

# Digital Trust and Cybersecurity Threats

---

## Textbook

---

# Digital Trust and Cybersecurity Threats



In today's online world, it's really important to understand how we interact digitally. This part of the book will explain tricky ways people try to fool us, called social engineering, and also teach us about digital money. We'll learn how trust can be misused and how to tell the difference between various digital assets. We'll also point out dangers, especially with digital money that doesn't have a "proof of work" system. All of this will help you use the internet more safely.

## How Social Engineering Attacks Happen

Social engineering is basically playing mind games with people, not using computer tricks, to get them to do something or give up information.<sup>1</sup>

It usually begins with getting information. Attackers secretly gather public and private details about people.<sup>2</sup> They often find this information on social media or company websites to build a complete picture of their target.<sup>3</sup>

Next, they try to build a relationship, which is sometimes called "pretexting."<sup>4</sup> Attackers gain trust by pretending to be someone else.<sup>5</sup> This could be a coworker or someone from the IT department. They use the information they gathered to create believable stories, like saying there's an urgent tech problem that needs login details.

Finally, in the exploitation stage, the attacker uses the trust and information they gained to get the victim to do what they want. This might involve clicking on a bad link, giving away passwords, or sending money. Attackers often create a feeling of urgency or offer fake rewards to rush the victim.<sup>6</sup>

These attacks can have a huge impact. Computer systems can be hacked, get infected with harmful software, and even shut down, which costs a lot of money.<sup>7</sup> Individuals can lose money, have their identity stolen, feel embarrassed, and become very upset. Businesses can lose their customers' trust and face legal problems.<sup>8</sup> The economy can suffer from businesses being shut down 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 constantly 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 something called a security. A digital currency, like Bitcoin, is mainly used for buying and selling things, storing value, and as a way to count money.<sup>9</sup> It's built on a technology called blockchain.<sup>10</sup> Its value comes from how many people want it or how useful it is, not from owning a piece of a company. If you own Bitcoin, you own a piece of digital money, not a share in a business.<sup>11</sup>

A security, often called a "security token," is like owning a piece of a company, similar to stocks or bonds.<sup>12</sup> These digital assets have to follow government rules for investments and can give you rights, like voting or a share of the company's profits.<sup>13</sup> Its value is directly connected to how well the company it represents is doing. The main difference is simple: one is for making purchases and storing value, while the other is an investment that shows you own a part of something.

## Digital Currencies

Digital currencies like Bitcoin (decentralized) and Central Bank Digital Currencies (CBDCs) are changing finance. Decentralized currencies operate without a central authority, offering transparency but often having high volatility, meaning their value can change wildly. This makes them risky for investors and less stable for everyday use.

In contrast, centralized digital currencies (like CBDCs) are controlled by a country's central bank, making them stable and backed by the government. While decentralized currencies challenge traditional finance by operating outside banks, CBDCs aim to make existing payment systems more efficient. Both types of digital currency impact the financial market by influencing payment speeds and investment risks, pushing regulators to adapt to these new forms of money.

## Understanding the Risks of Digital Currencies

While digital money offers exciting new ways to do things, it comes with unique risks you need to be aware of. One major risk is how quickly its value can change. Prices can go up and down very fast because of trading activity, news events, and global situations, which can lead to big money losses.<sup>14</sup> Unlike regular money, which is backed by governments, digital currencies don't have the same things to keep their value stable.

Security problems are also a concern. Even though blockchain technology is generally safe, the places where you keep and trade digital money can be hacked.<sup>15</sup> People can lose their digital money to scams, computer viruses, or ransomware that steals their digital wallets or secret keys.<sup>16</sup> Since there's no central authority for digital money, it's often hard to get your money back if it's stolen, and transactions usually cannot be undone.

Unclear rules are another risk. Governments around the world are still trying to figure out how to regulate digital money, which can cause sudden changes in rules that affect its value or whether it's legal to use.<sup>17</sup> Also, without clear rules, digital money can be used for illegal activities, which might lead to stricter government actions.<sup>18</sup>

A very important risk, especially for smaller digital currencies, is not having a "proof of work" (POW) system or another strong security method. POW, which Bitcoin uses, makes the network safe by requiring a lot of computer power to confirm transactions, making it very difficult to tamper with.<sup>19</sup> Without POW, it's easier and cheaper for bad actors to take control of the network (this is called a "51% attack").<sup>20</sup> This allows them to fake transactions or spend the same money twice. These types of digital currencies are much easier to manipulate and might not be safe for your money or transactions.

## Digital Money is Complicated

Finally, digital money can be complex, and people can make mistakes. It involves complicated ideas like private keys and digital addresses, which can be confusing. A simple mistake, like sending money to the wrong address, can mean losing it forever because transactions cannot be reversed. You are completely responsible for keeping your private keys safe, and if you lose them, you lose access to your digital money.<sup>21</sup> All these risks mean you need to do your research, invest carefully, and use strong security when dealing with digital currencies.

## Critical Thinking Questions

1. Imagine you see an online advertisement for a new digital currency that promises extremely high daily returns and says it's "risk-free" because it's backed by a new, secret technology. Based on the risks of digital currencies discussed, what specific red flags would you identify in this advertisement, and what steps would you take to investigate its legitimacy before considering any investment?
2. The text mentions that without a central authority, it's often hard to get your money back if it's stolen and transactions can't usually be undone.<sup>22</sup> How might the absence of a central authority be both a strength and a weakness of digital currencies? Provide an example for each.
3. Consider a scenario where a popular social media platform introduces its own "digital coin" that users can earn by interacting with content and then spend on virtual goods or donate to creators. Based on the definitions, would this be more like a digital currency or a security? What are the potential advantages and disadvantages for users of such a coin, both in terms of its purpose and its underlying technology (assuming it might or might not use Proof of Work)?

## 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.