

# TOP TEN CYBERSECURITY THREATS AND PREVENTION TIPS

Cybersecurity threats are becoming more sophisticated and dangerous in today's digital age. To protect yourself and your organization, you must be aware of the most common threats and know how to prevent them. Here are the top 10 cybersecurity threats and prevention tips you should be aware of:

## Phishing

Phishing is a fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details.

### HOW TO PREVENT

You should verify the sender's identity, check for suspicious links or attachments, and never give out personal information unless you are certain of the recipient's legitimacy.

## Social Engineering

These attacks involve criminals exploiting human psychology rather than technical vulnerabilities to trick people into providing them with sensitive information or access to data, networks and systems.

### HOW TO PREVENT

Be wary of unsolicited phone calls or emails, avoid clicking on unknown links, and be cautious of offers that seem too good to be true.

## Malware

Short for malicious software, this is a type of computer program designed to cause damage to a computer system, network, or device.

### HOW TO PREVENT

Install anti-malware software, update your operating system and software regularly, and avoid downloading files from untrusted sources.

## Ransomware

This type of malware encrypts files on a computer then demands payment to release them. It can be particularly devastating to organizations that rely on data to operate.

### HOW TO PREVENT

Back up your data regularly, install anti-malware software, and avoid downloading files from unknown sources.

## Zero-Day Vulnerabilities

Zero-day vulnerabilities are undetected weaknesses in a computing system that can be exploited by attackers.

### HOW TO PREVENT

Keep software up-to-date with the latest patches and use heuristic intrusion prevention systems with threat intelligence.

## Denial of Service (DoS)

Denial of Service, or DoS, is a type of cyber threat designed to disrupt the systems, website, or network of an organization with requests.

### HOW TO PREVENT

Implement network security controls and roll out DDoS mitigation services.

## Insider Threats

These are threats that come from within an organization. Employees or contractors with authorized access to the organization's systems and data can intentionally or unintentionally cause harm.

### HOW TO PREVENT

Organizations should limit who has access to sensitive systems and data. They can also use technology to help detect and stop any bad actions, like DLP systems. Finally, it's important to be prepared for an attack and know what to do if one happens.

## Supply Chain Attack

Supply chain attacks occur when an attacker targets a third-party supplier or vendor to access a target's system. This can take various forms, such as malware infections, data breaches, phishing, and man-in-the-middle attacks.

### HOW TO PREVENT

Conduct due diligence on vendors, implement a security system, monitor vendor activities, set security standards, educate employees, and have an incident response plan.

## Distributed Denial of Service (DDoS)

Distributed Denial of Service (DDoS) attacks involve overwhelming a website or network with traffic to disrupt access.

### HOW TO PREVENT

Use a DDoS protection service, limit access to your network, and use firewalls and intrusion detection systems.

## System Intrusion

System Intrusion is unauthorized access to a computer system or network, leading to data theft, system damage, or leaving a backdoor for future attacks.

### HOW TO PREVENT

Implement strong access controls, keep software and systems up-to-date, use network segmentation, monitor network and system logs, and train employees on cybersecurity best practices.

## Honorable Mention: Man in the Middle (MitM)

Man in the Middle (MitM) is a cyber threat where an attacker intercepts communication between two parties to eavesdrop on or manipulate the information being exchanged.

### HOW TO PREVENT

Users should use encryption, verify digital certificates, be cautious when using public Wi-Fi, phishing attacks, and use VPNs to protect data.

## PREPARE WITH TRAVA

Being aware of these common cybersecurity threats and prevention tips can help you protect yourself and your organization from potential threats. By implementing these best practices and staying up-to-date with the latest threats, you can help ensure that your digital life remains safe and secure.

Trava simplifies your most important decisions so you can earn more trust and close more business—faster. More details on the full blog post: [www.travasecurity.com/blog/top-10-cyber-security-threats-and-how-to-prevent-them](https://www.travasecurity.com/blog/top-10-cyber-security-threats-and-how-to-prevent-them)

talk to trava