



Computer Security and Safety, Ethics, and Privacy

Computer Security Risks

- Today, people rely on computers to create, store, and manage critical information.
- It is crucial to take measures to protect their computers and data from loss, damage, and misuse.
- A **computer security risk** is any event or action that could cause a loss of or damage to computer hardware, software, data, information, or processing capability.

Computer Security Risks

- While some breaches are accidental, many are intentional.
- Some intruders do no damage, and merely access data.
- Others may leave messages or alter or damage data.
- An intentional breach of computer security often involves a deliberate act that is against the law.

Computer Security Risks

- Any illegal act involving a computer is referred to as a **computer crime**.
- The term **cybercrime** refers to online or Internet-based illegal acts.
- Software used by cybercriminals sometimes is called *crimeware*.
- Perpetrators of cybercrime fall into seven basic categories: hacker, cracker, script kiddie, corporate spy, unethical employee, cyberextortionist, and cyberterrorist.

Computer Security Risks

- The term **hacker**, although originally a complimentary word for a computer enthusiast, now has a derogatory meaning and refers to someone who accesses a computer or network illegally.
- A **cracker** also is someone who accesses a computer or network illegally but has the intent of destroying data, stealing information, or other malicious actions.
- A **script kiddie** has the same intent as a cracker but does not have the technical skills and knowledge, using prewritten code to break into computers.

Computer Security Risks

- Some corporate spies have excellent computer and networking skills and are hired to break into a specific computer or identify risks in their own organization.
- Unethical employees may break into their employers' computers for a variety of reasons (exploit security, financial gains, etc.)

Computer Security Risks

- A **cyberextortionist** is someone who uses e-mail as a vehicle for extortion, threatening others for personal gain.
- A **cyberterrorist** is someone who uses the Internet or network to destroy or damage computers for personal reasons.
 - The term *cyberwarfare* describes an attack whose goal ranges from disabling a government's computer network to crippling a country.

Internet and Network Attacks

- Information transmitted over networks has a higher degree of security risk than information kept on an organization's premises.
- To determine if your computer is vulnerable to an Internet or network attack, you could use an **online security service**, which is a Web site that evaluates your computer to check for Internet and e-mail vulnerabilities.

Internet and Network Attacks

- Companies and individuals requiring assistance or information about Internet security braches can contact or visit the Web site for the *Computer Emergency Response Team Coordination Center, or CERT/CC*, which is a federally funded Internet security research and development center.

Computer Viruses, Worms, Trojan Horses, and Rootkits

- A computer **virus** is a potentially damaging computer program that affects, or infects, a computer negatively by altering the way the computer works without the user's knowledge.
- A **worm** is a program that copies itself repeatedly, in memory or on a network, using up resources and shutting down the computer or network.

Computer Viruses, Worms, Trojan Horses, and Rootkits

- A **Trojan horse** (named after the Greek myth) is a program that hides within or looks like a legitimate program and causes a condition or action when triggered.
- A **rootkit** is a program that hides in a computer and allows someone from a remote location to take full control of the computer.
 - Execute programs, change settings, etc.

Computer Viruses, Worms, Trojan Horses, and Rootkits

- Computer viruses, worms, Trojan horses, and rootkits are all classified as *malware* (*malicious software*), which are programs that act without a user's knowledge and deliberately alter the computer's operations.
- The *payload* is the destructive event or prank the program is intended to deliver.

Computer Viruses, Worms, Trojan Horses, and Rootkits

- Infected computers can suffer from one or more of the following symptoms:
 - OS running slower
 - Less available memory
 - Corrupted files
 - Unusual messages or images
 - Unusual sounds playing
 - Existing programs and files disappear
 - Programs or files not working properly
 - Unusual programs or files appear
 - OS does not start up or unexpectedly shuts down

Computer Viruses, Worms, Trojan Horses, and Rootkits

- Malware delivers its payload on a computer when a user
 - Opens an infected file
 - Runs an infected program
 - Boots the computer with infected removable media inserted
 - Connects to an unprotected computer or network
 - When a certain condition or event occurs, such as the clock changing to a specific date

Safeguards against Computer Viruses and Other Malware

- Methods that guarantee a computer or network is safe from computer viruses and other malware simply do not exist.
- Do not start a computer with removable media inserted in the drives.
 - If you must start the computer with removable media, be certain it is from a **trusted source**, which is an organization or person you believe will not send a virus.
- Never open an e-mail attachment unless you are expecting the attachment and it is from a trusted source.

Safeguards against Computer Viruses and Other Malware

- Some viruses are hidden in *macros*, which are instructions saved in software such as a word processing or spreadsheet program.
- Users should install an antivirus program and update it frequently.
- An **antivirus program** protects a computer against viruses by identifying and removing any computer virus found in memory, storage, or incoming files.

Safeguards against Computer Viruses and Other Malware

- An antivirus program scans for programs that attempt to modify the boot program, the operating system, and other programs that normally are read from but not modified.
- One technique used to identify a virus is to look for **virus signatures**, also called **virus definitions**, which are a known specific pattern of virus code.

Safeguards against Computer Viruses and Other Malware

- Another technique that antivirus programs use to detect viruses is to inoculate existing program files.
- To **inoculate** a program file, the antivirus program records information such as the file size and creation date in a separate inoculation file, thus enabling it to tell if a file has been tampered with.

Safeguards against Computer Viruses and Other Malware

- If an antivirus program identifies an infected file, it attempts to remove the malware.
- If it cannot remove the infected file, it will attempt to quarantine it.
- A **quarantine** is a separate area of a hard disk that holds infected files until the infection can be removed, ensuring other files will not become infected.

Safeguards against Computer Viruses and Other Malware

- In extreme cases, you may need to reformat the hard disk to remove malware from an infected computer.
- Stay informed about new virus alerts and virus hoaxes.
- A **virus hoax** is an e-mail message that warns users of a nonexistent virus or other malware.
 - They come in the form of chain mail and inform users to delete an important system file claiming it is malware.

Botnets

- A **botnet** is a group of compromised computers connected to a network such as the Internet that are used as part of a network that attacks other networks.
- A compromised computer, known as a **zombie**, is one whose owner is unaware the computer is being controlled remotely by an outsider.
- A *bot* is a program that performs a repetitive task on a network.
- Cybercriminals install malicious bots on unprotected computers to create a botnet, also called a *zombie army*.

Denial of Service Attacks

- A **denial of service attack**, or **DoS attack**, is an assault whose purpose is to disrupt computer access to an Internet service such as the Web or e-mail.
- This is done by flooding a victim computer with confusing data messages, thus making it unresponsive.
- A *DDoS (distributed DoS) attack*, is more devastating, in which a zombie army is used to attack computers or computer networks.

Back Doors

- A **back door** is a program or set of instructions in a program that allow users to bypass security controls when accessing a program, computer, or network.
- Some malware will install a back door once it infects the victim computer.

Spoofing

- **Spoofing** is a technique intruders use to make their network or Internet transmission appear legitimate to a victim computer or network.
- *E-mail spoofing* occurs when the sender's address or other components of the e-mail header are altered so that it appears the e-mail originated from a different sender.
- *IP spoofing* occurs when an intruder computer fools a network into believing its IP address is associated with a trusted source.

Safeguards against Botnets, DoS/DDoS Attacks, Back Doors, and Spoofing

- Some of the latest antivirus programs include provisions to protect a computer from DoS and DDoS attacks.
- Users can also implement firewall solutions, install intrusion detection software, and set up honeypots.

Firewalls

- A **firewall** is a hardware and/or software that protects a network's resources from intrusion by users on another network such as the Internet.
- A *proxy server* is a server outside the organization's network that controls which communications pass into the organization's network.
- A **personal firewall** is a utility program that detects and protects a personal computer and its data from unauthorized intrusions.

Intrusion Detection Software

- *Intrusion detection software* automatically analyzes all network traffic, assesses system vulnerabilities, identifies any unauthorized intrusions, and notifies network admins.

Honeypots

- A *honeypot* is a vulnerable computer that is set up to entice an intruder to break into it.
- They appear real to the intruder but are separated from the organization's network.
- They are used to learn how intruders are exploiting their network.

Unauthorized Access and Use

- **Unauthorized access** is the use of a computer or network without permission.
- **Unauthorized use** is the use of a computer or its data for unapproved or possibly illegal activities.
- At a minimum, organizations should have a written acceptable use policy (AUP) that outlines the computer activities for which the computer and network may and may not be used.

Identifying and Authenticating Users

- An *access control* is a security measure that defines who can access a computer, when, and what actions they can take.
- The computer should maintain an **audit trail** that records in a file both successful and unsuccessful access attempts.
- *Identification* verifies that an individual is a valid user.
- *Authentication* verifies that the individual is the person he or she claims to be.

User Names and Passwords

- A **user name**, or *user ID*, is a unique combination of characters (letters, numbers) that identifies a specific user.
- A **password** is a private combination of characters associated with the user name that allows access to certain computer resources.
- A *CAPTCHA*, which stands for Completely Automated Public Turing test to tell Computers and Humans Apart, is a program developed at CMU to verify that user input is not computer generated.
- A *passphrase* is a private combination of words, often containing mixed capitalization and punctuation, associated with a user name, to be used in place of a password.

Possessed Objects

- A *possessed object* is any item that you must carry to gain access to a computer or computer facility (badges, cards, keys).
- A **personal identification number (PIN)** is a numeric password, either assigned by a company or selected by a user.

Biometric Devices

- A **biometric device** authenticates a person's identity by translating a personal characteristic, such as a fingerprint, into digital code that is compared with a digital code stored in the computer verifying a physical or behavioral characteristic.
 - Ex. *Biometric payment* is used, where a customer's fingerprint is read and their account is charged.
- Biometric devices have disadvantages.
 - Ex. Cut finger for fingerprint readers.

Digital Forensics

- **Digital forensics**, also called *computer forensics*, *network forensics*, or *cyberforensics*, is the discovery, collection, and analysis of evidence found on computers and networks.

Hardware Theft and Vandalism

- **Hardware theft** is the act of stealing computer equipment.
- **Hardware vandalism** is the act of defacing or destroying computer equipment.

Safeguards against Hardware Theft and Vandalism

- Some labs attach physical security devices such as cables that lock the equipment to a desk.
- Some businesses use *real time location system (RTLS)* to track and identify the location of high-risk or high-value items.
- Mobile devices require extra security, such as logon passwords, encrypted data, and even software to photograph the thief.

Software Theft

- **Software theft** occurs when someone steals software media, intentionally erases programs, illegally copies a program, or illegally registers and/or activates a program.
- Software **piracy** is the unauthorized and illegal duplication of copyrighted software.
- Illegally obtaining registration numbers can be done with *keygens*, short for key generators.

Safeguards against Software Theft

- All owned software media should be stored securely.
- A **license agreement** is the right to use the software: you do not own it, you have the right to use it.
- A *single-user license agreement*, also called a *end-user license agreement (EULA)* is the most common license.
 - Install on one computer, make one backup copy, sell it if it is removed from the computer it is on.

Safeguards against Software Theft

- During **product activation**, which is conducted either online or by telephone, users provide the software product's identification number to receive an installation identification number unique to the computer on which the software is installed.

Information Theft

- **Information theft** occurs when someone steals personal or confidential information.
- It has potential of causing more damage than hardware or software theft.
- Information transmitted over networks offers a higher degree of risk.

Safeguards against Information Theft

- Most organizations attempt to prevent information theft by implementing the user identification and authentication controls discussed earlier.

Encryption

- **Encryption** is a process of converting readable data into unreadable characters to prevent unauthorized access.
- It is treated like any other data (it can be stored, sent, etc.)
- To read the data, the recipient must **decrypt**, or decipher, it into a readable form.

Encryption

- The unencrypted, readable data is called *plaintext*.
- The encrypted (scrambled) data is called *ciphertext*.
- An *encryption algorithm*, or *cypher*, is a set of steps that can convert readable plaintext into unreadable ciphertext.

Simple Encryption Algorithms

Name	Algorithm	Plaintext	Ciphertext	Explanation
Transposition	Switch the order of characters	SOFTWARE	OSTFAWER	Adjacent characters swapped
Substitution	Replace characters with other characters	INFORMATION	WLDIMXQUWIL	Each letter replaced with another
Expansion	Insert characters between existing characters	USER	UYSYEYRY	Letter Y inserted after each character
Compaction	Remove characters and store elsewhere	ACTIVATION	ACIVTIN	Every third letter removed (T, A, O)

Encryption

- An *encryption key* is a set of characters that the originator of the data uses to encrypt the plaintext and the recipient of the data uses to decrypt the ciphertext.
- With *private key encryption*, also called *symmetric key encryption*, both the originator and the recipient use the same secret key to encrypt and decrypt the data.
- *Public key encryption*, also called *asymmetric key encryption*, uses two encryption keys, a public and a private.
 - A message generated with a public key can be decrypted only with the private key.

Encryption

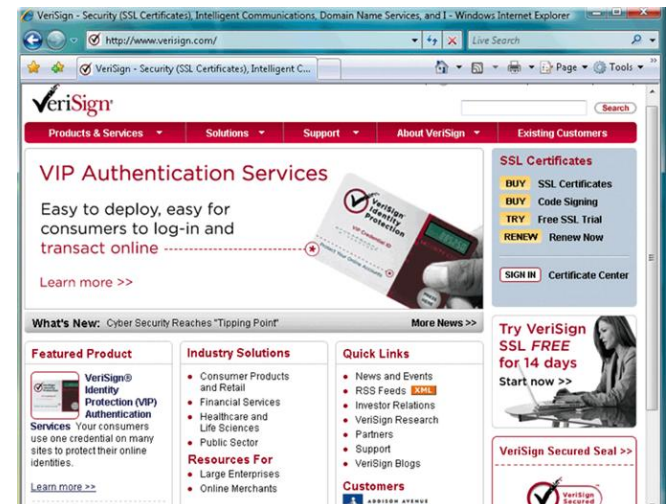
- Some operating systems and e-mail programs allow you to encrypt the contents of files.
- Programs such as *pretty Good Privacy (PGP)* can be used as well.
- A **digital signature** is an encrypted code that a person, Web site, or organization attaches to an electronic message to verify the identity of the message sender.
- It consists of the user's name and a *hash* of all or part of the message, which is a mathematical formula that generates a code from the contents of the message.

Encryption

- Many Web browsers offer *40-bit*, *128-bit*, and even *1024-bit encryption*, which are even higher levels of protection since they have longer keys.
- A Web site that uses encryption techniques is known as a **secure site**, which use digital certificates along with a security protocol.

Digital Certificates

- A **digital certificate** is a notice that guarantees a user or a Web site is legitimate.
- A *certificate authority (CA)* is an authorized person or company that issues and verifies digital certificates.

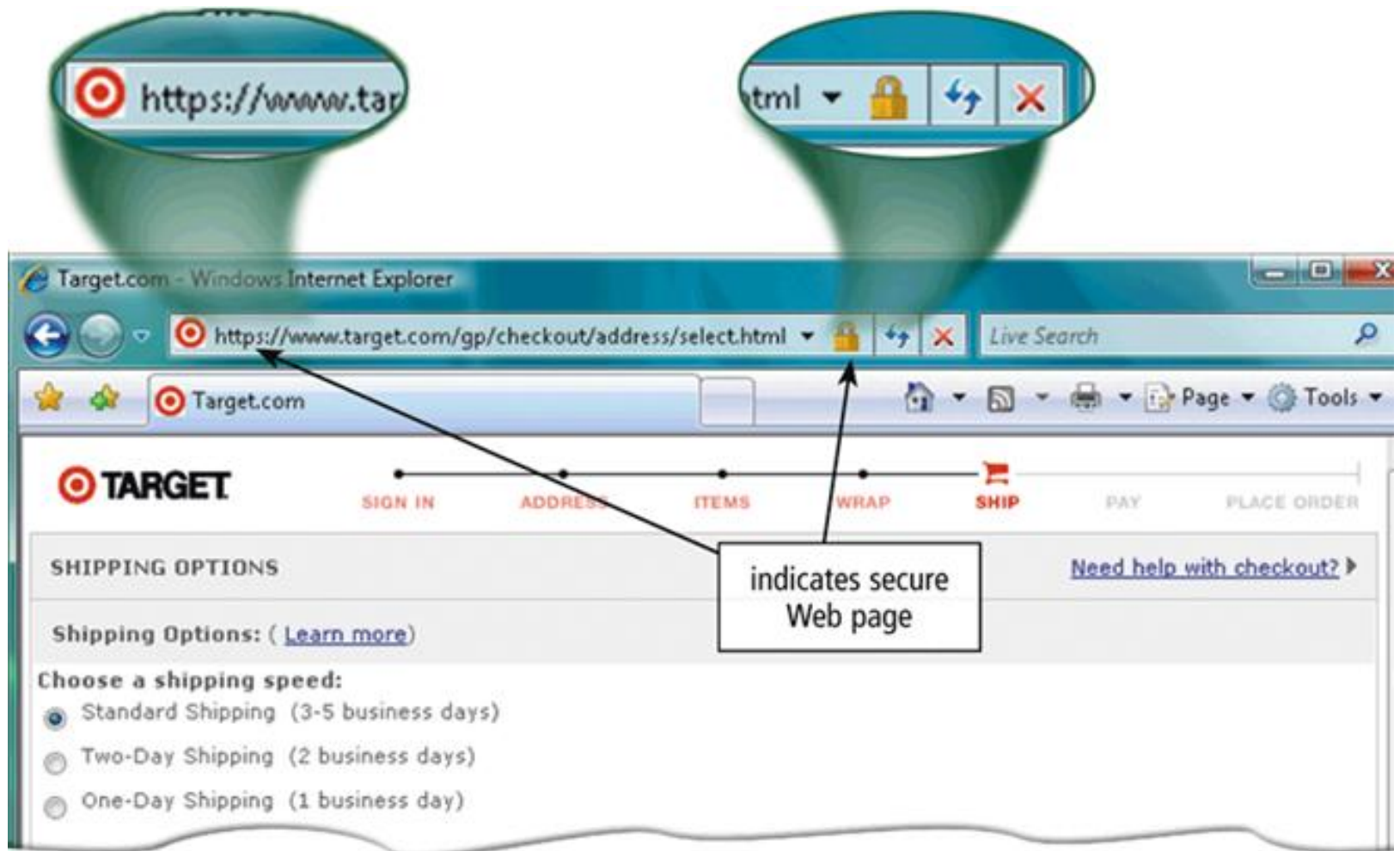


The screenshot displays the VeriSign website interface. At the top, there is a navigation bar with links for "Products & Services", "Solutions", "Support", "About VeriSign", and "Existing Customers". The main content area features a prominent "VIP Authentication Services" section with the text "Easy to deploy, easy for consumers to log-in and transact online" and a "Learn more >>" link. To the right, there is a "SSL Certificates" section with buttons for "BUY SSL Certificates", "BUY Code Signing", "TRY Free SSL Trial", and "RENEW Renew Now", along with a "SIGN IN Certificate Center" button. Below this, a "What's New" section highlights "Cyber Security Reaches 'Tipping Point'". The bottom of the page is divided into several columns: "Featured Product" for VeriSign@ Identity Protection (VIP) Authentication Services, "Industry Solutions" listing sectors like Consumer Products and Retail, Financial Services, Healthcare and Life Sciences, and Public Sector; "Resources For" Large Enterprises and Online Merchants; "Quick Links" for News and Events, RSS Feeds, Investor Relations, VeriSign Research, Partners, Support, and VeriSign Blogs; and "Customers" with a "VeriSign Secured Seal" logo. A sidebar on the right promotes a "Try VeriSign SSL FREE for 14 days" offer.

Transport Layer Security

- *Transport Layer Security (TLS)* a successor to *Secure Sockets Layer (SSL)*, provides encryption of all data that passes between a client and an Internet server.
- Both ends require a certificate and prevents perpetrators from accessing or tampering with communications
- TLS protected websites typically begin with https, instead of http.

Transport Layer Security



Secure HTTP

- *Secure HTTP (S-HTTP)* allows users to choose an encryption scheme for data that passes between a client and server.
- It is more difficult than TLS to use, but it is also more secure.

VPN

- When a mobile user connects to a main office using a standard Internet connection, a *virtual private network (VPN)* provides the mobile user with a secure connection to the company network server, as if the user has a private line.
- They help ensure that data is safe from being intercepted by unauthorized people by encrypting.