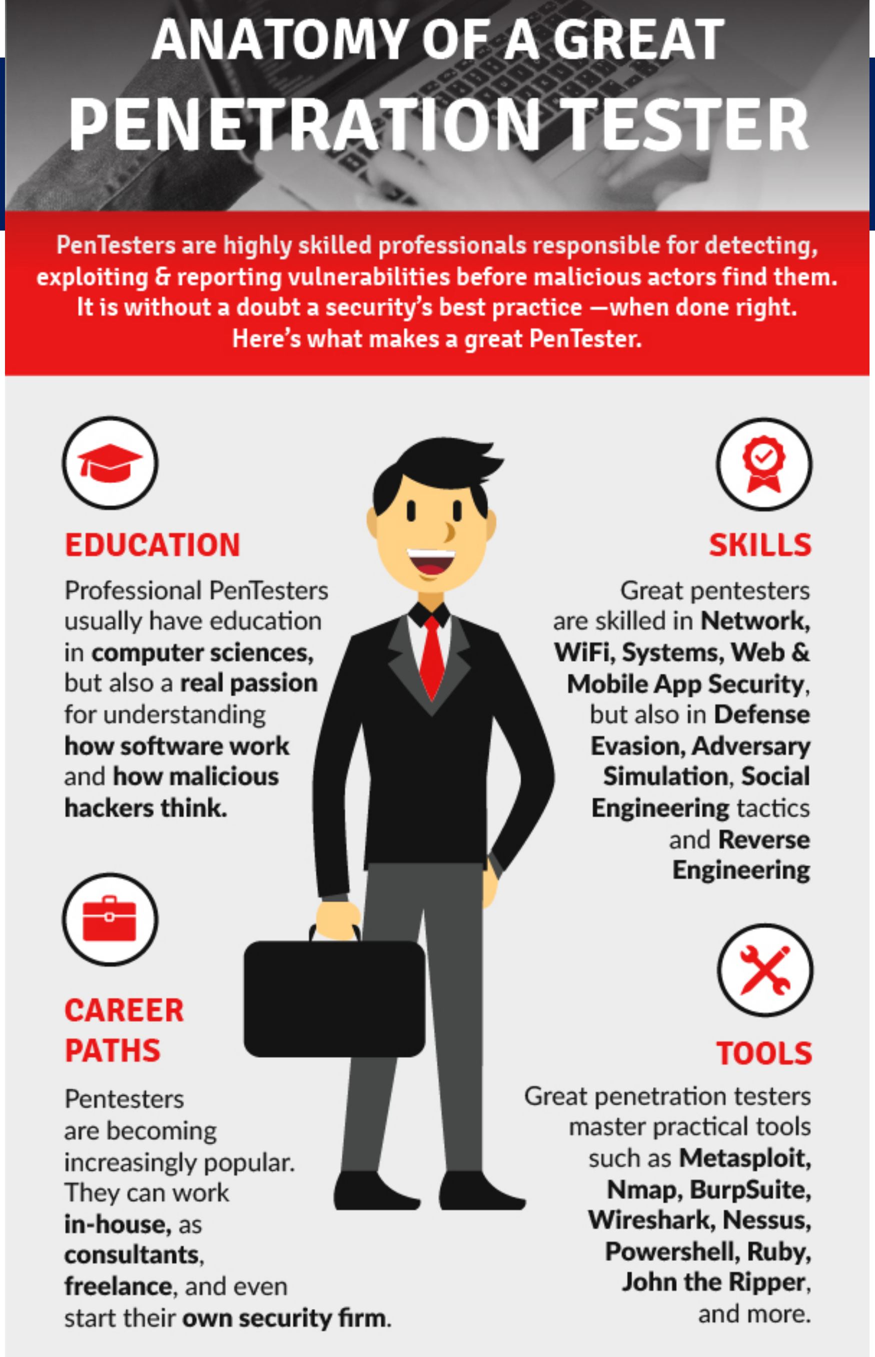
Legal aspects of Penetration Testing

Penetration Testing

Definition of Penetration Testing:

- A penetration test or pentest is a test evaluating the strengths of all security controls on the computer system. Penetration tests evaluate procedural and operational controls as well as technological controls.



ANATOMY OF A GREAT PENETRATION TESTER

PenTesters are highly skilled professionals responsible for detecting, exploiting & reporting vulnerabilities before malicious actors find them. It is without a doubt a security's best practice —when done right. Here's what makes a great PenTester.

EDUCATION

Professional PenTesters usually have education in **computer sciences,** but also a **real passion** for understanding **how software work** and **how malicious hackers think.**

SKILLS

Great pentesters are skilled in **Network, WiFi, Systems, Web & Mobile App Security**, but also in **Defense Evasion, Adversary Simulation**, **Social Engineering** tactics and **Reverse Engineering**

CAREER PATHS

Pentesters are becoming increasingly popular. They can work **in-house,** as **consultants**, **freelance**, and even start their **own security firm.**

TOOLS

Great penetration testers master practical tools such as **Metasploit, Nmap, BurpSuite, Wireshark, Nessus, Powershell, Ruby, John the Ripper**, and more.

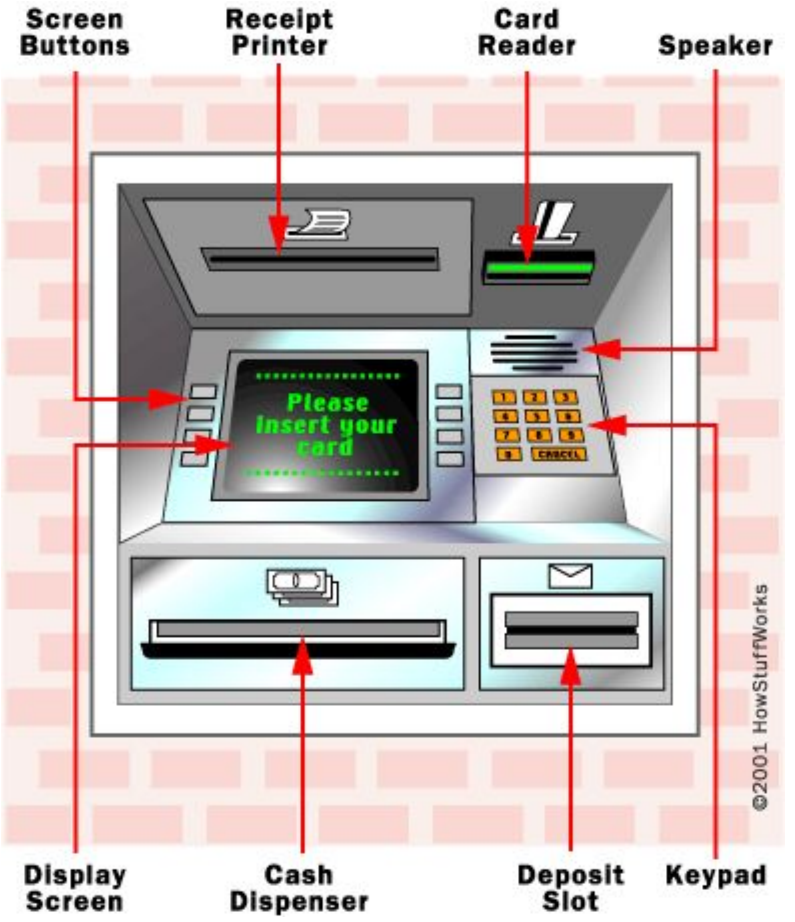
Who needs Penetration Testing

- Banks/Financial Institutions, Government Organizations, Online Vendors, or any organization processing and storing private information

- Most certifications require or recommend that penetration tests be performed on a regular basis to ensure the security of the system.

- PCI Data Security Standard's Section 11.3 requires organizations to perform application and penetration tests at least once a year.

- HIPAA Security Rule's section 8 of the Administrative Safeguards requires security process audits, periodic vulnerability analysis and penetration testing.



https://gbhackers.com/advanced-atm-penetration-testing-methods/

Penetration Testing Viewpoints

-External vs. Internal

Penetration Testing can be performed from the viewpoint of an external attacker or a malicious employee.

- Overt vs. Covert

Penetration Testing can be performed with or without the knowledge of the IT department of the company being tested.

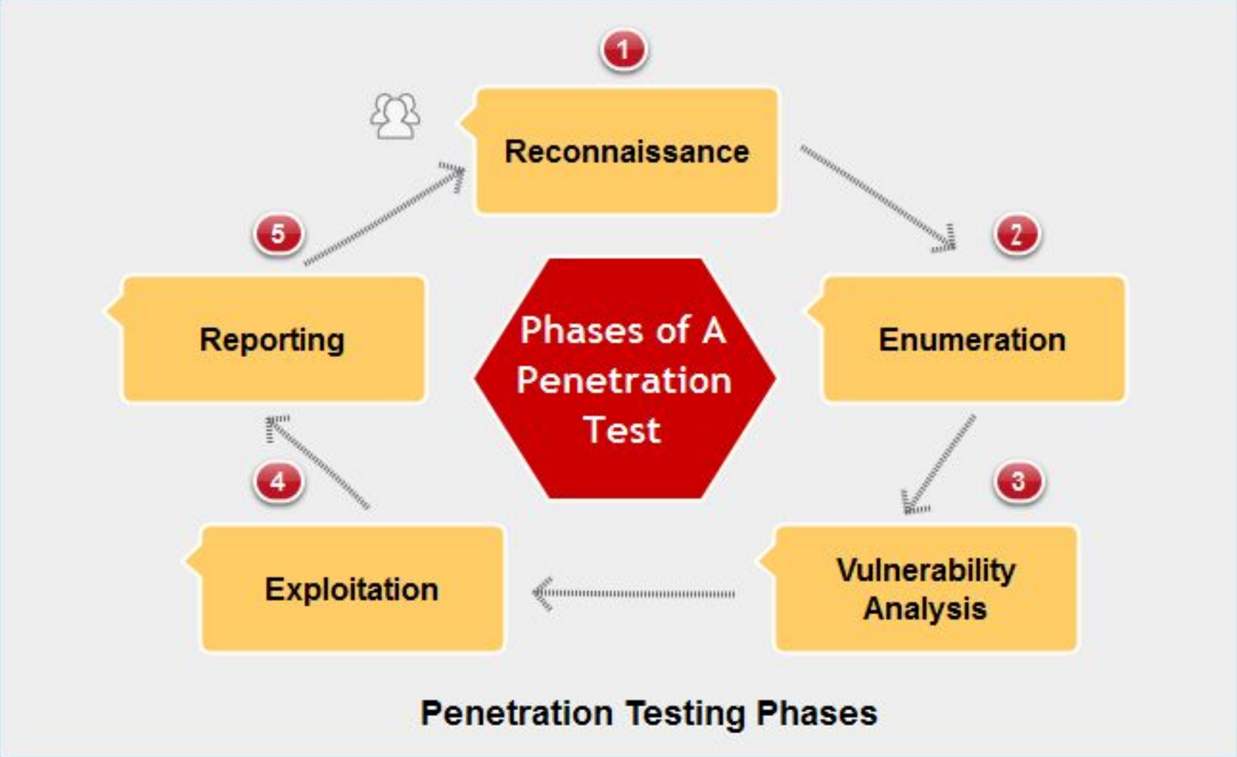
Phases of Penetration Testing

- Reconnaissance and Information Gathering

- Network Enumeration and Scanning

- Vulnerability Testing and Exploitation

- Reporting



Reconnaissance and Information Gathering

Purpose: To discover as much information about a target (individual or organization) as possible without actually making network contact with said target.

Methods:

- Organization info discovery via WHOIS
- Google search
- Website browsing

WHOIS Results for www.netflix.com

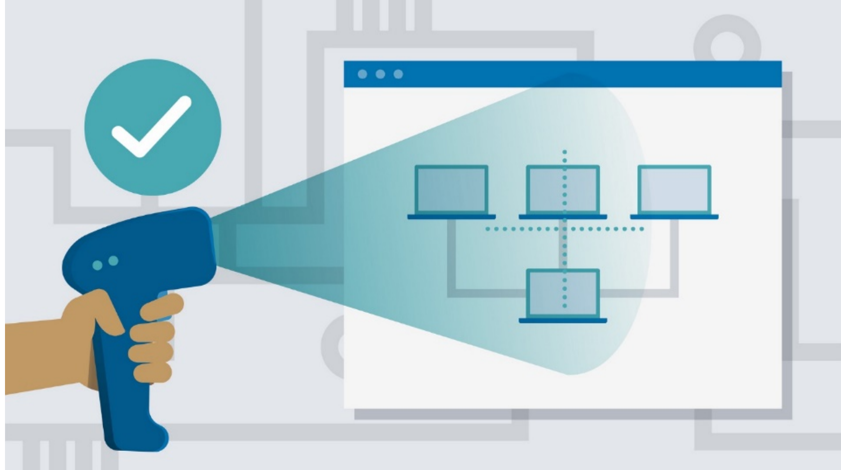
```
Domain Name: netflix.com
Registry Domain ID: 1404215_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2021-10-09T09:37:28+0000
Creation Date: 1997-11-11T05:00:00+0000
Registrar Registration Expiration Date: 2023-11-10T00:00:00+0000
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: email@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895770
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)
Domain Status: serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited)
Domain Status: serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: Netflix, Inc.
Registrant Street: 100 Winchester Circle,
Registrant City: Los Gatos
Registrant State/Province: CA
Registrant Postal Code: 95032
Registrant Country: US
Registrant Phone: +1.4085403700
Registrant Phone Ext:
Registrant Fax: +1.4085403737
Registrant Fax Ext:
Registrant Email: email@netflix.com
```

Network Enumeration and Scanning

Purpose: To discover existing networks owned by a target as well as live hosts and services running on those hosts.

Methods:

- Scanning programs that identify live hosts, open ports, services, and other info (Nmap, autoscan)
- DNS Querying
- Route analysis (traceroute)



NMap Results

```
nmap -sS 127.0.0.1


Starting Nmap 4.01 at 2006-07-06 17:23 BST
Interesting ports on chaos (127.0.0.1):
(The 1668 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
631/tcp  open  ipp
6000/tcp open  X11

Nmap finished: 1 IP address (1 host up) scanned in 0.207
        seconds
```

Vulnerability Testing and Exploitation

Purpose: To check hosts for known vulnerabilities and to see if they are exploitable, as well as to assess the potential severity of said vulnerabilities.

Methods:

- Remote vulnerability scanning (Nessus, OpenVAS)
- Active exploitation testing
  - Login checking and bruteforcing
  - Vulnerability exploitation (Metasploit, Core Impact)
  - 0day and exploit discovery (Fuzzing, program analysis)
  - Post exploitation techniques to assess severity (permission levels, backdoors, rootkits, etc)

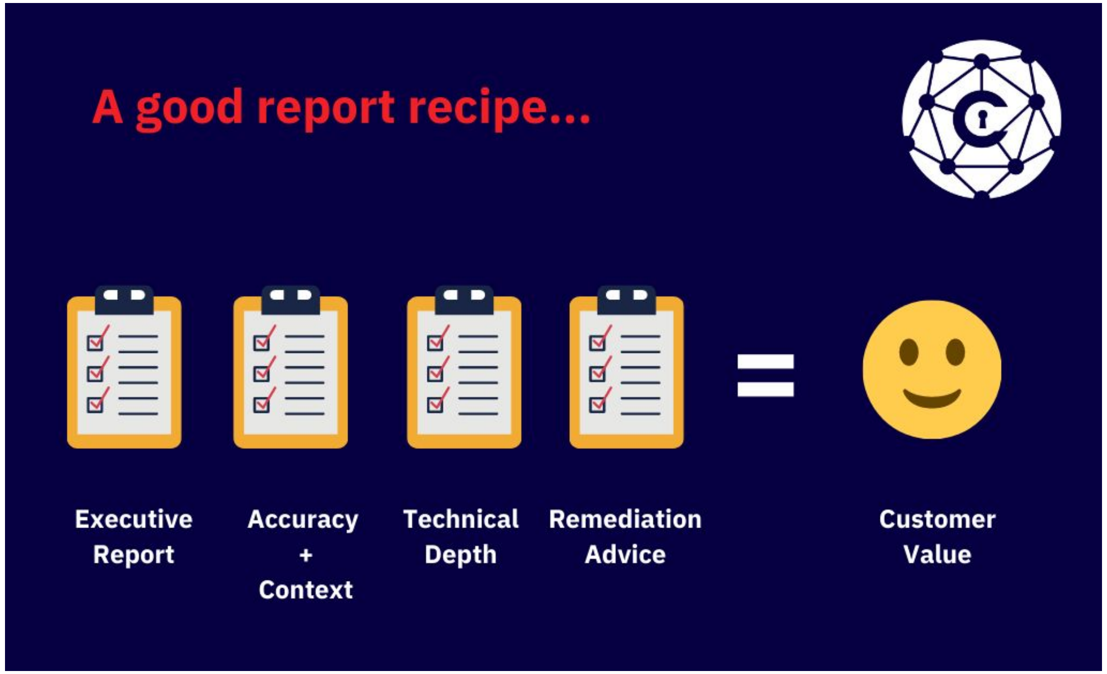
Reporting

Purpose: To organize and document information found during the reconnaissance, network scanning, and vulnerability testing phases of a pentest.

Methods:

Documentation tools (Dradis)

Organizes information by hosts, services, identified hazards and risks, recommendations to fix problems



How to Become a Penetration Tester

- Stay up to date on recent developments in computer security, reading newsletters and security reports are a good way to do this.

- Becoming proficient with C/C++ and a scripting language such as PEARL

- Microsoft, Cisco, and Novell certifications

- Penetration Testing Certifications

    - Certified Ethical Hacker (CEH)

    -GIAC Certified Penetration Tester (GPEN)

Legal aspects of Penetration Testing

Legal Issues

The legal issues that have to be considered when conducting penetration tests can be subdivided into three types:

- Legal issues that can induce or motivate a business or a public authority to conduct a penetration test.

- Legal regulations and principles that the tester should observe when conducting penetration tests and which should be clarified with the client prior to testing.

- Legal aspects which form the basis of the contract between client and penetration tester.

Legal Reasons for Penetration Testing

While there are no laws that require a company or public authority to commission penetration tests, there are binding legal provisions relating to

- Security handling and the availability of data relevant to tax and commercial law,
- Treatment of personal data,
- The establishment and organization of an internal control system.

What You Can Do Legally

- Laws involving technology change as rapidly as technology itself
- Find what is legal for you locally
  - Laws change from place to place
- Be aware of what is allowed and what is not allowed

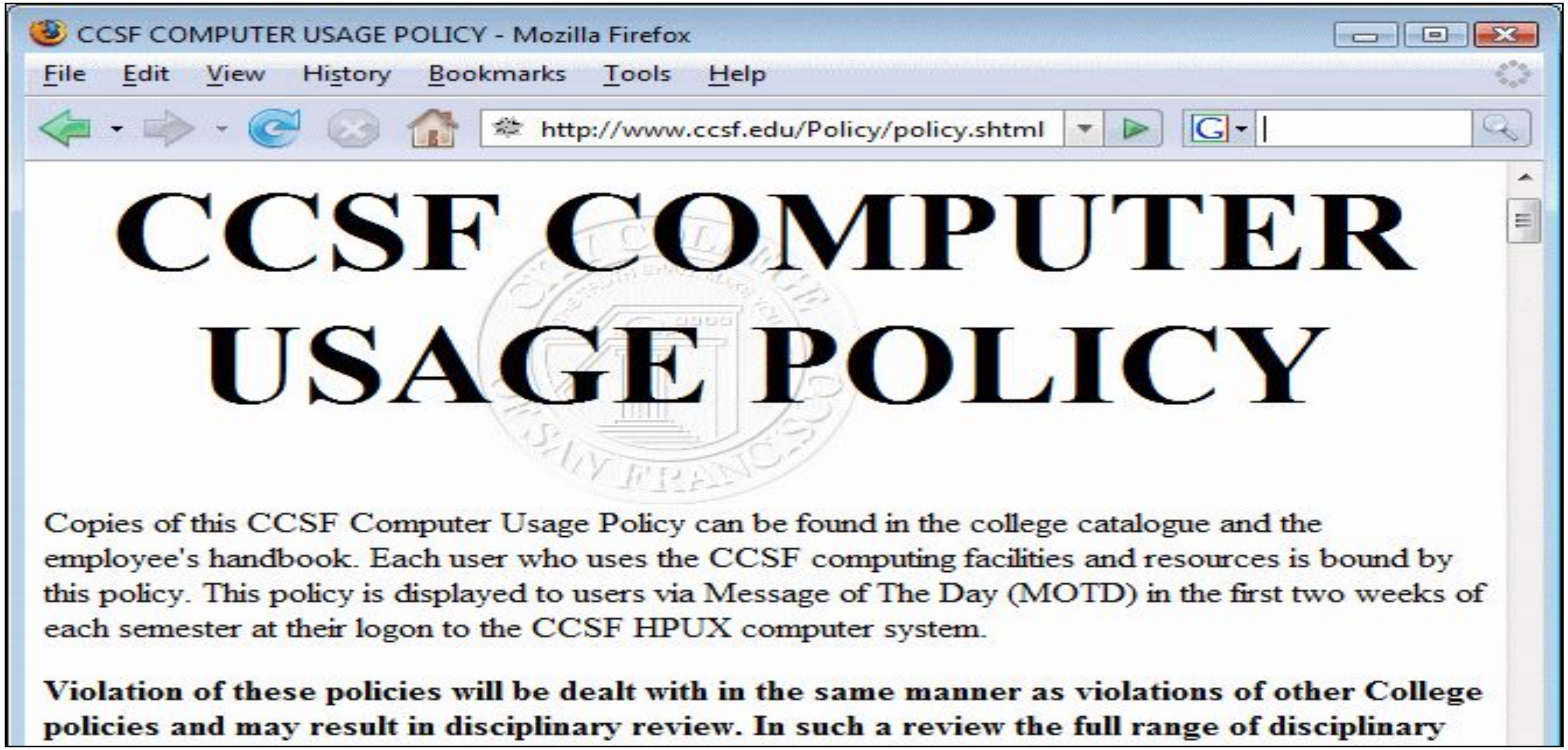
Laws of the Land

- Tools on your computer might be illegal to possess
- Contact local law enforcement agencies before installing hacking tools
- Written words are open to interpretation
- Governments are getting more serious about punishment for cybercrimes

Is Port Scanning Legal?

- Some states deem it legal
- Not always the case
- Federal Government does not see it as a violation
  - Allows each state to address it separately
- Read your ISP's "Acceptable Use Policy"
  - IRC "bots" may be forbidden
    - Program that sends automatic responses to users
    - Gives the appearance of a person being present

CCSF Computer Use Policy



CCSF COMPUTER USAGE POLICY - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.ccsf.edu/Policy/policy.shtml

CCSF COMPUTER USAGE POLICY

Copies of this CCSF Computer Usage Policy can be found in the college catalogue and the employee's handbook. Each user who uses the CCSF computing facilities and resources is bound by this policy. This policy is displayed to users via Message of The Day (MOTD) in the first two weeks of each semester at their logon to the CCSF HPUX computer system.

Violation of these policies will be dealt with in the same manner as violations of other College policies and may result in disciplinary review. In such a review the full range of disciplinary

www.ccsf.edu/Policy/policy.shtml (link Ch 1k)

Federal Laws

- Federal computer crime laws are getting more specific
  - Cover cybercrimes and intellectual property issues
- Computer Hacking and Intellectual Property (CHIP)
  - New government branch to address cybercrimes and intellectual property issues

What You Cannot Do Legally

- Accessing a computer without permission is illegal
- Other illegal actions
  - Installing worms or viruses
  - Denial of Service attacks
  - Denying users access to network resources
- Be careful your actions do not prevent customers from doing their jobs