



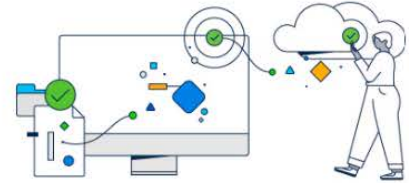
**CISCO Live !** Join us in San Diego for the tech event of the year.  
Event | June 8 -12, 2025 [Register now >](#)

## Cybersecurity

# What is cybersecurity?

The rise in digital cyberattacks has made cybersecurity a priority for businesses and individuals. For businesses, cybercrimes can lead to financial loss, operational disruption, data breaches, and a loss of trust, while individuals face identity theft, financial fraud, and privacy invasion.

[Read Cyber Threat Trends Report](#)



### What is cybersecurity all about?

Why is cybersecurity important?

Types of cybersecurity threats

Best practices for cybersecurity

## What is cybersecurity all about?

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These [cyberattacks](#) are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users through [ransomware](#); or interrupting normal business processes.

Implementing effective cybersecurity measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative.

A successful cybersecurity posture has multiple layers of protection spread across the computers, networks, programs, or data that one intends to keep safe. In an organization, a unified threat management gateway system can automate integrations across products and accelerate key security operations functions: detection, investigation, and remediation. People, processes, and technology must all complement one another to create an effective defense from cyberattacks.

[Take our free Introduction to Cybersecurity course](#)

### People

Users must understand and comply with basic data protection and privacy security principles like choosing strong passwords, being wary of attachments in email, and backing up data. Learn more about basic cybersecurity principles from these [Top 10 Cyber Tips \(PDF\)](#).

### Processes

Organizations must have a framework for how they deal with both attempted and successful cyberattacks. One well-respected model, the [NIST cybersecurity framework](#), can guide you. It explains how you can identify attacks, protect systems, detect and respond to threats, and recover from successful attacks.

### Technology

Technology is essential to giving organizations and individuals the computer security tools needed to protect themselves from cyberattacks. Three main entities must be protected: endpoint devices like computers, smart devices, and routers; networks; and the cloud. Common technology used to protect these entities include [next-generation firewalls](#), [Domain Name System \(DNS\)](#)

[filtering](#), [malware protection](#), antivirus software, and [email security solutions](#).

---

## Why is cybersecurity important?

In today's connected world, everyone benefits from advanced [cybersecurity solutions](#). At an individual level, a cybersecurity attack can result in everything from identity theft to extortion attempts, to the loss of important data like family photos. Everyone relies on critical infrastructure like power plants, hospitals, and financial service companies. Securing these and other organizations is essential to keeping our society functioning.

Everyone also benefits from the work of cyberthreat researchers, like the team of 250 threat researchers at Talos, who investigate new and emerging threats and cyberattack strategies. They reveal new vulnerabilities, educate the public on the importance of cybersecurity, and strengthen open-source tools. Their work makes the internet safer for everyone.



Cisco Security: A better way of doing security

[Watch now \(01:24\)](#)

---

## Types of cybersecurity threats

### Cloud security

[Cloud security](#) provides rapid threat detection and remediation, enhancing visibility and intelligence to prevent malware impacts. It delivers robust protection in multicloud environments, streamlining security without affecting user productivity, and is essential for the safety of applications, data, and users in both hybrid and remote work settings. The scalable nature of cloud security allows for the defense of an expanding array of users, devices, and cloud applications, ensuring comprehensive coverage across all points of potential attack.

[Cisco Cloud Protection Suite](#) | [Cisco Multicloud Defense](#)

### Identity

[Identity security](#) and [access management](#) involve safeguarding the digital identities of individuals, devices, and organizations. This involves implementing security processes, tools, and policies that control user access to accounts and enable productivity with frictionless access to important information without risk.

The three main goals of identity security are to:

1. Authenticate a user's identity
2. Authorize access to appropriate resources
3. Monitor access activity for weak posture and suspicious activity

[Discover more about Cisco Identity Intelligence](#) | [Discover more about Continuous Identity Security](#)

## Malware

[Malware](#) is a type of software designed to gain unauthorized access or to cause damage to a computer.

[Discover more about malware protection](#) | [Secure Endpoint](#) | [Secure Endpoint free trial](#)

## Phishing

[Phishing](#) is the practice of sending fraudulent emails that resemble emails from reputable sources. The aim is to steal sensitive data, such as credit card numbers and login information, and is the most common type of cyberattack. You can help protect yourself through education or a technology solution that filters malicious emails.

[Secure Email solution](#) | [Secure Email free trial](#)

## Ransomware

[Ransomware](#) is a type of malicious software that is designed to extort money by blocking access to files or the computer system until the ransom is paid. Paying the ransom does not guarantee that the files will be recovered or the system restored.

[Stop ransomware in its tracks](#)

## Social engineering

[Social engineering](#) is a tactic that adversaries use to trick you into revealing sensitive information. Attackers can solicit a monetary payment or gain access to your confidential data. Social engineering can be combined with any of the threats mentioned above to make you more likely to click on links, download malware, or trust a malicious source.

[Read more about social engineering tactics](#)

## Threat detection

An effective extended detection and response (XDR) system integrates solutions across the security stack, making it easier for analysts to focus on comprehensive threat detection, prioritize incident response, and improve productivity. With more visibility and context into data security threats, events that would not have been addressed before will surface to a higher level of awareness, thus allowing cybersecurity teams to quickly eliminate any further impact and reduce the severity and scope of the attack.

[Read more about XDR](#) | [Cisco XDR](#)

## Zero trust

[Zero trust](#) isn't a single product or technology. It's a security strategy that is best implemented by keeping an organization's business operations, risks, and security outcomes in mind. Although there are various paths to achieving zero trust maturity, most organizations prioritize deployment of technologies such as multi-factor authentication (MFA), [device posture checks](#), [zero trust network access \(ZTNA\)](#), and network segmentation as they implement zero-trust security.

[Read more about zero-trust networking](#) | [Cisco Duo](#) | [Cisco Secure Access](#)

---

## Best practices for cybersecurity

Adopting best practices for cybersecurity can significantly reduce the risk of cyberattacks.

Here are three key practices:

**1. Regular software and operating system updates**

Updating software and operating systems regularly helps to patch vulnerabilities and enhance security measures against potential threats.

**2. Using strong and unique passwords**

Creating strong and unique passwords for each online account can enhance cybersecurity, as cyberattacks often exploit weak or stolen passwords.

**3. Implementing multi-factor authentication (MFA)**

Multi-factor authentication involves multiple identification forms before account access, reducing the risk of unauthorized access. [Cisco Duo includes MFA](#) that can integrate with most major applications as well as custom apps.

Following these practices enhances cybersecurity and protects digital assets. It's vital to stay vigilant and informed about the latest threats and security measures to stay ahead of cybercriminals.

## Related security topics

### What is XDR?

Extended detection and response (XDR) delivers visibility to remediate security threats.

[Learn about XDR](#) >

### What is a firewall?

A firewall decides whether to allow or block specific traffic based on security rules.

[Learn about firewalls](#) >

### What is network security?

Network security is a suite of security technologies that protect a network and data.

[Learn about network security](#) >

### What is endpoint security?

Endpoint security solutions defend endpoints like mobile devices, computers, and IoT devices.

[Learn about endpoint security](#) >

### What is DNSSEC?

A Domain Name System Security Extension (DNSSEC) can help to verify and protect against DNS attacks.

[Learn about DNSSEC](#) >

### What is cyber resilience?

Cyber resilience is a strategy for stopping breaches, mitigating risk, and improving recovery time.

[Learn about cyber resilience](#) >

## Reduce complexity to improve protection

See how Cisco can revolutionize your security strategy.

[Read e-book](#)

[About Cisco](#) [Contact Us](#) [Careers](#) [Connect with a partner](#)



[Feedback](#) [Help](#) [Terms & Conditions](#) [Privacy](#) [Cookies / Do not sell or share my personal data](#) [Accessibility](#) [Trademarks](#) [Supply Chain Transparency](#)  
[Newsroom](#) [Sitemap](#)

©2025 Cisco Systems, Inc.

