

Digital Trust and Cybersecurity Threats

Textbook

Digital Trust and Cybersecurity Threats



In our digital world, knowing about online interactions is key. This chapter covers tricky social engineering tactics and the ins and outs of digital money. We'll look at how trust is misused and tell the difference between various digital assets, pointing out risks like those without a "proof of work." This will help you use the internet more safely.

Tracing the Social Engineering Attack Cycle

Social engineering uses mind games, not tech tricks, to get access.

It usually starts with **gathering information**. Attackers secretly collect public and private details about people, often from social media or company websites, to build a full picture.

Next comes **building a relationship**, or "pretexting." Attackers gain trust by pretending to be someone else, like a coworker or IT helper. They use the information they gathered to make up believable stories—like an urgent tech problem needing login details.

Finally, in the **exploitation** stage, the attacker uses this trust and info to get the victim to do what they want. This could mean clicking a bad link, giving away passwords, or sending money, often by creating a sense of urgency or offering fake rewards.

These attacks have a big impact. Computer systems can get hacked, infected with malware, and shut down, costing lots of money. People can lose money, have their identity stolen, feel embarrassed, and be upset. Companies lose customer trust and face legal problems. The economy suffers from business shutdowns and stolen ideas. This also makes people less trusting of online communication, meaning we all need to be careful and learn more to fight these changing threats.

Telling the Difference Between Digital Currency and a Security

To understand digital assets, you need to know the difference between digital money and a security. A **digital currency**, like Bitcoin, is mainly used for buying and selling things, storing value, and counting money. It's built on a technology called blockchain, and its value comes from how many people want it or how useful it is, not from owning part of a company. If you own Bitcoin, you own a piece of digital money, not a share in a business.

A **security**, or "security token," is like owning a piece of a company, similar to stocks or bonds. These digital assets follow government rules for investments and can give you rights like voting or a share of the company's profits. Its value is directly tied to how well the company it represents is doing. The main difference is simple: one is for transactions, the other is an investment that shows ownership.

Understanding the Risks of Digital Currencies

While digital money offers cool new ways to do things, it comes with unique risks you need to know. One big risk is how much its value can **change quickly**. Prices can go up and down very fast because of trading, news, and world events, which can lead to big money losses. Unlike regular money backed by governments, digital currencies don't have the same things to keep their value steady.

Security problems are also a worry. Even though blockchain tech is generally safe, the places where you keep and trade digital money can be hacked. People can lose their digital money to scams, viruses, or ransomware that steals their digital wallets or secret keys. Since there's no central boss for digital money, it's often hard to get your money back if it's stolen, and transactions can't usually be undone.

Unclear rules are another risk. Governments around the world are still figuring out what to do with digital money, which can cause sudden changes in rules that affect its value or legality. Also, without clear rules, digital money can be used for illegal activities, which might lead to stricter government action.

A very important risk, especially for smaller digital currencies, is not having **proof of work (POW)** or another strong security system. POW, used by Bitcoin, makes the network safe by requiring a lot of computer power to confirm transactions, making it hard to mess with. Without POW, it's easier and cheaper for bad actors to take control of the network (a "51% attack"), letting them fake transactions or spend money twice. These currencies are much easier to manipulate and might not be safe for your money or transactions.

Digital Money is Complex

Finally, digital money can be **complex, and people can make mistakes**. It involves complicated ideas like private keys and addresses, which can be confusing. A simple mistake, like sending money to the wrong address, can mean losing it forever because transactions can't be reversed. You are fully responsible for keeping your private keys safe, and if you lose them, you lose access to your digital money. All these risks mean you need to do your homework, invest carefully, and use strong security when dealing with digital currencies.

Critical Thinking Questions

1. Imagine you get an email from your school's IT department telling you to "verify your login details right away to avoid your account being shut down." Thinking about the social engineering attack cycle, what steps would you take to figure out if this email is real or a scam, and why are those steps important?
2. A new digital asset is being launched. It says it's a "digital currency" but also promises investors a share of the profits from an app it runs. Based on what you've learned about the differences, how would you classify this asset (currency, security, or something else)? What does your classification mean for people thinking about investing in it?
3. Think about the ethical duties of people who create new digital currencies, especially those without a strong security system like Proof of Work. What actions should they take, if any, to protect users from risks? What part do users play in checking how safe these currencies are?

Questions (5)

1. You receive an urgent email from someone claiming to be from your bank, asking you to click a link to "verify your account immediately" or it will be shut down. Thinking about the social engineering attack cycle, what stage is this email primarily designed

MULTIPLE CHOICE

Choose the correct answer:

- A. Information Gathering
- B. Pretexting (Building a Relationship)
- C. Exploitation
- D. Recovery

2. Before sending a deceptive email, an attacker spends weeks researching their target's public social media profiles and company website to learn about their interests and colleagues. What stage of the social engineering attack cycle does this describe?

MULTIPLE CHOICE

Choose the correct answer:

- A. Exploitation
- B. Building a Relationship (Pretexting)
- C. Information Gathering
- D. Recovery

3. A digital asset's value primarily comes from how many people want it and its use in transactions, and it's built on blockchain. It does not represent ownership in a company. Based on the passage, how would you classify this asset?

MULTIPLE CHOICE

Choose the correct answer:

- A. A security
- B. A digital currency
- C. A stock
- D. A bond

4. A new digital asset is being launched. It calls itself a "digital currency" but also promises investors rights like voting in company decisions and a share of the app's profits. Based on the distinctions in the passage, how would you classify this asset?

MULTIPLE CHOICE

Choose the correct answer:

- A. A pure digital currency
- B. A type of security (security token)
- C. A hybrid that doesn't fit either category
- D. A scam, regardless of its features

5. An employee receives an email that seems to be from a senior manager, asking for urgent login details to fix a critical system issue. The email uses specific details about recent company projects. This is an example of what social engineering technique?

MULTIPLE CHOICE

Choose the correct answer:

- A. Phishing
- B. Malware
- C. Pretexting
- D. Shoulder Surfing

Answer Keys & Solutions

Questions

1. You receive an urgent email from someone claiming to be from your bank, asking you to click a link to "verify your account immediately" or it will be shut down. Thinking about the social engineering attack cycle, what stage is this email primarily designed

MULTIPLE CHOICE

Correct Answer:

- | | |
|---|-------------|
| A. Information Gathering | ✗ Incorrect |
| B. Pretexting (Building a Relationship) | ✗ Incorrect |
| C. Exploitation | ✓ Correct |
| D. Recovery | ✗ Incorrect |

Explanation:

This stage is where the attacker tries to get the victim to take a specific action.

2. Before sending a deceptive email, an attacker spends weeks researching their target's public social media profiles and company website to learn about their interests and colleagues. What stage of the social engineering attack cycle does this describe?

MULTIPLE CHOICE

Correct Answer:

- | | |
|---|-------------|
| A. Exploitation | ✗ Incorrect |
| B. Building a Relationship (Pretexting) | ✗ Incorrect |
| C. Information Gathering | ✓ Correct |
| D. Recovery | ✗ Incorrect |

Explanation:

This is the initial phase where an attacker collects details about their victim.

3. A digital asset's value primarily comes from how many people want it and its use in transactions, and it's built on blockchain. It does not represent ownership in a company. Based on the passage, how would you classify this asset?

MULTIPLE CHOICE

Correct Answer:

- | | |
|-----------------------|-------------|
| A. A security | ✗ Incorrect |
| B. A digital currency | ✓ Correct |
| C. A stock | ✗ Incorrect |
| D. A bond | ✗ Incorrect |

Explanation:

Consider the primary purpose and underlying technology described for digital money.

4. A new digital asset is being launched. It calls itself a "digital currency" but also promises investors rights like voting in company decisions and a share of the app's profits. Based on the distinctions in the passage, how would you classify this asset?

MULTIPLE CHOICE

Correct Answer:

- | | |
|--|-------------|
| A. A pure digital currency | ✗ Incorrect |
| B. A type of security (security token) | ✓ Correct |
| C. A hybrid that doesn't fit either category | ✗ Incorrect |
| D. A scam, regardless of its features | ✗ Incorrect |

Explanation:

Think about what grants ownership rights and dividends in the traditional financial world.

5. An employee receives an email that seems to be from a senior manager, asking for urgent login details to fix a critical system issue. The email uses specific details about recent company projects. This is an example of what social engineering technique?

Correct Answer:

A. Phishing

✗ Incorrect

B. Malware

✗ Incorrect

C. Pretexting

✓ Correct

D. Shoulder Surfing

✗ Incorrect

Explanation:

This technique involves creating a believable story to gain trust.