

# Computer and Network Security: Threats, Malware, Attacks, Vulnerabilities, and Countermeasures

This document provides a comprehensive overview of computer and network security topics. It covers network security threats, different types of malware, common attacks, vulnerabilities, and countermeasures. The aim is to provide students with a clear understanding of the concepts along with practical examples and prevention techniques.

## Key terms (simple and clear)

An **asset** is anything valuable to an organization, such as data, computer systems, networks, or even employees. A **threat** is anything that has the potential to harm an asset. This could be an external attacker, a malicious program, or even a natural disaster. A **vulnerability** is a weakness in the system that can be taken advantage of by a threat. An **attack** is the actual action where a threat exploits a vulnerability in order to cause harm to the asset. **Malware** is short for malicious software, which refers to programs written with the intention of causing damage or stealing information.

Think of it like a house: the house itself is the asset, an unlocked door is a vulnerability, a thief is the threat, and the act of breaking in is the attack. In this analogy, malware is the harmful tool that the thief might use to break locks or steal valuables.

## Network Security Threats

Network security threats are potential dangers that aim to damage, disrupt, or gain unauthorized access to computer networks and the data they carry. These threats can come from external attackers, malicious insiders, software weaknesses, or even natural events. Understanding these threats is the foundation of building strong defenses in cybersecurity.

### 1. Unauthorized Access

Unauthorized access happens when an attacker or unauthorized person gains entry into a system or network without permission. This can lead to theft of data, installation of malware, or manipulation of files. Weak passwords, poor authentication methods, and misconfigured access controls are common reasons for this threat. *Example:* A hacker logging into an employee's email using a stolen password.

## 2. Eavesdropping (Sniffing)

Eavesdropping refers to secretly listening to or capturing network communication. Attackers use packet-sniffing tools to intercept sensitive data like usernames, passwords, or credit card details while they travel across the network. This is especially dangerous on unsecured public Wi-Fi.

*Example:* A cybercriminal capturing login information from users connected to a coffee shop's Wi-Fi.

## 3. Data Breach

A data breach occurs when sensitive or confidential information is accessed, copied, or stolen by unauthorized parties. Data breaches may expose financial data, personal details, or intellectual property. They often result in financial loss, reputational damage, and legal consequences.

*Example:* Customer databases of companies being leaked online.

## 4. Denial of Service (DoS) and Distributed DoS (DDoS)

These attacks overwhelm a network, server, or website with excessive traffic, making it slow or unavailable to legitimate users. In DDoS attacks, multiple compromised devices (botnets) flood the target system simultaneously.

*Example:* An online banking system becoming unavailable due to a DDoS attack.

## 5. Phishing and Social Engineering

Phishing is the use of fake emails, websites, or messages to trick users into giving away sensitive information like passwords or financial details. Social engineering manipulates people into making security mistakes or revealing confidential data.

*Example:* A fake email pretending to be from a bank asking users to “verify” their account details.

## 6. Insider Threats

Insider threats come from employees, contractors, or partners who misuse their access to harm the organization. It can be intentional (a disgruntled employee leaking data) or unintentional (careless handling of sensitive information).

*Example:* An employee accidentally sending sensitive documents to the wrong person.

## 7. Malware Infections

Malware (viruses, worms, ransomware, etc.) is a common network threat that spreads through email attachments, downloads, or infected websites. Once inside the network, it can disrupt operations, steal data, or take control of systems.  
*Example:* A ransomware attack encrypting files on a corporate server.

## 8. Man-in-the-Middle (MitM) Attacks

In this attack, an attacker secretly intercepts and possibly alters communication between two parties. It allows them to steal sensitive data or insert malicious content without the knowledge of either party.  
*Example:* An attacker intercepting credit card data during an online shopping transaction.

## 9. Advanced Persistent Threats (APT)

An APT is a sophisticated, long-term attack where hackers infiltrate a network and remain undetected for months or years. Their goal is to continuously steal data or monitor systems without raising suspicion.  
*Example:* Nation-state hackers spying on a government's defense network.

## 10. Physical Threats

Sometimes threats are not technical but physical. Natural disasters like earthquakes, floods, and fires, or human-caused events like theft or vandalism, can damage servers and network equipment, leading to downtime and data loss.  
*Example:* A flood damaging a data center.

## Malware

Malware, short for malicious software, refers to programs specifically designed to damage or disrupt systems. It can also be used to steal information, spy on users, or provide attackers with unauthorized access.

Types of malware include viruses, worms, Trojans, ransomware, spyware, adware, rootkits, keyloggers, botnets, and fileless malware. Each type works differently, but all pose significant risks to both individuals and organizations.

## Types of Malware

A **virus** is a piece of malicious code that attaches itself to another program. It only runs when the host program runs, and it can replicate by infecting more files. For example, an infected file on a USB stick might spread the virus whenever someone opens it. Viruses can delete files, corrupt data, and significantly slow down computers.

A **worm** is a self-replicating program that spreads across networks without needing a host file. Unlike a virus, it does not need to attach itself to another program. A worm might scan a network, find vulnerable systems, and automatically copy itself to those systems. Worms can cause major network slowdowns and system crashes due to their rapid spread.

A **Trojan horse**, or simply **Trojan**, is a program that disguises itself as useful or harmless software but carries a hidden malicious function. For example, a free game that secretly opens a backdoor for attackers is a Trojan. Trojans do not replicate themselves but often allow attackers to gain control of the victim's system or steal sensitive information.

**Ransomware** is a type of malware that locks or encrypts the victim's files and then demands payment for the decryption key. Victims are shown a ransom note and are unable to access critical files or systems until they pay. This can cause severe disruption in businesses, leading to financial loss and damage to reputation.

**Spyware** is designed to secretly monitor user activity, such as logging keystrokes, tracking browsing history, or collecting personal data. **Adware**, on the other hand, displays unwanted advertisements, sometimes aggressively, and may also collect information about the user's preferences. While adware may only be annoying, spyware can pose serious privacy and security risks.

A **rootkit** is a malicious program designed to hide the presence of malware and give attackers privileged access to a system. For example, a rootkit can modify operating system files so that security tools do not detect the malware. This makes it extremely hard to find and remove.

**Botnets** are networks of infected computers, known as bots or zombies, that are remotely controlled by an attacker called the botmaster. Botnets can be used to launch large-scale attacks such as Distributed Denial-of-Service (DDoS) attacks, send spam emails, or mine cryptocurrency without the user's knowledge.

**Fileless malware** does not rely on traditional files to infect a system. Instead, it operates directly in a computer's memory or uses legitimate system tools like PowerShell. Because it leaves little trace on disk, fileless malware is difficult to detect using traditional antivirus software.

A **keylogger** is a program that records keystrokes on a computer. Attackers use keyloggers to capture passwords, banking details, or other sensitive information typed by the user.

## Vulnerabilities

Vulnerabilities are weaknesses in systems, processes, or people that attackers can exploit. They can exist in software (bugs, unpatched code), configuration (default passwords, open ports), human behavior (weak passwords, lack of awareness), physical security (unlocked server rooms), or processes (poor patch management).

Recognizing vulnerabilities is the first step toward mitigating them. Security audits and regular updates are essential for reducing risk exposure.

## Various Types of Vulnerabilities

**Software vulnerabilities** are flaws or bugs in software programs. For instance, a buffer overflow or an unpatched operating system may provide an entry point for attackers to exploit.

**Configuration vulnerabilities** happen when systems are set up insecurely. Common examples include leaving default passwords unchanged, leaving ports open unnecessarily, or running services that are not needed. Such oversights create easy entry points for attackers.

**Human vulnerabilities** involve weaknesses in user behavior. These include using weak or reused passwords, falling for phishing emails, or not following security policies. Often, attackers rely on tricking people rather than breaking advanced security technology.

**Physical vulnerabilities** refer to weaknesses in physical security. If servers are left in unlocked rooms or if backup devices are not securely stored, attackers or unauthorized individuals may gain physical access to critical systems and data.

**Process vulnerabilities** occur when an organization lacks proper procedures. For example, if there is no incident response plan, no clear patch management process, or inadequate access controls, attackers can take advantage of the lack of structure.

## Attacks

An attack is a deliberate attempt to exploit vulnerabilities and compromise security. Attackers may target data, systems, or networks for financial gain, espionage, activism, or sabotage.

Common attack types include phishing, SQL injection, cross-site scripting (XSS), denial-of-service (DoS) and distributed denial-of-service (DDoS), man-in-the-middle (MitM), brute-force, supply chain attacks, and zero-day exploits. Understanding these helps in designing defenses and anticipating attacker strategies.

## Common Attack Types

A **phishing attack** works by sending fake emails or messages that appear legitimate in order to trick users into revealing their credentials or clicking malicious links. Phishing can lead to account compromise or malware installation. Preventing phishing requires user awareness training, email filtering systems, and the use of multi-factor authentication.

**SQL Injection** attacks occur when an attacker inserts malicious SQL commands into input fields of a web application. This allows them to read, modify, or delete information from a database. Preventing SQL Injection requires using parameterized queries, validating user inputs, and restricting database privileges.

**Cross-Site Scripting (XSS)** is when attackers inject malicious scripts into web pages that are then viewed by unsuspecting users. This can allow attackers to steal cookies, hijack sessions, or deliver malicious payloads. Developers can prevent XSS by validating input, escaping outputs, and applying content security policies.

A **Denial of Service (DoS)** or **Distributed Denial of Service (DDoS)** attack overwhelms a server or network with too much traffic, making it inaccessible to legitimate users. Preventing DoS attacks involves traffic filtering, using scalable infrastructure, and relying on DDoS protection services.

A **Man-in-the-Middle (MitM)** attack happens when an attacker secretly intercepts communication between two parties. For example, on a public Wi-Fi network, an attacker could intercept messages between a user and a website. Encryption with TLS/HTTPS, VPNs, and certificate validation can protect against MitM.

A **brute force attack** attempts to guess passwords by trying many combinations until one works. This can be prevented by enforcing account lockouts, rate limiting login attempts, requiring strong passwords, and enabling multi-factor authentication.

**Supply chain attacks** occur when attackers compromise third-party software or hardware components. For example, inserting malicious code into a popular software library could allow attackers to reach thousands of users at once. Prevention requires vetting suppliers, monitoring dependencies, and applying patches quickly.

A **zero-day attack** takes advantage of a vulnerability that is unknown to the vendor or the public. Because there is no patch available yet, these attacks are very dangerous. Organizations can defend against zero-day attacks by using layered security controls, monitoring for unusual system behavior, and responding quickly to incidents.

## Countermeasures

Countermeasures are actions, technologies, and procedures implemented to protect systems and data from threats and attacks. They play a crucial role in maintaining the confidentiality, integrity, and availability of information. Effective countermeasures reduce the chances of successful attacks and also help organizations recover quickly if an incident occurs. Below are the key countermeasures explained in detail.

### **Keeping Software and Systems Patched and Updated**

Unpatched systems are one of the most common ways attackers gain access to networks. Software often contains bugs or weaknesses that cybercriminals can exploit to compromise systems. Regularly installing updates and security patches ensures that known vulnerabilities are fixed and attackers cannot use them as entry points. For example, applying updates to operating systems, applications, and antivirus software helps prevent malware infections and exploitation of outdated programs.

### **Using Firewalls, IDS/IPS, and Secure Configurations**

Firewalls serve as the first line of defense by filtering incoming and outgoing traffic and blocking unauthorized access attempts. In addition, Intrusion Detection Systems (IDS) monitor network traffic for suspicious activity, while Intrusion Prevention Systems (IPS) can actively block harmful traffic. Secure configurations also play an important role, as default settings in hardware and software are often insecure. By disabling unnecessary services, changing default passwords, and properly configuring servers and routers, organizations can close common entry points for attackers.

## **Enforcing Strong Authentication**

Authentication ensures that only authorized individuals can access sensitive systems and data. Strong password policies requiring long, complex, and unique passwords make it harder for attackers to guess or crack accounts. However, passwords alone are not enough. Multi-Factor Authentication (MFA), which requires something the user knows (password), something they have (security token or mobile device), or something they are (biometric data), provides an extra layer of protection. For instance, banks often use MFA by requiring both a password and a one-time passcode sent to the user's phone.

## **Encrypting Sensitive Data**

Encryption is a powerful countermeasure that protects data by converting it into unreadable code unless the correct decryption key is used. It ensures confidentiality, even if attackers intercept or steal the data. Encryption should be applied both at rest (such as encrypting files, databases, and hard drives) and in transit (such as using SSL/TLS or VPNs to protect data sent over networks). A good example of this is the use of HTTPS on websites to secure online transactions and protect sensitive information like credit card details.

## **Conducting Regular Backups and Storing Them Securely**

Backups are essential to ensure business continuity and data recovery after incidents such as ransomware attacks, accidental deletion, or hardware failures. Regularly backing up important files ensures that even if systems are compromised, data can be restored. However, it is equally important to store these backups securely, such as offline, in the cloud, or at a geographically separate site. Many organizations maintain encrypted backups that are tested regularly to guarantee they can be restored when needed.

## **Providing User Awareness Training**

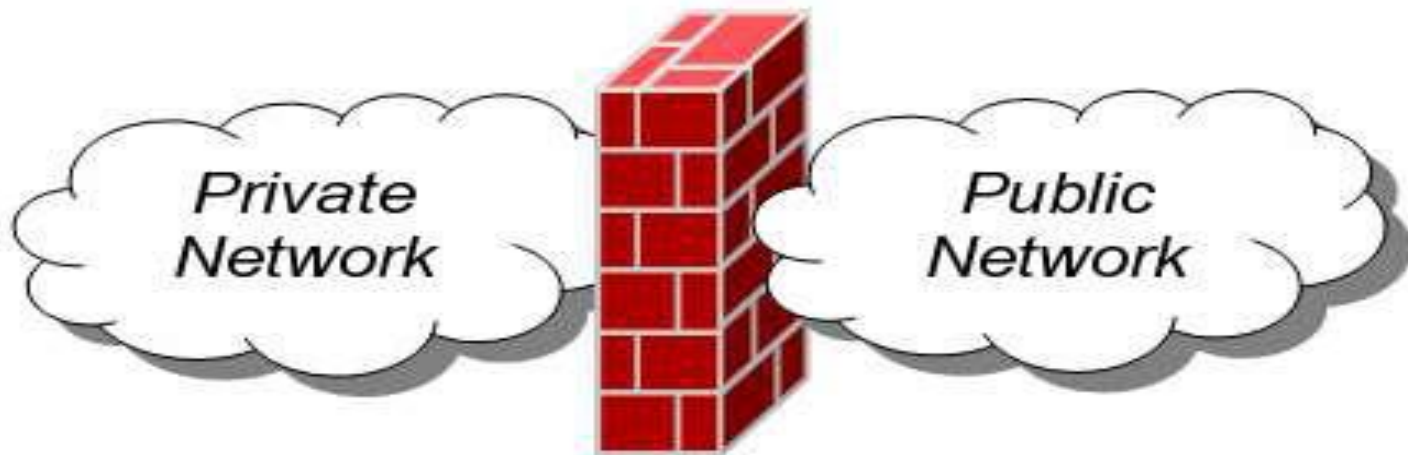
Employees are often considered the weakest link in cybersecurity, as many attacks rely on human error. Awareness training helps reduce this risk by educating users about phishing, social engineering, and other common attack techniques. Training sessions should teach employees how to identify suspicious emails, avoid clicking on unknown links, and report unusual activity. For example, companies often conduct simulated phishing campaigns to test whether staff can recognize fraudulent emails and take the correct action.

## **Conclusion**

Computer and network security is a continuous process of identifying threats, fixing vulnerabilities, and preparing against attacks. By implementing proper countermeasures, organizations can greatly reduce risks and maintain the confidentiality, integrity, and availability of their information systems.

# Firewall

- **Definition:** A Network Firewall is a system or group of systems used to control access between two networks -- a trusted network and an untrusted network -- using pre-configured rules or filters.



- Firewall is device that provides secure connectivity between networks (internal/external).
- It is used to implement and enforce a security policy for communication between networks.
- A firewall may be a hardware, software or a combination of both that is used to prevent unauthorized program or internet users from accessing a private network or a single computer.

- All messages entering or leaving the intranet pass through the firewall, which examines each message & blocks those that do not meet the specified security criteria.

# Why do we need a firewall?

- To protect confidential information from those who do not explicitly need to access it.
- To protect our network & its resources from malicious users & accidents that originate outside of our network.



# Types of firewall

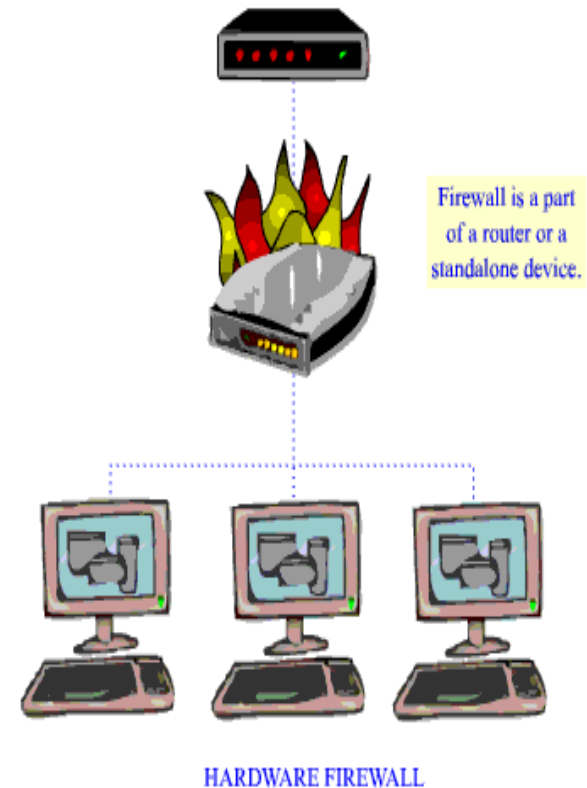
1. Hardware firewall

1. Software firewall

# 1. Hardware Firewall.

It is a physical device.

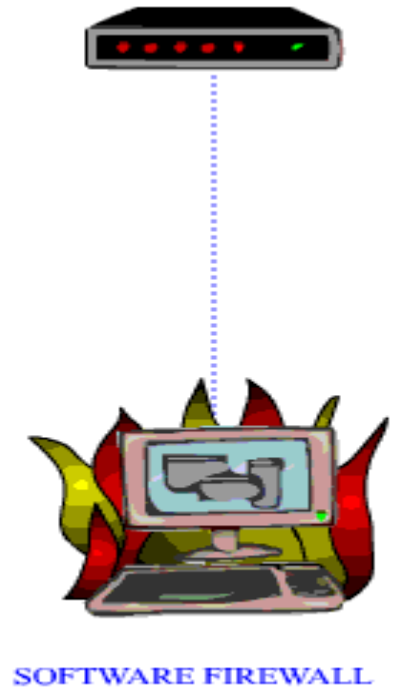
- It can be installed between the modem and computer.
- It can be incorporated into a broadband router being used to share the internet connection.
- Protects an entire network.



- Usually more expensive, harder to configure.
- E.g.- Cisco pix, Netscreen, Watchguard etc.

## 2. Software Firewall

- It is a software application.
- It is installed onto the computer system that you wish to protect .
- Protects a single computer.
- This is usually the computer with modem attached to it.



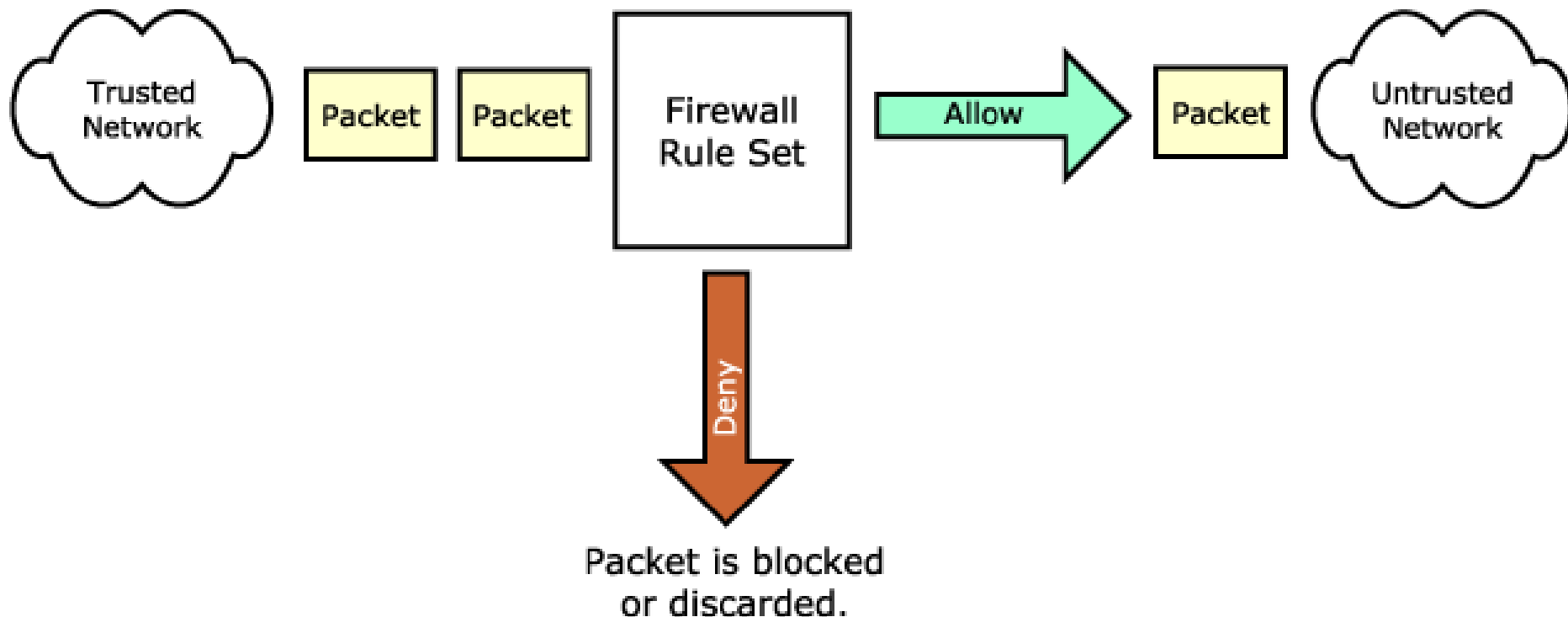
- Usually less expensive, easier to configure.
- E.g.- Norton internet security, MacAfee internet security etc.

# Types of firewall technique

- Packet filter
- Application gateway
- Circuit-level gateway
- Bastion host

# Packet filter

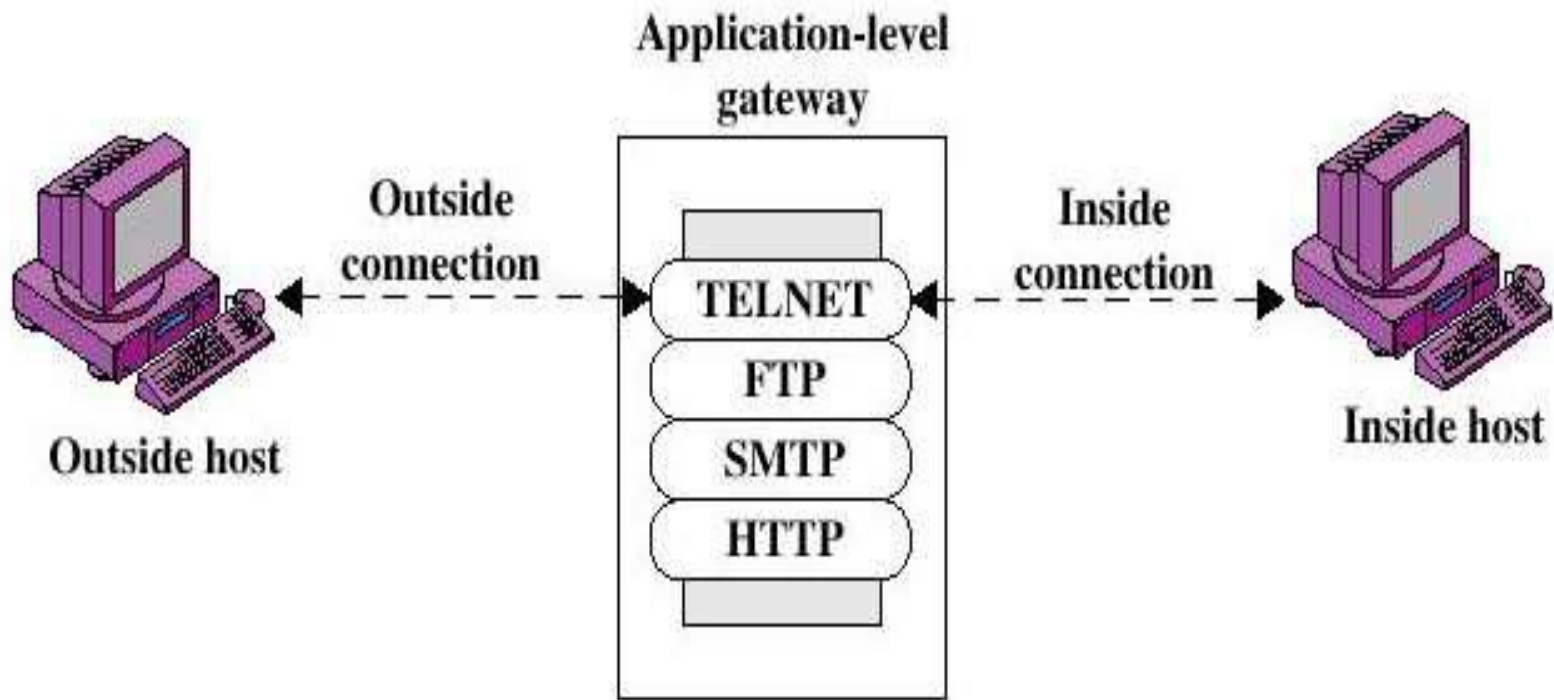
- It looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules.



- Packet filtering is fairly effective & transparent to users, but it is difficult to configure.
- In addition, it is susceptible to IP spoofing.

# **Application gateway**

- In such type of firewall remote host or network can interact only with proxy server, proxy server is responsible for hiding the details of the internal network i.e. intranet.
- Users uses TCP/IP application, such as FTP & Telnet servers.

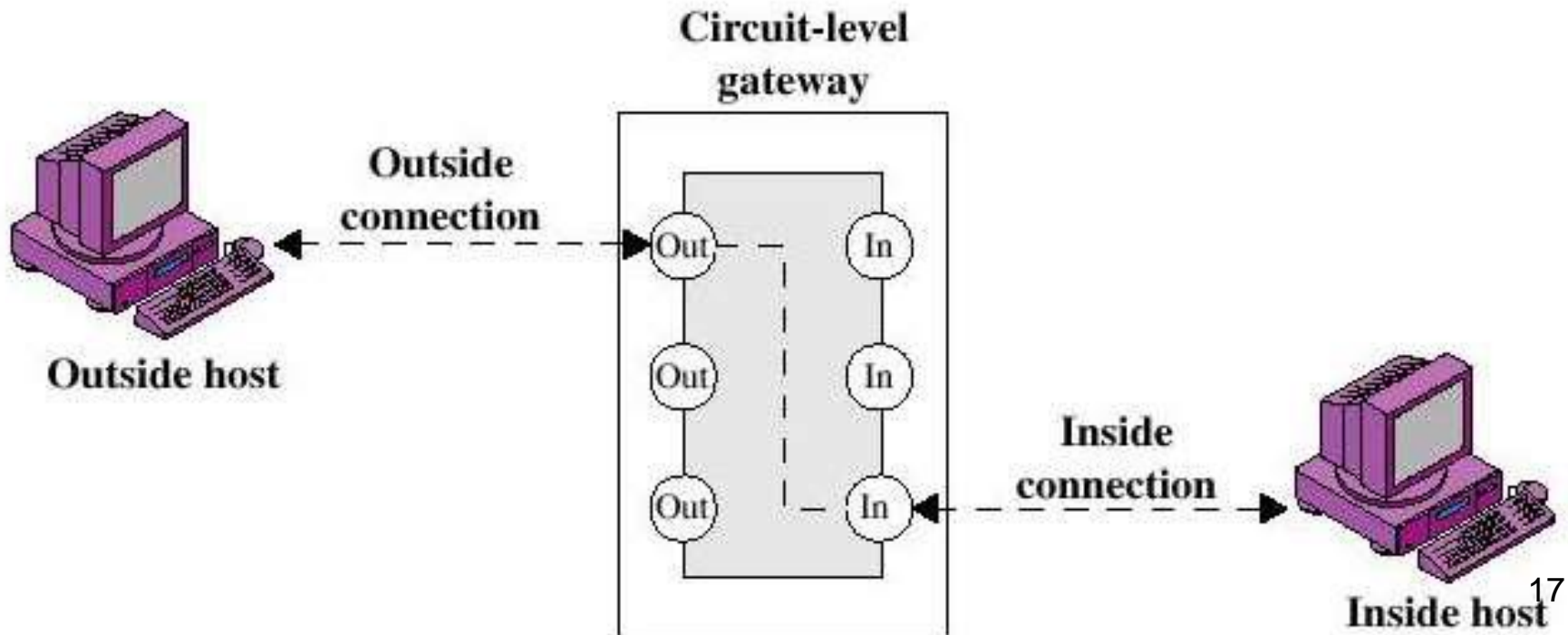


- This is very effective, but can impose a performance degradation.

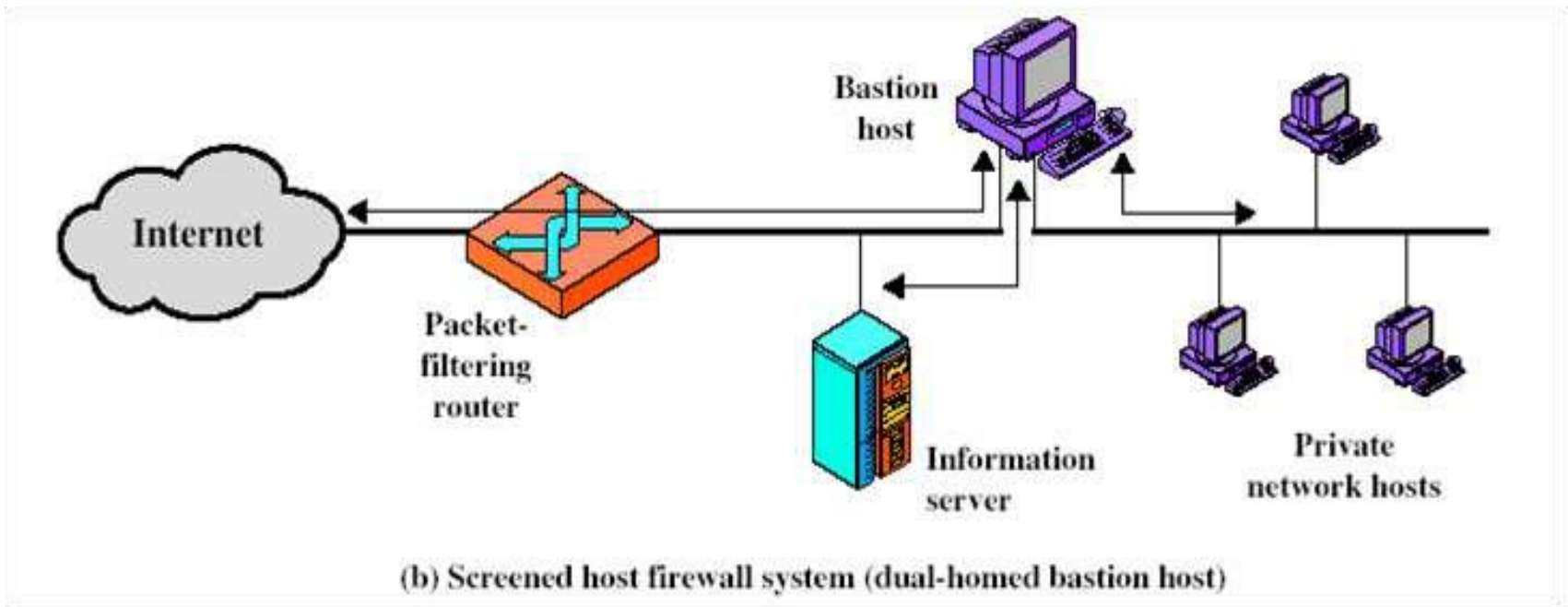
# Circuit – level Firewall

- This can be a stand – alone system or it can be a specialized functions performed by an application – level gateway for certain applications.
- It does not permit an end – to – end TCP connection; rather, the gateway sets two TCP connections.
- A typical use of the circuit – level gateway is a situation in which the system administrator trusts the internal users.

- The gateway can be configured to support application level or proxy service on inbound connections and circuit level functions for outbound connections.



# Bastion Host



- Bastion host is a special purpose computer on a network specifically designed and configured to withstand attacks.

- It generally hosts a single application, provides platform for application gateway and circuit-level gateway.
- It supports limited/specific applications to reduce the threat to the computer.
- Include application-Telnet, SMTP, FTP

# What a personal firewall can do•

Stop hackers from accessing your computer.

- Protect your personal information.
- Blocks “pop up” ads and certain cookies.
- Determines which programs can access the internet.
- Block invalid packets.

# **What a personal firewall can not do**

- Cannot prevent e-mail viruses
  - only an antivirus product with update definitions can prevent e-mail viruses.
- After setting it initially, you cannot forget about it
  - The firewall will require periodic updates to the rule sets and the software itself.

# Firewall Settings

The screenshot shows the Windows Control Panel window titled "System and Security". The left sidebar lists various system settings categories, with "System and Security" selected. The main content area displays several system status tiles, including "Security and Maintenance", "Windows Firewall", "System", "Power Options", "File History", "Backup and Restore (Windows 7)", "Storage Spaces", "Work Folders", "Administrative Tools", "Flash Player (32-bit)", and "Lenovo - System Health and Diagnostic...". The "Windows Firewall" tile is highlighted, showing options to "Check firewall status" and "Allow an app through Windows Firewall". The taskbar at the bottom includes the Start button, a search bar, and several application icons. The system tray on the right shows the time as 10:07 PM on 7/6/2016.

System and Security

Control Panel > System and Security >

Control Panel Home

- **System and Security**
- Network and Internet
- Hardware and Sound
- Programs
- User Accounts
- Appearance and Personalization
- Clock, Language, and Region
- Ease of Access

**Security and Maintenance**  
Review your computer's status and resolve issues | Change User Account Control settings | Troubleshoot common computer problems

**Windows Firewall**  
Check firewall status | Allow an app through Windows Firewall

**System**  
View amount of RAM and processor speed | Allow remote access | Launch remote assistance | See the name of this computer

**Power Options**  
Change battery settings | Require a password when the computer wakes | Change what the power buttons do | Change when the computer sleeps

**File History**  
Save backup copies of your files with File History | Restore your files with File History

**Backup and Restore (Windows 7)**  
Backup and Restore (Windows 7) | Restore files from backup

**Storage Spaces**  
Manage Storage Spaces

**Work Folders**  
Manage Work Folders

**Administrative Tools**  
Free up disk space | Defragment and optimize your drives | Create and format hard disk partitions | View event logs | Schedule tasks

**Flash Player (32-bit)**

**Lenovo - System Health and Diagnostic...**

Search the web and Windows

10:07 PM  
7/6/2016

# Legal and Ethical Issue

---

**A person without ethics  
can't climb up to  
the tip of success.**

- Security Aspects of Computer
- Copyrights, Patents, Trade Secret
- Comparison
- Computer Crime
- Law , Ethics
- Ethical Reasoning
- The Taxonomy of Ethical Theories
- Case Studies of Ethics
- Digital Security Act, IEEE & ACM Code of Ethics

# Security Aspects of Computer

---

- Protecting computing systems against criminals.
- Protecting code and data.
- Protecting programmers' and employers' rights.
- Protecting private data about individuals
- Protecting users of programs.



# Copyrights

---

- Copyrights are designed to protect the expression of ideas.
- The right to copy an expression of an idea is protected by a copyright
- A copyright applies to a creative work, such as a story, photograph, song, or pencil sketch



# Patents

---

- Patents are unlike copyrights in that they protect inventions, tangible objects, or ways to make them, not works of the mind
- A patent can protect a "new and useful process, machine, manufacture, or composition of matter."



# Trade Secret

---

- A trade secret is information that gives one company a competitive edge over others.

**Example:** the formula for a soft drink is a trade secret, as is a mailing list of customers or information about a product due to be announced in a few months.



# Comparison

| Topics                       | Copyright  | Patent  | Trade Secret                      |
|------------------------------|--|---|-----------------------------------|
| <b>Protects</b>              | Expression of idea, not idea itself  | Invention—the way something works             | A secret, competitive advantage   |
| <b>Protected object made</b> | Yes; intention is to promote publication                                   | Design filed at Patent Office                 | No                                |
| <b>Requirement to</b>        | Yes  | No  | No                                |
| <b>Ease of filing</b>        | Very easy, do-it-yourself  | Very complicated; specialist lawyer suggested | No filing                         |
| <b>Duration</b>              | Life of human originator plus 70 years, or total of 95 years for a company | 19 years                                      | Indefinite                        |
| <b>Legal protection</b>      | Sue if unauthorized copy sold  | Sue if invention copied                       | Sue if secret improperly obtained |



# Computer Crime

---

- Computer crime can be defined as unauthorized access of computers, networks, or services differ from those about trespass.
- **Computer Crime Is Hard to define:**
  - Some people in the legal process do not understand computers and computing
  - Creating and changing laws are slow processes



# Computer Crime

---

## ➤ **Computer Crime Is Hard to Prosecute:**

- Lack of understanding
- Lack of physical evidence.
- Lack of recognition of assets.
- Lack of political impact.
- Complexity of Case.
- Juveniles.



# Law

---

- The law is used to regulate people for their own good and for the greater good of society. It is described by formal, written documents and interpreted by courts.
- **Issues Related to law:**
  - Laws apply to everyone.
  - There is regular process through the courts for determining which law supersedes which if two laws conflict.
  - Identify certain actions as right and others as wrong.
  - Laws can be enforced.



# Ethics

---

- Ethics is a set of principles or norms for justifying what is right or wrong in a given situation.
  
- **Issues Related to Ethics:**
  - Ethics are personal. Two persons may have different frameworks for making moral judgment.
  - Ethical position can and often do come into conflict.
  - Two people may assess ethical value differently.
  - There is no enforcement for ethical choice.



# Comparison

| Law   | Ethics  |
|---|---|
| Described by formal, written documents              | Described by unwritten principles                               |
| Interpreted by courts                               | Interpreted by each individual                                  |
| Established by legislatures representing all people | Presented by philosophers, religions, professional groups       |
| Applicable to everyone                              | Personal choice   |
| Priority determined by courts if two laws conflict  | Priority determined by an individual if two principles conflict |
| Court is final arbiter of "right"                   | No external arbiter   |
| Enforceable by police and courts                    | Limited enforcement   |



# Ethical reasoning

---

- Ethical reasoning refers by analyzing certain situations making and justifying an ethical choice .
- Study of ethics can yield two positive results
  - First, in situations where we already know what is right and what is wrong, ethics should help us justify our choice.
  - Second, if we do not know the ethical action to take in a situation, ethics can help us identify the issues involved so that we can make reasoned judgments.



# Ethical reasoning

---

## ➤ **Steps to Make and Justify an Ethical Choice**

- Understand the situation
- Know several theories of ethical reasoning

List the ethical principles involved

- Determine which principles outweigh others



# The Taxonomy of Ethical Theories

## Taxonomy of Ethical Theories.

|            | Consequence-based                       | Rule-based  |
|------------|---|---|
| Individual | Based on consequences to individual     | Based on rules acquired by the individual—from religion, experience, analysis |
| Universal  | Based on consequences to all of society | Based on universal rules, evident to every                                    |



# Case Studies of Ethics

---

- **Case I: Use of Computer Services**
- **Case II: Privacy Rights**
- **Case III: Denial of Service**
- **Case IV: Ownership of Programs**
- **Case V: Proprietary Resources**
- **Case VI: Fraud**
- **Case VII: Accuracy of Information**
- **Case VIII: Ethics of Hacking or Cracking**



# Case I: Use of Computer Services

- Dave works as a programmer for a large software company. He writes and tests utility programs such as compilers. His company operates two computing shifts: during the day program development and online applications are run; at night batch production jobs are completed.
- Dave has access to workload data and learns that the evening batch runs are complementary to daytime programming tasks; that is, adding programming work during the night shift would not adversely affect performance of the computer to other users.
- Dave comes back after normal hours to develop a program to manage his own stock portfolio. His drain on the system is minimal, and he uses very few expendable supplies, such as printer paper.

Is Dave's behavior ethical?



# Case Studies of Ethics

---

## ➤ **Case I: Use of Computer Services**

### ❑ **Values Issues**

Some of the ethical principles involved in this case are listed below.

- Ownership of resources
- Effect on others
- Universalism principle
- Possibility of detection, punishment



# Case Studies of Ethics

## ➤ Case II: Privacy Rights

### ❑ Values Issues

Some of the ethical principles involved in this case are listed below.

- Job responsibility
- Use
- Possible misuse
- Confidentiality
- Tacit permission
- Propriety



# Self Study (Mandatory)

- Digital Security Act Bangladesh (<https://www.cirt.gov.bd/wp-content/uploads/2020/02/Digital-Security-Act-2020.pdf>)
  - *Main Points*
  - *Analysis and Criticism*
- IEEE code of Ethics (<https://www.ieee.org/about/corporate/governance/p7-8.html>)
- ACM Code of Ethics and Professional Conduct (<https://www.acm.org/code-of-ethics>)



# Digital Security Act Bangladesh

রেজিস্টার্ড নং ভি এ-১

বাংলাদেশ



গেজেট

অতিরিক্ত সংখ্যা  
কর্তৃপক্ষ কর্তৃক প্রকাশিত

রবিবার, অক্টোবর ৬, ২০১৯

Government of the People's Republic of Bangladesh  
Legislative and Parliamentary Affairs Division  
Ministry of Law, Justice and Parliamentary Affairs

## NOTIFICATION

Dated: 30 September, 2019 AD/15 Ashwin, 1426 BE

**S.R.O. NO. 310-Law/2019.**—In exercise of the powers conferred by section 62 of the Digital Security Act, 2018, the Government is pleased to publish the following English translation of the Act to be called the Authentic English Text of the Act, and it shall be deemed to have been effective from the date on which the Act comes into force under sub-section (2) of section 1 of the Act:

### DIGITAL SECURITY ACT, 2018

Act No. XLVI of 2018

**An Act to make provisions for ensuring digital security and identification, prevention, suppression and trial of offences committed through digital device and for matters ancillary thereto**

**WHEREAS** it is expedient and necessary to make provisions for ensuring digital security and identification, prevention, suppression and trial of offences committed through digital device and for matters ancillary thereto;

**THEREFORE,** it is hereby enacted as follows:—

( ২০১৯ )

মূল্য : টাকা ২৪.০০



# IEEE code of Ethics



The professional home for the engineering and technology community worldwide

Search all IEEE websites



[About](#) [Membership](#) [Communities](#) [Conferences](#) [Standards](#) [Publications](#) [Education](#)

[JOIN IEEE](#)

[Home](#) > [About](#) > [Corporate](#) > [Governance](#)

## IEEE Code of Ethics

[Related information](#)

The following is from the IEEE Policies, Section 7 - Professional Activities (Part A - IEEE Policies).

[Click here to download a copy of the IEEE Code of Ethics](#)

### 7.8 IEEE Code of Ethics

We, the members of the IEEE, in recognition of the importance of our technologies in affecting the quality of life throughout the world, and in accepting a personal obligation to our profession, its members and the communities we serve, do hereby commit ourselves to the highest ethical and professional conduct and agree:

I. To uphold the highest standards of integrity, responsible behavior, and ethical conduct in professional activities.

1. to hold paramount the safety, health, and welfare of the public, to strive to comply with ethical design and sustainable

#### Governance Procedures

- [Board 30-Day Review/Approval Process](#)
- [Revisions to IEEE Governing Documents](#)
- [Glossary of Terms \(PDF, 62 KB\)](#)
- [IEEE Email Terms and Conditions](#)

Activate Windows  
Go to Settings to activate Windows



# ACM Code of Ethics and Professional Conduct



*Celebrating 75 Years of Advancing Computing as a Science & Profession*

[Digital Library](#)

[CACM](#)

[Queue](#)

[TechNews](#)

[Career Center](#)

[Join](#)

[Volunteer](#)

[myACM](#)

[Search](#)

[ABOUT ACM](#) [MEMBERSHIP](#) [PUBLICATIONS](#) [SIGS](#) [CONFERENCES](#) [CHAPTERS](#) [AWARDS](#) [EDUCATION](#) [LEARNING CENTER](#) [PUBLIC POLICY](#) [DIVERSITY, EQUITY & INCLUSION](#)

[Home](#) > [Code Of Ethics](#)

## ACM Code of Ethics and Professional Conduct

### ACM Code of Ethics and Professional Conduct

#### Preamble

Computing professionals' actions change the world. To act responsibly, they should reflect upon the wider impacts of their work, consistently supporting the public good. The ACM Code of Ethics and Professional Conduct ("the Code") expresses the conscience of the profession.

The Code is designed to inspire and guide the ethical conduct of all computing professionals, including current and aspiring practitioners, instructors, students, influencers, and anyone who uses computing technology in an impactful way. Additionally, the Code serves as a basis for remediation when violations occur. The Code includes principles formulated as statements of responsibility, based on the understanding that the public good is always the primary consideration. Each principle is supplemented by

#### On This Page

##### [Preamble](#)

##### [1. GENERAL ETHICAL PRINCIPLES.](#)

[1.1 Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing.](#)

[1.2 Avoid harm.](#)

[1.3 Be honest and trustworthy.](#)

[1.4 Be fair and take action not to](#)

Activate Windows  
Go to Settings to activate Windows

