹³ *The Register*, 10/31/01; http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/

¹⁴ <http://management.silicon.com/itdirector/0,39024673,39293831,00.htm?r=2>

- According to a study by British Telecom, 44% of resold second-hand BlackBerry devices were not wiped of sensitive personal and corporate information and were found to contain details of bank accounts, board meetings, and financial data.
- According to figures released by UK payments association Apacs, losses from online banking fraud nearly tripled in the first half of 2008 over the same period in 2007.
- According to a recent study by Panda Security, adware is responsible for one-third of all new malicious software, especially fake antivirus scanners¹⁵.
- International research has shown that 97% of Internet users cannot distinguish between secure and insecure websites, meaning that their computers are at constant risk of infection with malware. 80% of the computers surveyed had programs that were dangerous in terms of information security¹⁶.
- According to a study by the National Cyber Security Alliance, a large number of Americans still fail to use basic Internet security tools, and there remains a substantial gap between the protections people think they have and what is actually installed on their computers.
- According to data compiled by the Identity Theft Resource Center, during the first 9 months of 2008 there were 516 reported breaches that resulted in the potential exposure of more than 30 million consumer identities, exceeding the numbers for the entire previous year¹⁷.
- A recent study by Cornell University of wireless networks at 38 hotels found that 33 of them were lacking in adequate security safeguards to prevent breach and access to data of other individuals using the network¹⁸.
- The FBI reports that, for the first time ever, revenues from cybercrime have exceeded drug trafficking as the most lucrative illegal global business, estimated at more than \$1 trillion annually in illegal profits¹⁹.
- The annual CSI/FBI survey released in October 2007 found that U.S. businesses lost an average of \$350,424 in 2007 as a result of cybersecurity incidents—more than doubled from losses incurred from 2006²⁰.
- In its first-half 2008 Security Intelligence Report, Microsoft announced that 90% of newly reported vulnerabilities involved applications (as opposed to operating systems)²¹.
- A 2007 survey commissioned by eBay showed that 93% of Australian internet users don't know what phishing is.
- A study by Harvard University and UC/Berkeley found that 90% of participants were fooled by good phishing web sites, 68% proceeded without hesitation when presented with popup warnings about fraudulent certificates, and 23% did not look at the address bar, status bar, or the security indicators²².

¹⁵ *Quarterly Report*, PandaLabs; July –September 2008; http://news.cnet.com/8301-1009_3-10056912-83.html?part=rss&subj=news&tag=2547-1009_3-0-20

¹⁶ “*Adware and Spyware: Unraveling the Financial Web*”. McAfee White Paper, August 2006.

¹⁷ “*Data Breaches Best 2007 Record*”, http://news.cnet.com/8301-1009_3-10059270-83.html?part=rss&subj=news&tag=2547-1009_3-0-20

¹⁸ “*Study: Hotel Network Security Lacking*”, 10/6/08, <http://www.scmagazineus.com/Study-Hotel-network-security-lacking/article/118819/>

¹⁹ “*The New Face of Cybercrime*,” ChannelWeb, 10/13/08, <http://www.crn.com/security/210800781>

²⁰ *Ibid.*

²¹ “*Microsoft: Despite better tools, online threats are growing*”, 11/3/08, New York Times News Service

²² “*Why Phishing Works*”; http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf