Cyber Security

2024

Common Cyber Attacks

Vathna.lay@cadt.edu.kh

Objectives

After finishing this lesson, you will be able to:

- **Understanding Threats:** You will understand the key tactics used in widespread cyberattacks
- **Categorization:** You can differentiate between attacks focused on disruption vs. those focused on impersonation and data theft.
- **Real-World Connection:** You will recognize examples of how these attacks appear in news stories and everyday life

Attacks That Inflict Damage

- Some cyberattacks are designed to cause damage, not directly steal data.
- These attacks aim to disrupt services, destroy data, or cause physical harm.
- Attack types include
  - DoS (Denial-of-Service),
  - DDoS (Distributed Denial-of-Service),
  - botnets
  - data destruction attacks.

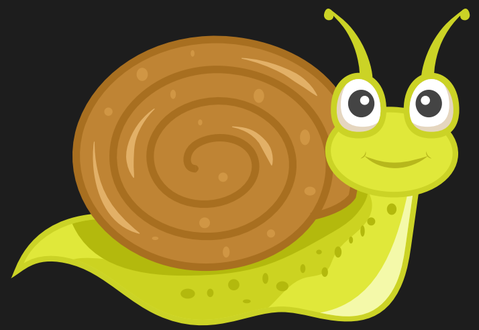
Denial-of-Service (DoS)

DoS attacks overwhelm a system with requests, using normal or specially crafted ones to exhaust processing power, memory, or network resources.

DDoS Attack

A more powerful DoS: DDoS attacks are like DoS attacks on steroids, using a massive network of infected devices to overwhelm a target with traffic.

How DDoS Attacks Impact Individuals



Slow Internet

Website Outages

Forced Misinformation

Question

Which of the following best describes the key difference between a DoS and a DDoS attack?

- A. DoS attacks target websites, while DDoS attacks target email servers.
- B. DoS attacks use a single attacker machine, while DDoS attacks use multiple infected devices.
- C. DoS attacks are more difficult to defend against than DDoS attacks.
- D. DDoS attacks are recent, while DoS attacks have been around for decades.

Question

You receive a suspicious email alert claiming unusual activity on your bank account. It urges you to click a link to verify your information. What would the attacker's likely goal be if this were part of a DoS/DDoS strategy?

A. To steal your banking login details.

B. To spread malware that could turn your computer into a bot.

C. To distract you while they launch a large DDoS attack against your bank.

D. To trick you into giving up your social security number.

Question

Which of the following situations is an example of a DoS attack rather than a DDoS attack?

A. A disgruntled employee overloads the company server by running a resource-intensive program.

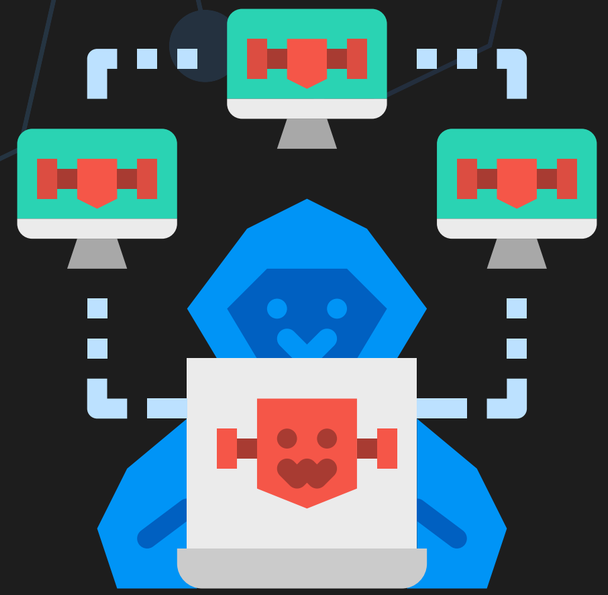
B. Hacktivists launch an attack on a government website using a network of infected devices.

C. A hacker targets a company with a flood of fake traffic, causing its website to crash.

D. A competitor pays a criminal service to take down a rival's online store.

Botnets and Zombies

- **Botnet:** Network of infected computers
- **Zombie:** Individual computer under attacker control
- **DDoS:** Often launched using botnets



Data Destruction Attack

- **Goal:** Not just disruption, but the permanent destruction or corruption of a victim's data.
- **Motivations:** Ransomware attacks (refusal to pay), financial gain, political or military sabotage.
- **Wiper Attacks:** A specific type of data destruction attack that uses malware to make data recovery extremely difficult.

Question

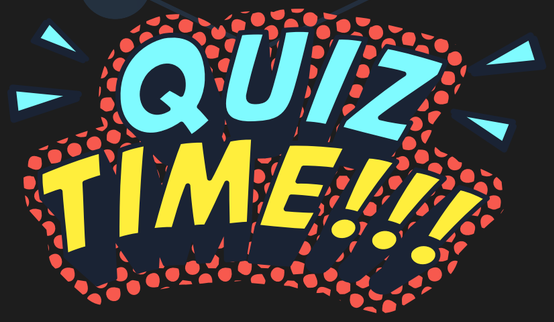
What's the relationship between a "zombie" and a "botnet"?

A. A zombie is a type of malware that creates botnets.

B. A zombie is an individual computer within a botnet.

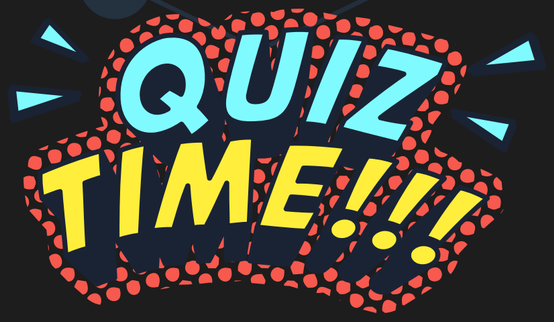
C. A botnet is a smaller version of a zombie.

D. Zombies and botnets are unrelated terms.



Class Activity

A hacker sends malicious emails designed to trick users into downloading malware. If successful, this could help the hacker with which goal?



A. Building a botnet to launch DDoS attacks

B. Impersonating a CEO to trick employees

C. Deleting critical files on infected machines

D. Redirecting users to fake websites for phishing.

Question

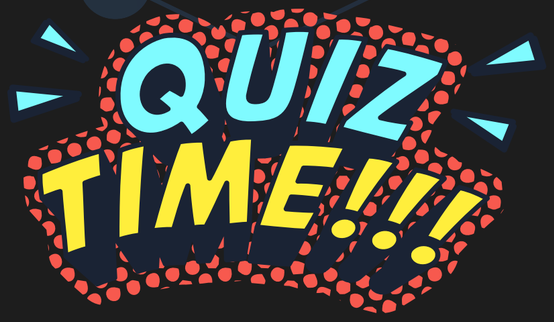
Which type of attack is primarily focused on causing permanent damage to stored data?

A. Denial-of-Service (DoS)

B. Phishing Attack

C. Data Destruction Attack

D. CEO Fraud



Question

Protecting personal data means ensuring:

A. Data and software on the infected device may be lost if no backups exist.

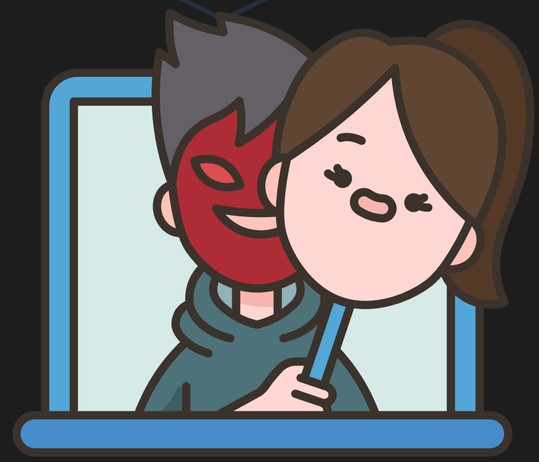
B. The victim might receive fake emails pretending to be from their boss.

C. The victim's website could become temporarily unavailable.

D. The victim could be tricked into installing malware on a network.

Impersonation Attacks

- **The Internet's Risk:** Impersonation of trusted sources has become easier and more convincing online.
- **Key Tactics**:
  - **Fake websites** that closely mimic legitimate ones.
  - **Emails designed** to appear as if they're from reputable people or organizations.



Phishing

- **Core Concept:** Phishing involves impersonating a trusted source (bank, company, etc.) to trick victims.
- **Tactics:**
  - Emails with urgent requests to click links
  - Fake websites designed to look like the real thing
- **Goal:** Steal login credentials, personal data, or spread malware
- **Serious Problem:** Phishing attacks are widespread and impact many businesses each year.

Question

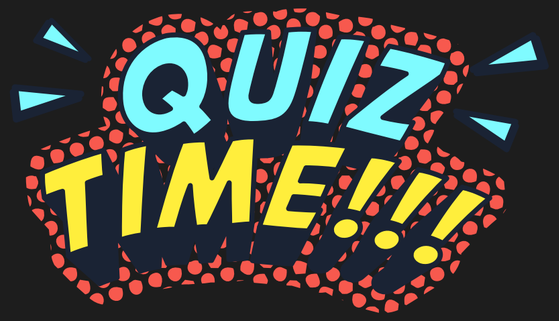
Why are impersonation attacks more prevalent in the internet age compared to earlier times?

A. The internet makes it easier to create convincing fakes and reach many targets quickly.

B. Criminals now are simply smarter than they used to be.

C. Laws against impersonation didn't exist before the internet.

D. Impersonation attacks also happened frequently before the internet.



Questions

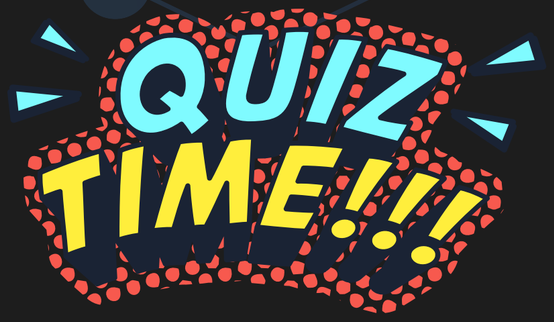
You receive an email claiming your bank account has unusual activity. The email's sender looks official, and it urges you to click a link to verify your information. This could be an example of:

A. A DoS attack

B. A data destruction attack

C. An impersonation attack

D. A wiper attack



Questions

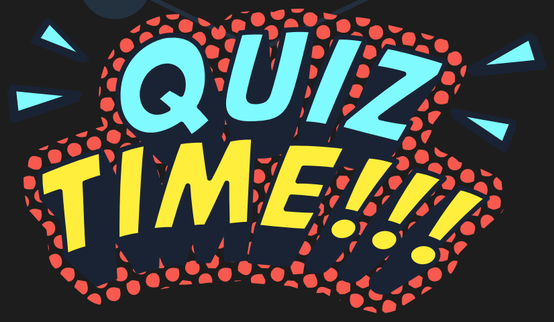
Which of the following best describes the goal of a phishing attack?

A. To trick users into giving up sensitive information

B. To shut down a website by overwhelming it with traffic

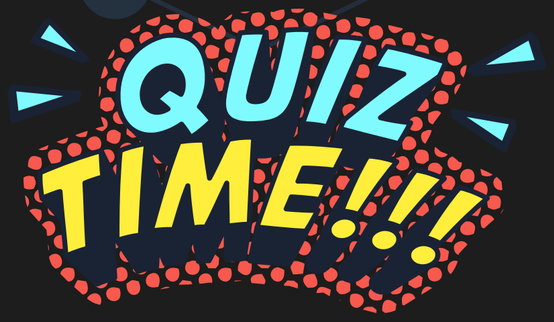
C. To permanently erase data on infected computers

D. To prevent users from accessing their email



Questions

You receive an email claiming to be from your email provider. It warns that your account will be deleted unless you click a link to verify. This is LIKELY an example of:



A. A phishing attack

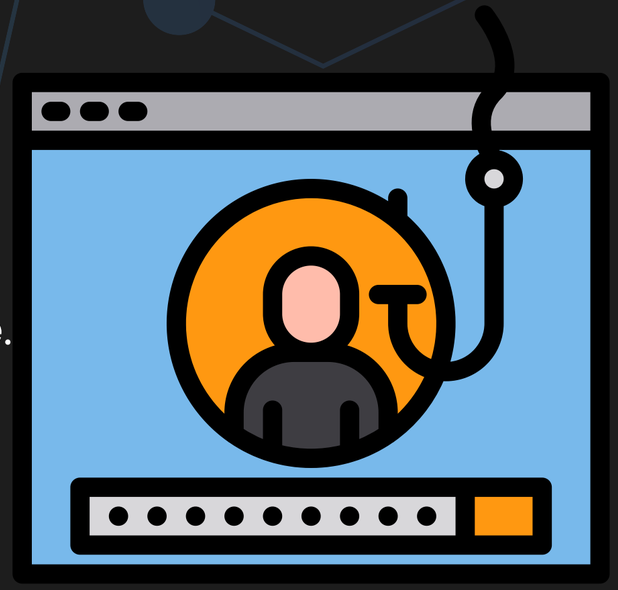
B. A DDoS attack

C. A wiper attack

D. CEO Fraud

Spear Phising

- **What is it?** A highly targeted form of phishing, customized to a specific person or organization.
- **Increased danger:** Attackers use research (often gathered from social media) to make emails more convincing.
- **Goal:** Same as regular phishing – steal credentials, data, or install malware. But, success rate is often higher due to personalization.



CEO Fraud

- **Type of Impersonation:** Attackers pretend to be a company's CEO or high-level executive.
- **The Trick:** Urgent emails requesting actions like wire transfers, sending sensitive data.
- **High Stakes:** Victims can lose large sums of money and potentially their jobs.
- **Pandemic Impact**: Working from home increased vulnerability due to less in-person verification.

Smashing

- **Definition:** Phishing attacks carried out through text messages (SMS).
- **Goal:** Same as phishing: steal logins, install malware, or trick victims into giving up personal data.
- **Danger:** People may be more likely to trust text messages than emails, increasing the risk.

Vishing

- **Definition:** Phishing attacks conducted over the phone (voice calls).
- **Technology:** Uses Voice over IP (VoIP) systems today, but the core method remains calling people.
- **Tactics:** Similar to phishing emails, with urgency and impersonation to trick victims into revealing data or taking unwanted actions.

Pharming

- **Technical attack:** Targets network infrastructure (such as DNS servers) to redirect users to fake websites.
- **Looks like phishing:** Victims see the correct website address but land on the attacker's site anyway.
- **Tricks everyone**: Even cautious users can fall for it since the attack doesn't rely on clicking suspicious links.

Whaling: Going for big Fish

- **Type of Spear Phishing:** Highly targeted attacks aimed at CEOs, high-level executives, or influential individuals.
- **Why "Whaling"?:** Focus on the big targets.
- **Goal:** Steal sensitive company data, authorize fraudulent payments, or access critical systems.

Questions

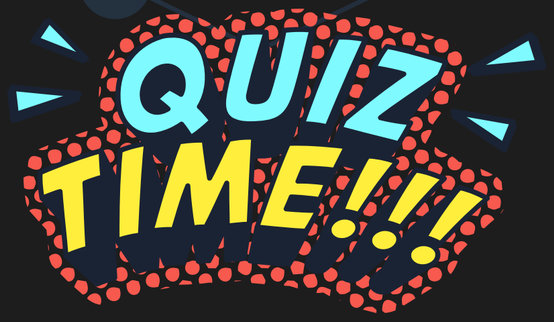
What makes spear phishing more dangerous than general phishing attacks?

A. Spear phishing uses more technical tricks to infect devices.

B. Spear phishing emails are personalized to seem more believable.

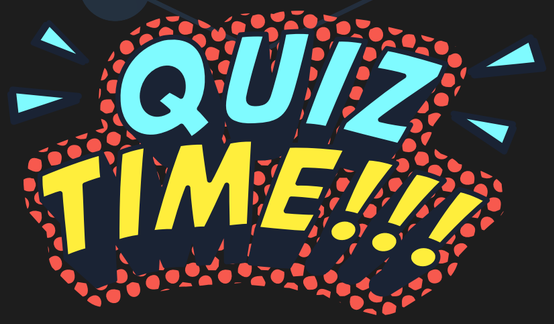
C. Spear phishing targets only large companies, not individuals.

D. Spear phishing can cause data destruction, not just theft



Questions

You receive an email seemingly from your company's HR department, asking you to confirm your salary information by clicking a link. This could be an example of:



A. Spear phishing

B. A wiper attack.

C. Smishing

D. A DoS attack

Questions

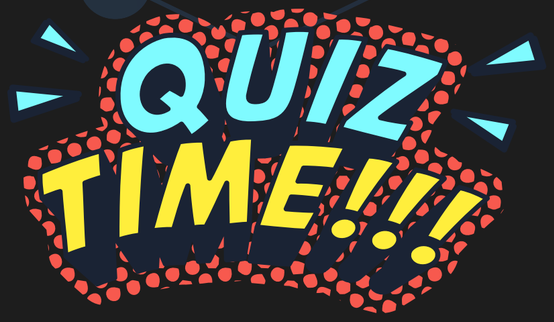
A key difference between CEO fraud and regular phishing is that CEO fraud often:

A. Targets individuals rather than large organizations.

B. Seeks to obtain login credentials.

C. Requests immediate actions with financial consequences.

D. Uses fake websites to collect information.



Questions

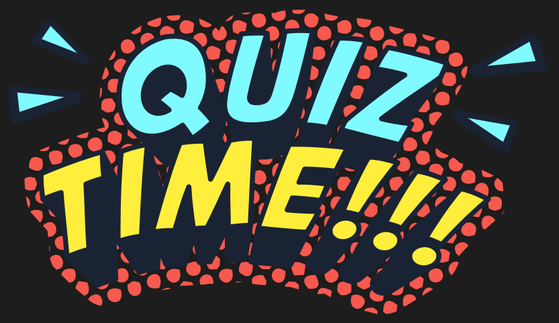
The CEO of your company emails you, asking you to urgently send confidential tax documents to an unfamiliar email address. You should:

A. Follow the instructions immediately.

B. Verify the request through other channels (phone call, in-person).

C. Report the email as a phishing attempt.

D. Ignore the email.



Questions

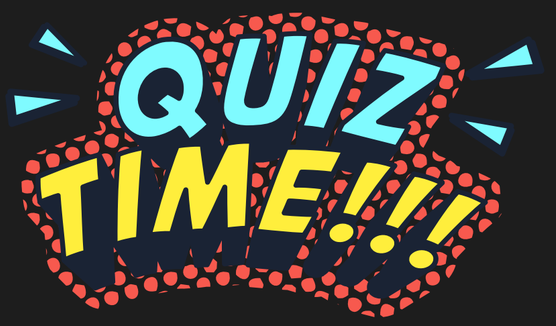
What does the term "smishing" refer to?

A. Phishing attacks through text messages

B. Spam messages promoting fake products

C. Malware that crashes your phone's operating system

D. An attack that blocks text messages from reaching you



Questions

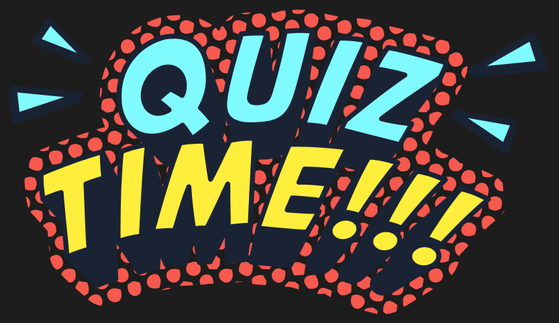
You receive a text message stating your bank account has been locked, with a link to "verify" your information. This is MOST LIKELY:

A. A smishing attempt

B. A legitimate alert from your bank

C. A wiper attack in disguise

D. A harmless prank from a friend



Questions

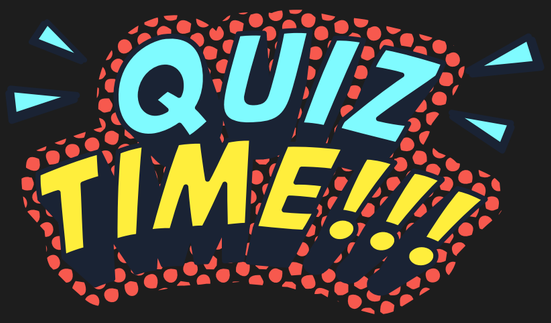
Vishing is similar to phishing, but what's the key difference in how they're carried out?

A. Vishing attacks steal data directly from your phone, while phishing uses emails

B. Phishing uses fake websites, while vishing uses social engineering over the phone.

C. Vishing targets businesses, while phishing targets individuals.

D. Phishing is a recent attack method, while vishing has been around for decades.



Questions

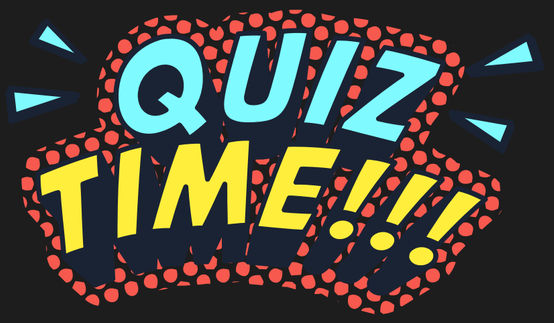
You receive a call from someone claiming to be from your internet service provider, stating your service will be disconnected unless you verify your account information. This could be an example of:

A. A DoS attack

B. Vishing

C. A data destruction attack

D. Smishing.



Questions

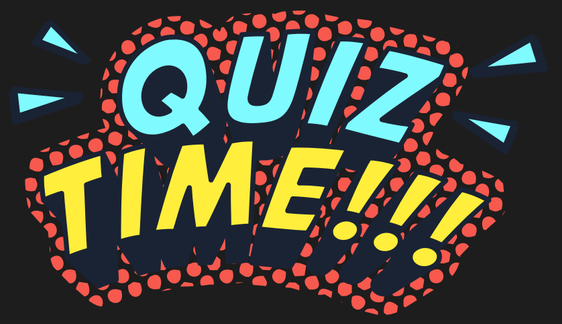
The main difference between pharming and regular phishing is:

A. Pharming steals data, phishing leads to malware.

B. Pharming attacks are easy to spot, phishing is more convincing.

C. Pharming involves technical manipulation of internet traffic, phishing relies on tricking the user.

D. Pharming focuses on businesses, phishing targets individuals.



Questions

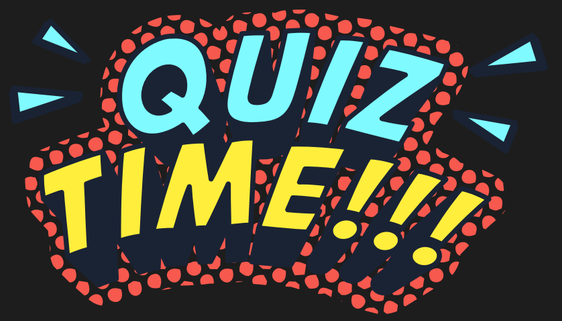
You carefully type your bank's website address into your browser, but end up on a site asking for your login details. This could be a sign of:

A. A pharming attack

B. Spear phishing

C. A DDoS attack

D. A wiper attack



Questions

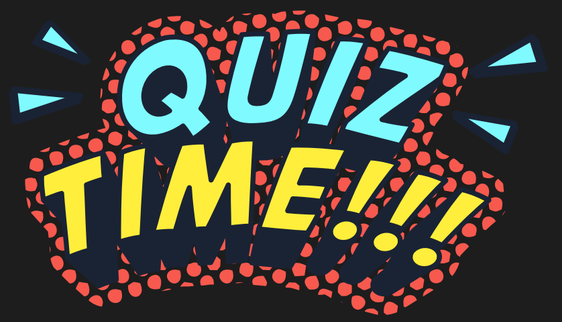
What makes a whaling attack different from other forms of phishing?

A. Whaling uses advanced malware that regular phishing doesn't.

B. Whaling targets high-profile individuals within organizations.

C. Whaling attacks occur exclusively via text message.

D. Whaling is a harmless form of internet prank.



Questions

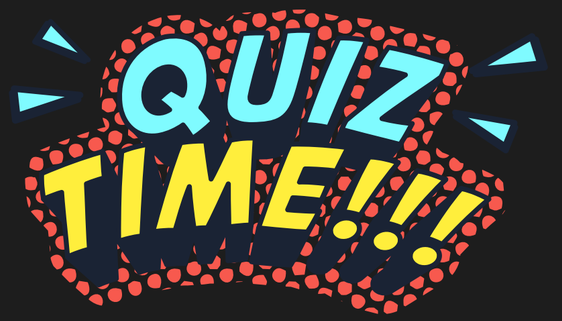
An attacker carefully studies a company's website and social media to craft a believable email to the company's CFO. This is MOST LIKELY the start of a:

A. DDoS attack

B. CEO fraud attempt.

C. Whaling attack

D. Data destruction attack




?
Q&A