# Hacking the Law: A Hacker's Safety Guide to Electronic Crime Laws of Pakistan

Jawad A Sarwana

Abraham & Sarwana
P.I.D.C House
Karachi

Ph : 568 7360 / 568 7370
Fax : 568 7364
Email : abrahams@cyber.net.pk

# Overview

- Is our computer system vulnerable?
- Who should we look for help?
- Can we trust them?
- How can they help us?
- What stops them from helping us?
- Look before you Leap!
- Conclusion

# Is our Computer System vulnerable?

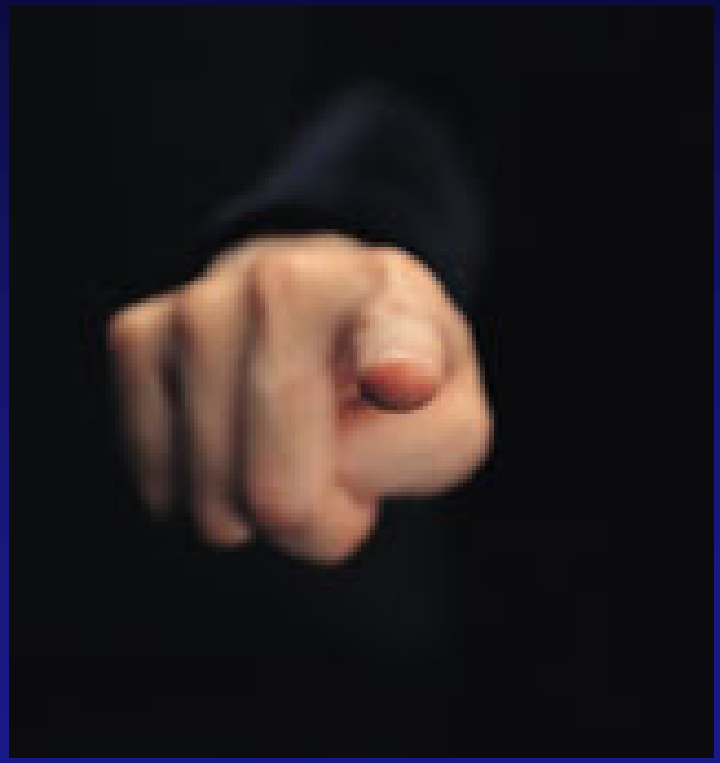
**"Nearly 16,000 new viruses, worms and trojans have appeared in 2005"**

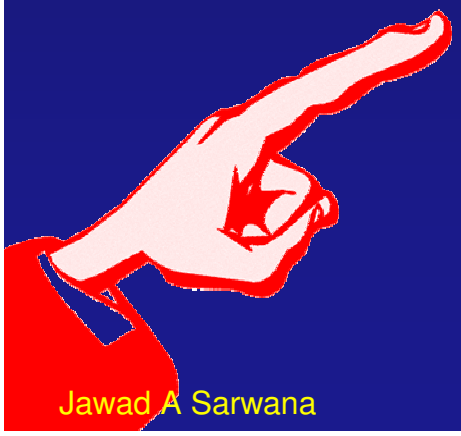
*--Security Management Report 2005*

*published by Sophos, an Anti-virus software company*

- In Sept 2004, SBP issued Business Continuity Guidelines to safeguard their IT based banking systems from act of terrorism and natural disasters.
- Most recently, in the first week of Dec 2005, SBP issued Guidelines for Account Holders using Credit/Debit and Smart Cards.
- FIA – NR3C – ***National Response Center for Cyber Crimes***

# Where do we look for help?





# Computer hackers: Evil or Good?

| Black Hat | v. | White Hat |
|---|---|---|

Malafide Intention

Bonafide Intention

Grey Hat

# Can We Trust Them?

**Hacker Ethic - A brief History**

# Steven Levy's Principal of the Hacker Ethic

- Access to computers—and anything which might teach you something about the way the world works—should be unlimited and total. Always yield to the Hands-on Imperative!
- All information should be free.
- Mistrust authority—promote decentralization.
- Hackers should be judged by their hacking, not bogus criteria such as degrees, race, or position.
- You can create art and beauty on a computer.
- Computers can change your life for the better.

# The 21st Century Hacker's Ethics:

- the belief that information-sharing is a powerful positive good, and that it is an ethical duty of hackers to share their expertise by writing free software and facilitating access to information and computing resources wherever possible; and/or

- the belief that system hacking for fun and exploration is ethically acceptable as long as the hacker commits no theft,vandalism, or breach of confidentiality.

# How can they help us?

- Educating Government and Business Houses on IT Security
- Examples: Penetration testing, Port scanning, etc.
- Ensuring Product Quality

# What stops them from helping us?

# The Law!!!!!!

# Section 36 of the Electronic Transaction Ordinance, 2002 states:

## Violation of Privacy of Information

"Any person

who gains or attempts to gain access to any information system

with or without intent to acquire the information contained therein or to gain knowledge of such information,

whether or not he is aware of the nature or contents of such information,

when he is not authorized to gain access, as aforesaid,

shall be guilty of an offence under this ordinance punishable with either description of a term not exceeding seven years, or fine which may extend to one million rupees or with both."

# Section 37 of the Electronic Transaction Ordinance, 2002 states:

**Damage to Information System, etc:**

1. Any person who does or attempts to do any act with intent to alter, modify, delete, move, generate, transmit, or store any information through or in any information system knowingly that he is not authorized to do any of the foregoing shall be guilty of an offence under this ordinance.

2. Any person who does or attempts to do any act with intent to impair the operation of or prevent or hinder access to, any information contained in any information system, knowingly that he is not authorized to do any of the foregoing, shall be guilty of an offence under this ordinance.

3. The offences under sub sections (1) and (2) of this section will be punishable with either description of a term not exceeding seven years or fine which may extend to one million rupees or with both.

# Look before you Leap

# Sections 4 of the Electronic Crimes Bill 2004 states

**Criminal access**

"Whoever gains unauthorized access to the whole or any part of an electronic system with or without infringing security measures with intent to infringe privacy or commit further offence is said to commit the offence of criminal access. Whoever commits the offence of criminal access shall be punished with imprisonment of either description for a term which may extend to two years, or with fine not exceeding three hundred thousand rupees or with both."

# Sections 5 of the Electronic Crimes Bill 2004 states:

**Criminal data access**

Whoever intentionally causes electronic system to perform any function for the purpose of gaining unauthorized access to any data held in any electronic system is said to commit the offence of criminal data access. Whoever commits the offence of criminal data access shall be punished with imprisonment of either description for a term which may extend to three years, or with fine or with both."

# Other Jurisdictions

- Budapest Convention on Cyber Crime, 2001
- The U.S. Constitution's First Amendment
- UCITA, 2000 (USA)

# UCITA

**A State's Consumer Protection Law Trumps UCITA.** An information contract is expressly subject to and may not waive any consumer protection provided in state or federal law. Included are laws providing for conspicuous disclosure, unfair or deceptive trade practice laws, and laws relating to electronic signatures and records.

**Right to Criticize Protected.** Information contract terms that prohibit criticism of an information product are unenforceable. Parties may contract in a manner consistent with other law such as the law of trade secrets.

UCITA --- Continued

# UCITA

**Remedies for Known Material Defect Preserved**. Remedies for a known material defect of a product are expressly made available as fully as for defective goods or services.

**Reverse Engineering for Interoperability Expressly Authorized**. An information contract may not prohibit reverse engineering that is done for the purpose of making an information product work together with other information products.

- The Internet Engineering Task Force (IETF)

  45 Days Notice Period for Reporting Security Vulnerabilities

# Conclusion