**Network Security Concepts**

Today, hacks, data breaches, and cyberattacks are more common than ever before. In fact, the number of data breaches that exposed private records [more than doubled between 2015 and 2017 alone](https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/" \t "https://www.comptia.org/content/guides/_blank). The increasing number and severity of these attacks make network security a topic of utmost importance, especially for [current and prospective certified IT professionals](https://www.comptia.org/certifications/network).

Network security is a smaller subset that falls under the larger umbrella of cybersecurity, and it refers to the practice of preventing unauthorized users from accessing computer networks and their associated devices. It involves physically protecting network servers and devices from external threats, as well as taking steps to secure the digital network. In an age of increasingly sophisticated and frequent cyberattacks, network security matters more now than ever before.

## The Importance of Network Security

Network security is vital to [maintaining the integrity of your data](https://www.comptia.org/blog/not-all-heroes-wear-capes-5-ways-to-better-protect-data) and the privacy of your organization and employees. It encompasses everything from the most basic practices, such  [creating strong passwords](https://www.comptia.org/blog/security-awareness-training-passwords) and fully logging out of community computers, to the most complex, high-level processes that keep networks, devices and their users safe. More and more sensitive information is stored online and in these various devices, and if an unauthorized user gains access to that data, it could lead to disastrous results.

Network security is the key to keeping that sensitive information safe, and as more private data is stored and shared on vulnerable devices, network security will only grow in importance and necessity. Experts expect that [more than 2,314 exabytes (or over 2 trillion gigabytes) of data](https://www.emc.com/analyst-report/digital-universe-healthcare-vertical-report-ar.pdf" \t "https://www.comptia.org/content/guides/_blank) will exist by 2020; managing that amount of data is difficult enough, and protecting it will be another issue entirely.

While each and every member of your organization can take strides to help keep things secure, network security has become more complex in recent years. Adequately protecting networks and their connected devices requires [comprehensive network training](https://www.comptia.org/training/by-certification/network), a thorough understanding of how networks actually work and the skills to put that knowledge into practice. It’s crucial for networks to be thoroughly and properly set up, secured and monitored to fully preserve privacy.

Network security is any activity designed to protect the usability and integrity of your network and data.

* It includes both hardware and software technologies
* It targets a variety of threats
* It stops them from entering or spreading on your network
* Effective network security manages access to the network

### **Types of Network Security:**

### **Firewalls**

Firewalls put up a barrier between your trusted internal network and untrusted outside networks, such as the Internet. They use a set of defined rules to allow or block traffic. A firewall can be hardware, software, or both. Cisco offers [unified threat management](https://meraki.cisco.com/products/appliances?DTID=odicdc000132&CCID=cc000828) (UTM) devices and threat-focused [firewalls](https://www.cisco.com/c/en/us/products/security/firewalls/index.html).

**Email security**

Email gateways are the number one threat vector for a security breach. Attackers use personal information and social engineering tactics to build sophisticated phishing campaigns to deceive recipients and send them to sites serving up malware. An email security application blocks incoming attacks and controls outbound messages to prevent the loss of sensitive data.

**Anti-virus and anti-malware software**

"Malware," short for "malicious software," includes viruses, worms, Trojans, ransomware, and spyware. Sometimes malware will infect a network but lie dormant for days or even weeks. The [best antimalware programs](https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-antivirus-protection.html) not only scan for malware upon entry, but also continuously track files afterward to find anomalies, remove malware, and fix damage.

### **Network segmentation**

Software-defined segmentation puts network traffic into different classifications and makes [enforcing security policies](https://www.cisco.com/c/en/us/products/security/what-is-network-security-policy-management.html?DTID=odicdc000132&CCID=cc000828" \o "US Site) easier. Ideally, the classifications are based on endpoint identity, not mere IP addresses. You can assign access rights based on role, location, and more so that the right level of access is given to the right people and suspicious devices are contained and remediated.

### **Access control**

Not every user should have access to your network. To keep out potential attackers, you need to recognize each user and each device. Then you can enforce your security policies. You can block noncompliant endpoint devices or give them only limited access. This process is network access control (NAC).

### **Application security**

Any software you use to run your business needs to be protected, whether your IT staff builds it or whether you buy it. Unfortunately, any application may contain holes, or vulnerabilities, that attackers can use to infiltrate your network. Application security encompasses the hardware, software, and processes you use to close those holes.

**Behavioral analytics**

To detect abnormal network behavior, you must know what normal behavior looks like. Behavioral analytics tools automatically discern activities that deviate from the norm. Your security team can then better identify indicators of compromise that pose a potential problem and quickly remediate threats.

### **Cloud security**

Cloud security is a broad set of technologies, policies, and applications applied to defend online IP, services, applications, and other imperative data. It helps you better manage your security by shielding users against threats anywhere they access the Internet and securing your data and applications in the cloud.

### **Data loss prevention**

Organizations must make sure that their staff does not send sensitive information outside the network. Data loss prevention, or DLP, technologies can stop people from uploading, forwarding, or even printing critical information in an unsafe manner.

### **Intrusion prevention systems**

An intrusion prevention system (IPS) scans network traffic to actively block attacks. [Secure IPS](https://www.cisco.com/c/en/us/products/security/ngips/index.html) appliances do this by correlating huge amounts of global [threat intelligence](https://www.cisco.com/c/en/us/products/security/what-is-cyber-threat-intelligence.html?DTID=odicdc000132&CCID=cc000828) to not only block malicious activity but also track the progression of suspect files and malware across the network to prevent the spread of outbreaks and reinfection.

### **Mobile device security**

Cybercriminals are increasingly targeting mobile devices and apps. Within the next 3 years, 90 percent of IT organizations may support corporate applications on personal mobile devices. Of course, you need to control which devices can access your network. You will also need to configure their connections to keep network traffic private.

### **Security information and event management**

SIEM products pull together the information that your security staff needs to identify and respond to threats. These products come in various forms, including physical and virtual appliances and server software.

**VPN**

A virtual private network encrypts the connection from an endpoint to a network, often over the Internet. Typically, a remote-access VPN uses IPsec or Secure Sockets Layer to authenticate the communication between device and network.

**Web security**

A web security solution will control your staff’s web use, block web-based threats, and deny access to malicious websites. It will protect your web gateway on site or in the cloud. "Web security" also refers to the steps you take to protect your own website.

### **Wireless security**

### Wireless networks are not as secure as wired ones. Without stringent security measures, installing a wireless LAN can be like putting Ethernet ports everywhere, including the parking lot. To prevent an exploit from taking hold, you need products specifically designed to protect a wireless network.

**Network Security Threats**

### 1. Computer virus

### We’ve all heard about them, and we all have our fears. For everyday Internet users, computer viruses are one of the most common threats to cybersecurity. Statistics show that approximately 33% of household computers are affected with some type of malware, more than half of which are viruses.

### Computer viruses are pieces of software that are designed to be spread from one computer to another. They’re often sent as email attachments or downloaded from specific websites with the intent to infect your computer — and other computers on your contact list — by using systems on your network. Viruses are known to send spam, disable your security settings, corrupt and steal data from your computer including personal information such as passwords, even going as far as to delete everything on your hard drive.

### 2. Trojan horse

### Metaphorically, a “Trojan horse” refers to tricking someone into inviting an attacker into a securely protected area. In computing, it holds a very similar meaning — a Trojan horse, or “Trojan,” is a malicious bit of attacking code or software that tricks users into running it willingly, by hiding behind a legitimate program.

### They spread often by email; it may appear as an email from someone you know, and when you click on the email and its included attachment, you’ve immediately downloaded malware to your computer. Trojans also spread when you click on a false advertisement.

### Once inside your computer, a Trojan horse can record your passwords by logging keystrokes, hijacking your webcam, and stealing any sensitive data you may have on your computer.

### 3. Computer worm

### Computer worms are pieces of malware programs that replicate quickly and spread from one computer to another. A worm spreads from an infected computer by sending itself to all of the computer’s contacts, then immediately to the contacts of the other computers.

### Interestingly, they are not always designed to cause harm; there are worms that are made just to spread. Transmission of worms is also often done by exploiting software vulnerabilities.

# **Impact of Cyber Crimes**

# Impact on Economy

People today are highly dependent on computers and the internet for money transfers and making payments. Therefore, the risk of being subjected to online money frauds is extremely high. Norton CyberCrime disclosed in 2011 that over 74 million people in the United States were victims of cybercrime in 2010, which directly resulted in financial losses of approximately $32 billion. Even in India, with the emergence and popularity of “cashless India”, chances of being duped online are also increasing, if one is not smart enough to use safe online transaction platforms and apps.

Not just individuals suffer from financial losses due to cybercrimes; some of the surveys conducted have stated that approximately 80% of the companies participating in the surveys accepted financial losses due to cybercrimes.

## Leakage of Personal Information

Not just financial losses, people also suffer from leakage of their personal information. Many social networking sites, no matter how safe, are still an open platform for everyone to see someone else’s life, which can be dangerous. Apart from this, hackers can also hack into one’s account and collect whatever information they want to. Spamming and phishing also cause harm to people.

## Loss of Consumer Trust

With such financial losses and a threat to personal information, consumers start losing trust in such sites and apps. Even if the person committing the crime is someone else, the site or app is declared to be fraudulent and unsafe. Also, it makes people reluctant to start a transaction when their credit card information is asked. This affects the credibility of an e-business and consequently jeopardizes a potential business.

## The threat to National Security

Nowadays, the military of most of the countries is using advanced computer technologies and networks. Information warfare, albeit old, is used to spread malware, which can cause network crashes and spread misinformation. Not just militaries but terrorists and cybercriminals also these technologies to intrude in other Country’s security networks and obtain information. They also send threats and warnings through computer systems.

**Cyber Law in India and the IT Act, 2000**

In India, cyber laws are contained in the Information Technology Act, 2000. The main object of this Act is to provide legal recognition to e-commerce and electronic formats and to facilitate the filing of electronic records with the Government. This legislation lays down rules and regulations related to cybercrimes, electronic information and formats, electronic authentication and digital signatures, and liability of network service providers. The I.T. Act is based on the [United Nations Model Law on Electronic Commerce 1996 (UNCITRAL Model)](https://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf" \t "https://blog.ipleaders.in/introduction-to-cyber-crime-and-cyber-law/_blank) recommended by the General Assembly of the United Nations by a resolution dated 30 January 1997.

The Indian Cyber Law covers these major aspects of Cyberspace and cybercrime:

1. The Indian Cyber Law makes every format in electronic form legal, which means anything that you write, share and publish electronically is now considered legal.
2. It also makes all electronic contracts legal, which means that an offer can be electronically made and accepted, and it would amount to a valid and binding electronic contract.
3. The Indian Cyber Law recognizes and legalizes the concept of digital signatures and electronic authentications.
4. Indian Cyber Law covers almost all kinds of cybercrimes and provides punishment for the same.
5. It also punishes the people of other nationalities, provided their crimes involve any computer or network situated in India.

## **What is Hacking?**

Hacking is the activity of identifying weaknesses in a computer system or a network to exploit the security to gain access to personal data or business data. An example of computer hacking can be: using a password cracking algorithm to gain access to a computer system.

Computers have become mandatory to run a successful businesses. It is not enough to have isolated computers systems; they need to be networked to facilitate communication with external businesses. This exposes them to the outside world and hacking. System hacking means using computers to commit fraudulent acts such as fraud, privacy invasion, stealing corporate/personal data, etc. Cyber crimes cost many organizations millions of dollars every year. Businesses need to protect themselves against such attacks.