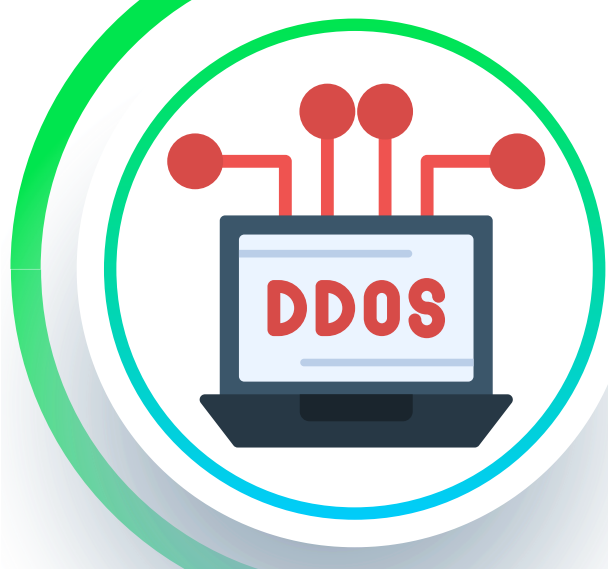
Top 4 Most Common Types of Cybersecurity Attacks

1. DOS AND DDOS

A denial-of-service (DoS) attack is **designed to overwhelm the resources of a system to the point where it is unable to reply to legitimate service requests**. A distributed denial-of-service (DDoS) attack is similar in that it also seeks to drain the resources of a system.

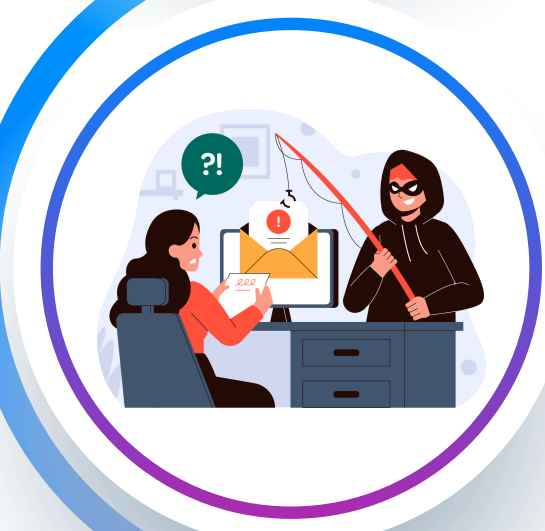


2. MITM

Man-in-the-middle (MITM) types of cyber attacks refer to **breaches in cybersecurity that make it possible for an attacker to eavesdrop on the data sent back and forth between two people, networks, or computers**. It is called a "man in the middle" attack because the attacker positions themselves in the "middle" or between the two parties trying to communicate.

3. PHISHING

A phishing attack occurs when a malicious actor sends emails that seem to be coming from trusted, legitimate sources in an attempt to grab sensitive information from the target. Phishing attacks combine social engineering and technology and are so-called because the attacker is, in effect**, "fishing" for access to a forbidden area by using the "bait" of a seemingly trustworthy sender.**



4. WHALE-PHISHING

A whale-phishing attack is so-named because **it goes after the "big fish" or whales of an organization, which typically include those in the C-suite or others in charge of the organization**. These individuals are likely to possess information that can be valuable to attackers, such as proprietary information about the business or its operations.

Learn more

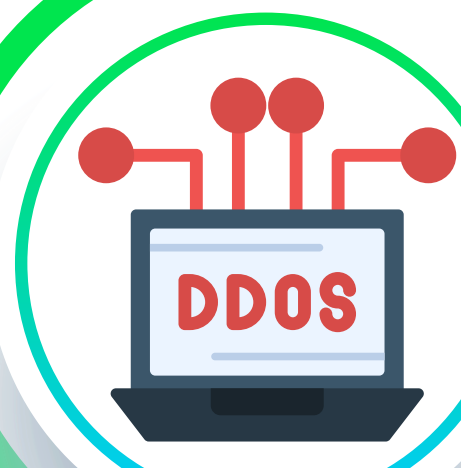
SYNERGIE CONSULTATION

CREATE BY :
SYNERGIECONSULTATION.COM

Les 4 types d'attaques de cybersécurité les plus courantes

1. DOS AND DDOS

Une attaque par déni de service (DoS) est **conçue pour submerger les ressources d'un système au point qu'il soit incapable de répondre aux demandes de service légitimes.** Une attaque par déni de service distribué (DDoS) est similaire dans la mesure où elle cherche également à drainer les ressources d'un système.

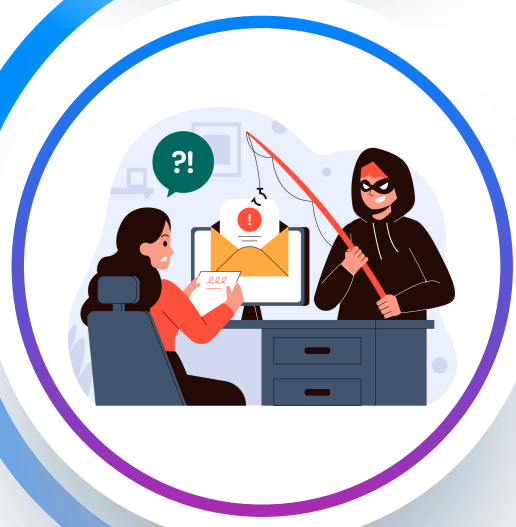


2. MITM

Les attaques de type « Man in the middle » (MITM) désignent des **failles de cybersécurité qui permettent à un attaquant d'intercepter les données échangées entre deux personnes, deux réseaux ou deux ordinateurs.** On parle alors d' attaque de type « man in the middle » car l'attaquant se positionne au « milieu » ou entre les deux parties qui tentent de communiquer

3. PHISHING

Une attaque de phishing se produit lorsqu'un acteur malveillant envoie des e-mails qui semblent provenir de sources fiables et légitimes dans le but de récupérer des informations sensibles de la cible. Les attaques de phishing combinent l'ingénierie sociale et la technologie et sont appelées ainsi parce que l'attaquant **« pêche » en fait l'accès à une zone interdite en utilisant l'« appât » d'un expéditeur apparemment digne de confiance.**



4. WHALE-PHISHING

Une attaque de phishing par baleine est ainsi nommée car elle cible les **« gros poissons » ou baleines d'une organisation, qui incluent généralement les cadres supérieurs ou les autres responsables de l'organisation.** Ces individus sont susceptibles de détenir des informations qui peuvent être précieuses pour les attaquants, telles que des informations confidentielles sur l'entreprise ou ses opérations.

En apprendre plus

SYNERGIE CONSULTATION

CREATE BY :
SYNERGIECONSULTATION.COM