The fight against cyber darkness

Number of Players:

4 players, where each player represents a company.

Materials:

Game board
42 security cards (blue)
20 attack cards (red)
24 chance cards (yellow)
Stock value points (different colours)
Crypto coins (orange)

In addition, you must bring:
Game pieces or post-it notes in 4 colours
Scissors
A die

The story behind

Welcome to the game. In it four start-ups compete to build the most secure and profitable business. But watch out! Threats such as hacking, phishing and internal vulnerabilities lurk everywhere. Can you navigate through these challenges and overcome the cyber darkness?

Goal:

The goal is to achieve as high a share price as possible while maintaining good IT security.

How to play:

1. Setup:
    a. Place the security cards (blue) on the board face up
    b. Shuffle the attack cards (red) and place them face down on the board
    c. Shuffle the chance cards (yellow) and place them face down on the board
    d. Place cryptocoins and share price points in their spaces on the board
    e. Each player chooses a game piece and places it on the starting square.
    f. Each player receives 100 stock value points (different colours) and 3 crypto coins (orange).
    g. Each player has the option to buy a security card (blue) by spending 1 crypto coin
2. The game
    a. START: Roll the die to determine who starts. The player who hits the lowest shall begin.
    b. MOVE: Roll the die, then move the piece according to the number shown on the die.
    c. ACTION: Always read the cards out loud. The action depends on which field the player lands on:

i. Blue: Safety field. The player can choose to buy a security card. The cards are paid for with cryptocoins, and the price is written on the card. Each security card protects against 2-6 types of IT attacks. The player is free to choose which available safety card he/she may want to buy.

ii. Red: Attack Card: The player draws an attack card
    1. The player reads the name of the card aloud, as well as how the attack works.
    2. ATTENTION! Some attacks can hit all companies at once. This appears at the top of the map.
    3. If the player's business is hit, the player can use their security cards to fend off the attack.
        a. The security cards show which attacks they protect against.
        b. If the player has a security card that parries the attack, the player will receive a bonus. The size of the bonus appears on the attack card.
        c. If the player does not have a security card that prevents the attack, the player must pay the cost shown on the attack card
        d. The player keeps the security card after it has been used and it can be used again
    4. Keep used attack cards

iii. Yellow: Chance card. The player draws a chance card and follows the instructions on the card. Used cards are placed at the bottom of the chance card stack

iv. Orange: Cryptocoin field. The player takes an IT security course and receives a cryptocoin.

v. Green:
    1. Starting field: Player receives 50 share price points and 2 cryptocoins when he/she lands on or passes start
    2. Semi-annual report: The player receives 25 stock value points when he/she lands on or passes the semi-annual report field.

3. Bankruptcy: If the player's total share price points are below 0, the player is bankrupt and exits the game.
4. Ending: The game ends when the first player has passed the start field for the second time.
5. The winner: The winner is the company with the highest share price value:
    a. Each security card has a value of value of x10 stock price points. Example: If the security card costs 2 cryptocoins, it has a value of 20 stock price points.
    b. Crypto coins have no value when the game is over
    c. Add up the total number of share price points

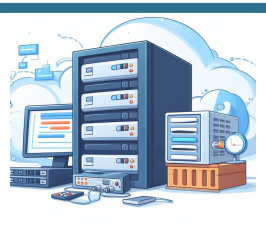
ANTI-PHISHING TRAINING

Train employees to recognize phishing attempts

Defends against the following

Phishing attacks
Spoofing
Data Leak
Ransomware

Cost
2 Crypto coins



AUTOMATIC BACKUP

Creates automatic copies of data to prevent data loss.

Defends against the following

Ransomware
Malware
Insider threat
SQL Injection

Cost
2 Crypto coins

BIOMETRIC AUTHENTICATION

Use physiological features such as fingerprints or facial recognition to provide access

Defends against the following
Credential Stuffing
Brute force

Cost
1 Crypto coin

DATA MASKING

Hides sensitive data with random characters

Defends against the following
Data Leak
SQL Injection
XSS Attack
Man-in-the-middle

Cost
2 Crypto coins

DDoS PROTECTION

Filters and redirects malicious traffic during DDoS attacks

Defends against the following
DDoS Attack
Zero-Day exploit

Cost
1 Crypto coin

ENDPOINT SECURITY

Protects network endpoints such as computers and mobile devices from malicious activity

Defends against the following
Zero-Day Exploit
Rootkit
Watering Hole
XSS Attack
Eavesdropping
Clickjacking

Cost
3 Crypto coins

FIREWALL

Blocks or allows network traffic based on security rules.

Defends against the following
Intern Hacking
DDoS Attack
Malware
Phishing attack
Ransomware
SQL Injection

Cost
3 Crypto coins

IDS

Monitors networks for signs of potential intrusions and sends alerts when they occur

Defends against the following
Intern Hacking
DDoS Attack
Eavesdropping
Clickjacking

Cost
2 Crypto coins

INCIDENT RESPONSE TEAM

A dedicated team ready to respond quickly to security breaches

Defends against the following
Phishingangreb
Spoofing
Insider threat
Social engineering

Cost
2 Crypto coins

ENCRYPTION

Converts plain text to code to protect data

Defends against the following
Ransomware
Spoofing

Cost
2 Crypto coins

LOG ANALYSE

Monitoring and analysing system logs to detect unusual or suspicious activity.

Defends against the following
Credential Stuffing
Man-in-the-middle

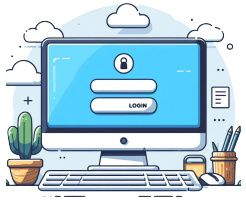
Cost
1 Crypto coin

MULTI-FACTOR AUTHENTICATION

Requires two or more forms of proof to validate a user's identity

Defends against the following
Data Leak
SQL Injection
Social engineering
Credential stuffing

Cost
2 Crypto coins



PASSWORD MANAGER

Software that generates and stores complex passwords, so users don't have to remember them.

Defends against the following
Keylogger
Credential stuffing

Cost
1 Crypto coins

PATCH MANAGEMENT

Manages software updates and patches.

Defends against the following
XSS Attack
Zero-day exploit

Cost
1 Crypto coin

RED TEAM EXERCISES

Simulated attacks on the organization's network to test its defence mechanisms

Defends against the following
Social Engineering
Phishing attack
SQL Injection
Man-in- the-middle

Cost
2 Crypto coins

REMOTE WIPE

Can remove data from a remote device to protect against unauthorized access

Defends against the following
Insider Threat
Rootkit

Cost
1 Crypto coin

SECURE EMAIL GATEWAY

Filters e-mail to detect and block threats.

Defends against the following
Clickjacking
Keylogger

Cost
1 Crypto coin

VPN

Creates a secure, encrypted connection for Internet access.

Defends against the following
Eavesdropping
Watering hole

Cost
1 Crypto coin

WHITELISTING

Allows only approved applications to run on a network or device.

Defends against the following
Malware
Rootkit
Spoofing
Watering hole

Cost
2 Crypto coins

ZERO TRUST ARCHITECTURE

No users or systems are automatically trusted; all must be verified.

Defends against the following
Insider Threat
Data Leak
Man-in-the-Middle
Intern hacking
Social engineering
Spoofing

Cost
3 Crypto coins

NO IT SECURITY INVESTMENT

You choose not to invest in IT security this turn.
As you save money in the company in the short term, you get an immediate capital gain of 15 points.

Cost
1 Crypto coin

Do not use

Do not use

Do not use

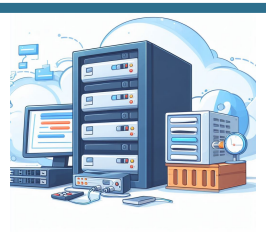
ANTI-PHISHING TRAINING

Train employees to recognize phishing attempts

Defends against the following

Phishing attacks
Spoofing
Data Leak
Ransomware

Cost
2 Crypto coins



AUTOMATIC BACKUP

Creates automatic copies of data to prevent data loss.

Defends against the following

Ransomware
Malware
Insider threat
SQL Injection

Cost
2 Crypto coins

BIOMETRIC AUTHENTICATION

Use physiological features such as fingerprints or facial recognition to provide access

Defends against the following
Credential Stuffing
Brute force

Cost
1 Crypto coin

DATA MASKING

Hides sensitive data with random characters

Defends against the following

Data Leak
SQL Injection
XSS Attack
Man-in-the-middle

Cost
2 Crypto coins

DDoS PROTECTION

Filters and redirects malicious traffic during DDoS attacks

Defends against the following
DDoS Attack
Zero-Day exploit

Cost
1 Crypto coin

ENDPOINT SECURITY

Protects network endpoints such as computers and mobile devices from malicious activity

Defends against the following
Zero-Day Exploit
Rootkit
Watering Hole
XSS Attack
Eavesdropping
Clickjacking

Cost
3 Crypto coins

FIREWALL

Blocks or allows network traffic based on security rules.

Defends against the following
Intern Hacking
DDoS Attack
Malware
Phishing attack
Ransomware
SQL Injection

Cost
3 Crypto coins

IDS

Monitors networks for signs of potential intrusions and sends alerts when they occur

Defends against the following
Intern Hacking
DDoS Attack
Eavesdropping
Clickjacking

Cost
2 Crypto coins

INCIDENT RESPONSE TEAM

A dedicated team ready to respond quickly to security breaches

Defends against the following
Phishing attack
Spoofing
Insider threat
Social engineering

Cost
2 Crypto coins

ENCRYPTION

Converts plain text to code to protect data

Defends against the following
Ransomware
Spoofing

Cost
2 Crypto coins

LOG ANALYSE

Monitoring and analysing system logs to detect unusual or suspicious activity.

Defends against the following
Credential Stuffing
Man-in-the-middle

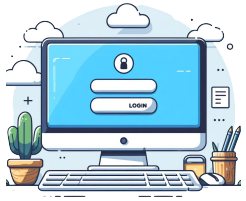
Cost
1 Crypto coin

MULTI-FACTOR AUTHENTICATION

Requires two or more forms of proof to validate a user's identity

Defends against the following
Data Leak
SQL Injection
Social engineering
Credential stuffing

Cost
2 Crypto coins



PASSWORD MANAGER

Software that generates and stores complex passwords, so users don't have to remember them.

Defends against the following
Keylogger
Credential stuffing

Cost
1 Crypto coins

PATCH MANAGEMENT

Manages software updates and patches.

Defends against the following
XSS Attack
Zero-day exploit

Cost
1 Crypto coin

RED TEAM EXERCISES

Simulated attacks on the organization's network to test its defence mechanisms

Defends against the following
Social Engineering
Phishing attack
SQL Injection
Man-in- the-middle

Cost
2 Crypto coins

REMOTE WIPE

Can remove data from a remote device to protect against unauthorized access

Defends against the following
Insider Threat
Rootkit

Cost
1 Crypto coin

SECURE EMAIL GATEWAY

Filters e-mail to detect and block threats.

Defends against the following
Clickjacking
Keylogger

Cost
1 Crypto coin

VPN

Creates a secure, encrypted connection for Internet access.

Defends against the following
Eavesdropping
Watering hole

Cost
1 Crypto coin

WHITELISTING

Allows only approved applications to run on a network or device.

Defends against the following
Malware
Rootkit
Spoofing
Watering hole

Cost
2 Crypto coins

ZERO TRUST ARCHITECTURE

No users or systems are automatically trusted; all must be verified.

Defends against the following
Insider Threat
Data Leak
Man-in-the-Middle
Intern hacking
Social engineering
Spoofing

Cost
3 Crypto coins

NO IT SECURITY INVESTMENT

You choose not to invest in IT security this turn.
As you save money in the company in the short term, you get an immediate capital gain of 15 points.

Cost
1 Crypto coin

Do not use

Do not use

Do not use

NEW HIRE

You hire a skilled security expert and therefore get an extra turn.

Roll the die immediately.

You also receive 25 stock value points

FINANCIAL BONUS

Your stocks are doing well.

You receive 30 stock value points.

SECURITY AUDIT

External consultants review the company's IT security. Your business is doing well.

Choose a free security card worth 1 crypto coin.

You also receive 10 stock value points

WHISTLEBLOWER

Your company receives insider information that prevents the next IT attack.

Save this card for the next time your company is under attack.

You also receive 20 stock value points immediately.

GOOD NEWS

The security measures in your company boost the company's reputation.

You gain immunity next turn so you can't be hit by attacks. Save this card until you have played the next turn.

You also receive 20 stock value points immediately

FINE

Your company has not complied with the GDPR rules and therefore receives a fine that causes share prices to fall.

You lose 10 stock value points.

BAD NEWS

Your company is exposed to a serious hacker attack, which reveals shortcomings in the company's IT security. It gives bad press coverage.

You lose the next turn as you are busy dealing with the media.

TERMINATION

One of your skilled IT employees has resigned due to a lack of development opportunities in the company.

You lose the next turn as you are busy hiring a new employee.

PHISHING

An accountant falls for a phishing attempt and sends a large sum of money to an unknown fraudster.

You lose an optional security card.

FAILURE TO UPDATE

Your company's IT security systems are not up to date. It is being exploited by hackers.

The next time you land on an attack field, you must draw two attack cards.
Save the card until then.

REUSE OF PASSWORDS

Many employees in your company use the same password for different services. It poses a very high risk that a hacker can gain access to many systems if a password is leaked.

You must skip a round while you get to grips with IT security.

MISSING BACKUP

Your company does not regularly make backup copies of the critical data. This makes the company vulnerable to the loss of valuable and business-critical data.

You lose 10 stock value points.
NOTE: If you have the "Automatic Backup" security card, you will not lose points.

STORM SURGE

A storm surge hits the country and causes water in the company's server room.

The IT department has to use a lot of resources to handle the situation and you lose a crypto coin.

PRIZE AWARD

Your company receives an industry award for good IT security, which increases employee morale.

The next time you land on an attack field, do not draw an attack card.
Save this card until next turn.
You also receive 20 stock value points.

NEW SECURITY-TECHNOLOGY

A research breakthrough provides the company with a new defence against malware.

You will receive a free security card worth 1 crypto coin.
You also receive 15 stock value points.

COLLABORATION WITH COMPETITORS

You are part of a collaboration to improve IT security in the industry. It is going to be a success.

The next time you manage to ward off an attack with a security card, you will receive a double bonus.
Save this card until then.

SUSTAINABILITY

Your company receives positive publicity in the media for its sustainability initiatives. This causes the share price to rise.

Receive 20 stock value points.

POOR OVERVIEW

A review of the security reveals that there is a lack of overview of the most critical data and systems that should be protected in your company.

You lose 1 crypto coin.

MISSING TWO-FACTOR LOGIN

Your company does not use two-factor login. This makes employees' digital activities more insecure.

You should skip a step while you get a handle on IT security.
NOTE! If you have the security card "Multifactor Authentication", you should not skip this turn.

WEAK PASSWORDS

Several employees use passwords that are too weak. This increases the risk of the company being hacked.

The next time you land on an attack field, draw two attack cards.
Save this card until then.

GDPR COURSE

All employees have completed an online GDPR course.

Receive 10 stock value points.

SoMe CAMPAIGN

Your company is very successful with a fun social media campaign.

Receive 15 stock value points

PRODUCT DEVELOPMENT

Your company is launching a new breakthrough product.

Receive 15 stock value points

EFFICIENCY

Your company introduces new initiatives in production that reduce costs and improve operational efficiency.

Receive 15 stock value point

QUESTION TO YOUR NEIGHBOUR ON THE RIGHT

How long does it theoretically take for a hacker to crack this password?: G5jDh40PgD3

A) 35 minutes
B) 4 days
C) 41 years

If your neighbour answers correctly, he/she must advance 2 spaces.

Answer: C) 41 years

QUESTION TO YOUR NEIGHBOUR ON THE RIGHT

What is it called when people try to trick you into giving them personal information via fake emails?

A) Pswimming
B) Hunting
C) Phishing

If your neighbour answers correctly, he/she moves forward 1 space.

Answer: C) Phishing

QUESTION TO YOUR NEIGHBOUR ON THE RIGHT

What is called software that does destructive or unwanted things on your computer, for example by using viruses.

A) Wall-ware
B) Malware
C) Event manager

If your neighbour answers correctly, he/she must advance 3 spaces.

Answer: B) Malware

QUESTION TO YOUR NEIGHBOUR ON THE RIGHT

What safety measure should your company invest in as a minimum, regardless of size?

A) Encryption technology
B) Antivirus
C) Data discovery

If your neighbour answers correctly, he/she must advance 2 spaces.

Answer: B) Antivirus

QUESTION TO YOUR NEIGHBOUR ON THE RIGHT

How long does it theoretically take for a hacker to crack this password?: H2Gj4f

A) 1 second
B) 30 seconds
C) 4 hours

If your neighbour answers correctly, he/she must advance 1 space.

Answer: A) 1 second, as it only contains 6 characters

QUESTION TO YOUR NEIGHBOUR ON THE RIGHT

What the function of a VPN?

A) To increase the speed of the network
B) To create a secure and encrypted connection over the Internet
C) To manage user accounts and access rights

If your neighbour answers incorrectly, he/she must move back 1 square.

Answer: B) To create a secure and encrypted connection over the Internet

QUESTION TO YOUR NEIGHBOUR ON THE RIGHT

Which of the following types of attacks is considered a form of social engineering?

A) Brute force attack
B) Phishing
C) DDoS attacks

If your neighbour answers correctly, he/she receives 15 stock value points.
Answer: B) Phishing

QUESTION TO YOUR NEIGHBOUR ON THE RIGHT

What gives you the best protection in the fight against the cyber threat?

A) New work computers
B) Teaching hacking methods
C) Awareness training

If your neighbour answers correctly, he/she must advance 2 spaces.

Answer: C) Awareness training

INSIDER THREAT

An employee inadvertently puts the company's security at risk when he shares sensitive data with unauthorized persons.

Loss on attack
Your company loses 20 stock value points

Bonus on successful defence:
1 Crypto coin

DATA LEAK

Hackers have gained unauthorized access to your company's data and this data has been shared.

Loss on attack
Your company loses 30 stock value points

Bonus on successful defence:
2 Crypto coins

MAN-IN-THE-MIDDLE

A hacker has gained access to read, change or steal information that is sent between two devices in your company.

Loss on attack
Your company loses 15 stock value points

Bonus on successful defence:
1 Crypto coin

SQL INJECTION

A hacker has used malicious SQL code on your company's website and obtained your customers' credit card information.

Loss on attack
Your company loses 20 stock value points

Bonus on successful defence:
1 Crypto coin

ZERO-DAY EXPLOIT

All companies are being attacked
There is a vulnerability in your company's software. It is exploited by IT criminals before you can detect and fix it.

Loss on attack
Your company loses 20 stock value points

Bonus on successful defence:
1 Crypto coin

ROOTKIT

Your company is exposed to a rootkit attack, where hidden software gives the attacker control over the company's IT system.

Loss on attack
Your company loses 20 stock value points

Bonus on successful defence:
2 Crypto coins

CREDENTIAL STUFFING

All companies are being attacked
A hacker uses stolen usernames and passwords from other services to try to log into your systems.

Loss on attack
Your company loses 15 stock value points

Bonus on successful defence:
1 Crypto coin

EAVES DROPPING

A hacker listens in on your company's communications, which can lead to the leakage of confidential information.

Loss on attack
Your company loses 20 stock value points

Bonus on successful defence:
1 Crypto coin

PHISHING ATTACK

All companies are being attacked
Your company is exposed to fake emails and messages that try to steal company information.

Loss on attack
Your company loses 20 stock value points

Bonus on successful defence:
1 Crypto coin

INTERN HACKING

One of your employees abuses his access rights to obtain sensitive data about the company.

Loss on attack
Your company loses 30 stock value points

Bonus on successful defence:
2 Crypto coins

DDoS Attack

All companies are being attacked
Your company's website is overloaded with massive traffic, so it goes down.

Loss on attack
Your company loses 15 stock value points

Bonus on successful defence:
1 Crypto coin

RANSOMWARE

Hackers infect your company's IT systems with malware that locks your files. The hackers demand a ransom to release the files.

Loss on attack
2 Crypto coins

Bonus on successful defence:
1 Crypto coin

KEY LOGGER

Hackers have installed keyloggers on the company's computers. They can therefore record everything that is typed on a keyboard. That way, they can get hold of passwords and confidential data.

Loss on attack
1 security card

Bonus on successful defence:
2 Crypto coins

BRUTE FORCE

Hackers try to crack your employees' passwords by repeated guesses.

Loss on attack
Your company loses 25 stock value points

Bonus on successful defence:
2 Crypto coins

SOCIAL ENGINEERING

IT criminals try to manipulate your employees into giving up sensitive information.

Loss on attack
1 security card

Bonus on successful defence:
1 Crypto coin

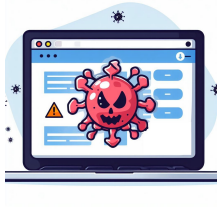
MALWARE

All companies are being attacked

Hackers insert malicious software designed to damage or hack your company's IT system.

Loss on attack
Your company loses 15 stock value points

Bonus on successful defence:
1 Crypto coin



XSS ATTACK

Hackers insert malicious code into your company's website to steal customer login information.

Loss on attack
Your company loses 15 stock value points

Bonus on successful defence:
1 Crypto coin

SPOOFING

An IT criminal sends an email to an employee in your accounting department. The criminal pretends to be the director and asks the employee to transfer a sum of money.

Loss on attack
Your company loses 30 stock value points
Bonus on successful defence:
2 Crypto coins

CLICKJACKING

The users of your company's web-shop are tricked into clicking on hidden links and buttons. In this way, criminals gain unauthorized access to steal data.

Loss on attack
Your company loses 15 stock value points

Bonus on successful defence:
1 Crypto coin

WATERING HOLE

All companies are being attacked
Hackers infect websites that your employees visit frequently. The purpose is to spread malware to users' computers.

Loss on attack
Your company loses 20 stock value points
Bonus on successful defence:
1 Crypto coin

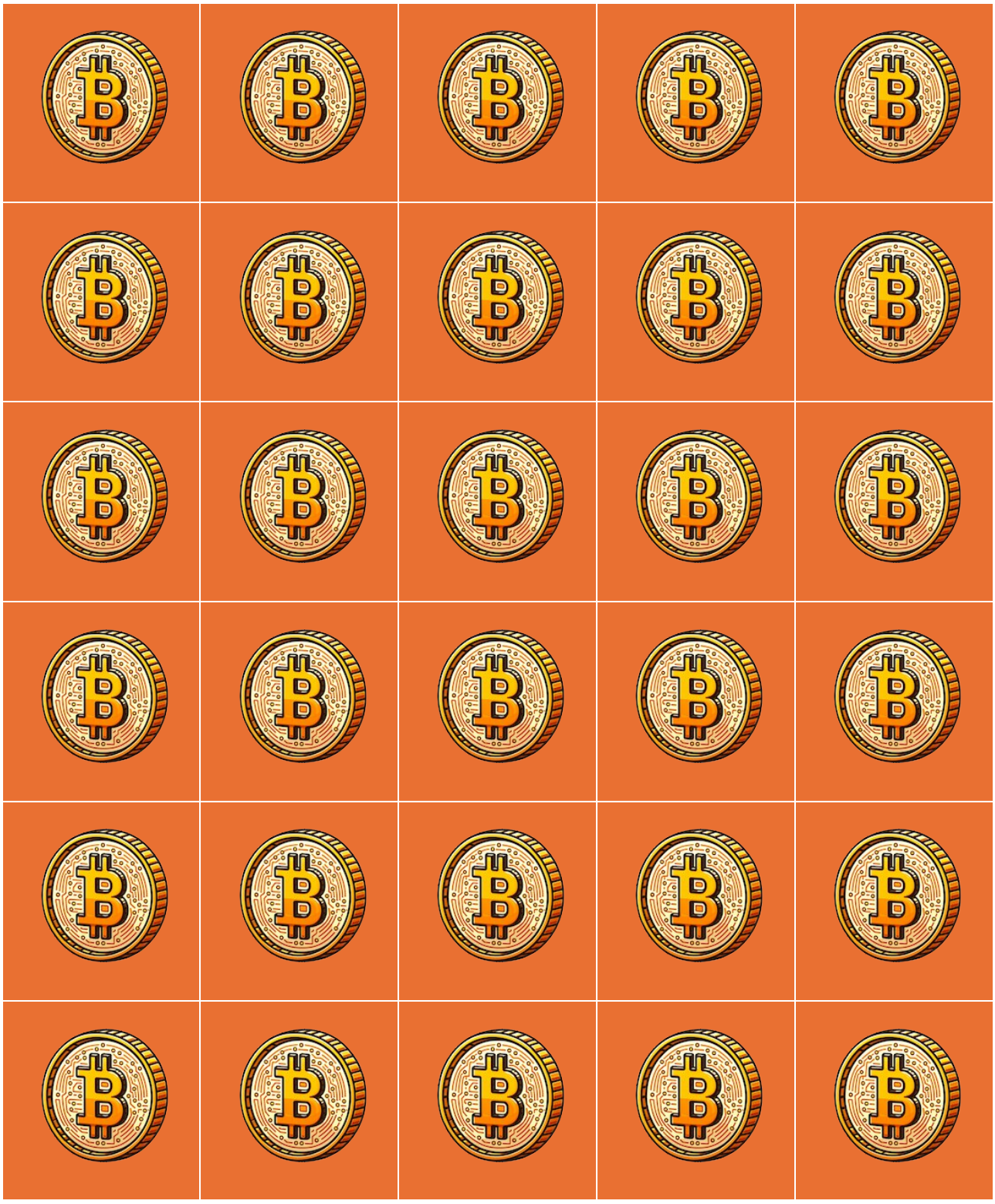
Do not use

Do not use

Do not use

Do not use

CRYPTO COINS



STOCK VALUE POINTS

5	5	5	5	5
5	5	5	5	5
5	5	5	5	5
10	10	10	10	10
10	10	10	10	10
10	10	10	10	10
20	20	20	20	20
20	20	20	20	20
20	20	20	20	20
50	50	50	50	50
50	50	50	50	50