AVENQOR
EDUCATION ONLY

Security First: Scams, Phishing, Custody

Practical anti-scam training

Protect your assets and knowledge.

Scams Phishing Custody Hygiene

Legal and Risk Notice

- This course is for educational purposes only and does not provide financial advice.
- Trading in high-risk markets can result in significant financial loss.
- No guarantees of profit are made in this course.
- Always verify information independently before acting.
- This course does not endorse any specific trading platform or product.

Who This Is Not For

- Individuals seeking guaranteed profits.
- Those unwilling to accept the risks associated with trading.
- People looking for specific investment advice.

How to Use This Course

Recommended Pace

- Take your time to understand each module thoroughly.
- Review the exercises and checklists after each module.
- Consider revisiting sections for reinforcement.

Instructions

- Read each module carefully and take notes.
- Complete the exercises to apply your knowledge.
- Use the glossary for unfamiliar terms.
- Engage with the self-test quiz to assess your understanding.
- Review the one-page summary for key points.
- Stay updated on security practices as they evolve.

This course is designed to be printed for offline study.

Keep a journal of your learning and personal security experiences.

Set a regular schedule for reviewing course materials.

Table of Contents

Click on the module titles to navigate directly to the sections.

Preface / Orientation

Who This Is For

- Complete beginners wanting a solid foundation in security practices.
- Self-taught users seeking structured knowledge on scams and security.
- Individuals interested in protecting their digital assets.

What You Will Learn

- Identify various types of scams and phishing attempts.
- Understand social engineering tactics used by scammers.
- Implement custody hygiene to protect your assets.
- Recognize the importance of transaction finality.
- Build a personal security stack for safer trading.
- Develop verification habits to avoid scams.

What This Course Will Not Do

- Provide specific investment advice or recommendations.
- Guarantee profits or success in trading.
- Replace the need for ongoing education in security practices.
- Offer real-time trading or investment strategies.

Prerequisites

- No prior knowledge is required.
- A willingness to learn and apply security practices.

Understanding Scam Categories

Goal: To familiarize learners with different types of scams prevalent in trading markets.

Phishing Scams

Phishing scams involve tricking individuals into providing sensitive information, such as passwords or private keys, by masquerading as trustworthy entities.

> Phishing: A fraudulent attempt to obtain sensitive information by disguising as a trustworthy source.

These scams can occur via email, social media, or fake websites.

> Hypothetical example
>
> For example, a user may receive an email that appears to be from a legitimate exchange asking them to verify their account by clicking a link.

Understanding these patterns is crucial for avoiding losses.

Why it matters: Recognizing phishing attempts can prevent unauthorized access to your accounts.

Impersonation and Fake Airdrops

Impersonation scams involve fraudsters pretending to be someone else, often a known figure in the crypto space, to solicit funds or information.

> Impersonation: Pretending to be someone else to deceive others.

Fake airdrops promise free tokens but require users to send funds or personal information.

> Hypothetical example
>
> A user might see a social media post claiming to give away free tokens if they send a small amount of cryptocurrency.

Why it matters: Awareness of these scams helps users avoid falling victim to fraudulent schemes.

Understanding these patterns can help you avoid unnecessary losses.

Scam Awareness Checklist

- Verify the source of any communication before acting.
- Never share your private keys or passwords.
- Be cautious of unsolicited offers, especially those promising high returns.
- Check for official announcements from platforms you use.
- Use official channels to verify claims.
- Report suspicious activity to relevant authorities.
- Educate yourself continuously about new scams.

Exercise: Identify Scam Patterns

Purpose: To practice recognizing different scam types in hypothetical scenarios.

1. Review the provided scenarios and identify which scams are present.
2. Discuss with a peer or write down your findings.
3. Reflect on how you would respond to each scenario.
4. Consider what preventive measures you could take.
5. Share your insights in a group discussion.

Expected Output: A list of identified scams and proposed responses.

Risk Awareness

- Scams can lead to total loss of funds.
- Always verify the authenticity of communications.
- Be cautious of urgency and unsolicited offers.
- Educate yourself regularly to stay updated on new scams.

Key Takeaways

- Phishing and impersonation are common scams.
- Always verify sources before sharing information.
- Awareness is key to preventing losses.
- Stay informed about the latest scam tactics.
- Implement a personal security plan.

Social Engineering Techniques

Goal: To understand how scammers manipulate individuals to gain access to sensitive information.

Urgency and Authority

Scammers often create a sense of urgency to prompt quick action without thought.

> Urgency: A psychological tactic that pressures individuals to act quickly.

They may impersonate authority figures to gain trust.

> Hypothetical example
>
> A scammer might claim they are from a regulatory body and need immediate verification of your identity.

Why it matters: Recognizing these tactics can help you pause and verify before acting.

Understanding these patterns can help you avoid unnecessary losses.

Reward Hooks

Scammers often use the promise of rewards to entice individuals.

> Reward Hook: A tactic that offers something desirable to manipulate behavior.

These hooks can lead to sharing sensitive information.

> Hypothetical example
>
> A user may receive a message claiming they have won a prize but must provide personal information to claim it.

Why it matters: Being aware of these hooks can prevent you from falling for scams.

Understanding these patterns can help you avoid unnecessary losses.

Social Engineering Awareness Checklist

- Be skeptical of unsolicited communications.
- Verify claims of urgency or authority.
- Avoid sharing personal information without verification.
- Recognize the signs of reward hooks.
- Educate yourself on common social engineering tactics.
- Discuss these tactics with peers to reinforce learning.
- Stay updated on new manipulation techniques.

Exercise: Analyze Social Engineering Scenarios

Purpose: To practice identifying social engineering tactics in hypothetical situations.

1. Review the scenarios provided and identify the tactics used.
2. Discuss your findings with a partner or write them down.
3. Reflect on how you would respond to each scenario.
4. Consider what preventive measures you could take.
5. Share your insights in a group discussion.

Expected Output: A list of identified social engineering tactics and proposed responses.

Risk Awareness

- Social engineering can lead to significant financial loss.
- Always verify the identity of individuals before sharing information.
- Be cautious of urgent requests for information.
- Educate yourself regularly about manipulation tactics.

Key Takeaways

- Urgency and authority are common manipulation tactics.
- Reward hooks can lead to sharing sensitive information.
- Awareness is key to preventing social engineering scams.
- Stay informed about the latest tactics used by scammers.
- Implement a personal security plan.

Custody Hygiene Practices

Goal: To understand how to protect your digital assets through proper custody practices.

Understanding Custody Risks

Custody refers to the management and protection of digital assets.

> Custody: The responsibility for safeguarding assets.

Losses can occur through hacks, scams, or negligence.

> Hypothetical example
>
> A user may lose funds if their exchange account is hacked.

Why it matters: Understanding custody risks helps you take proactive measures to protect your assets.

Understanding these patterns can help you avoid unnecessary losses.

Reducing Attack Surface

Reducing your attack surface involves minimizing vulnerabilities.

> Attack Surface: The total sum of vulnerabilities in a system.

This can be achieved through secure practices and tools.

> Hypothetical example
>
> Using a hardware wallet reduces the risk of online hacks.

Why it matters: A smaller attack surface means fewer opportunities for scammers.

Understanding these patterns can help you avoid unnecessary losses.

Custody Hygiene Checklist

- Use strong, unique passwords for all accounts.

- Enable two-factor authentication (2FA) where possible.
- Consider using hardware wallets for long-term storage.
- Regularly review and update your security practices.
- Be cautious of sharing access to your accounts.
- Educate yourself on custody best practices.
- Stay informed about new security tools and techniques.

Exercise: Evaluate Your Custody Practices

Purpose: To assess your current custody practices and identify areas for improvement.

1. Review your current custody methods and tools.
2. Identify potential vulnerabilities in your practices.
3. Discuss with a peer or write down your findings.
4. Consider what changes you could make to enhance security.
5. Share your insights in a group discussion.

Expected Output: A list of identified vulnerabilities and proposed improvements.

Risk Awareness

- Custody risks can lead to total loss of assets.
- Always use secure methods for managing your assets.
- Be cautious of sharing access to your accounts.
- Educate yourself regularly about custody best practices.

Key Takeaways

- Understanding custody is crucial for asset protection.
- Reducing your attack surface minimizes risks.
- Implementing strong security practices is essential.
- Stay informed about custody hygiene.
- Regularly review your security measures.

Transaction Finality Explained

Goal: To understand the concept of transaction finality and its implications.

What is Transaction Finality?

Transaction finality refers to the point at which a transaction cannot be reversed.

> Transaction Finality: The irreversible state of a completed transaction.

Once confirmed, transactions on blockchain networks are permanent.

> Hypothetical example
>
> If you send cryptocurrency to the wrong address, it cannot be recovered.

Why it matters: Understanding finality helps you make informed decisions before executing transactions.

Understanding these patterns can help you avoid unnecessary losses.

Implications of Finality

The irreversible nature of transactions means caution is necessary.

> Irreversible: A state that cannot be undone.

Mistakes can lead to permanent losses.

> Hypothetical example
>
> Sending funds to a scammer's address results in total loss.

Why it matters: Being aware of transaction finality can prevent costly mistakes.

Understanding these patterns can help you avoid unnecessary losses.

Transaction Finality Awareness Checklist

- Double-check addresses before sending funds.

- Understand the implications of irreversible transactions.
- Be cautious when executing transactions, especially with large amounts.
- Educate yourself on transaction processes.
- Stay informed about blockchain technology.
- Discuss transaction finality with peers to reinforce learning.
- Regularly review your understanding of transaction processes.

Exercise: Analyze Transaction Scenarios

Purpose: To practice evaluating transaction finality in hypothetical situations.

1. Review the provided transaction scenarios.
2. Identify potential risks and mistakes in each scenario.
3. Discuss your findings with a partner or write them down.
4. Consider what preventive measures you could take.
5. Share your insights in a group discussion.

Expected Output: A list of identified risks and proposed responses.

Risk Awareness

- Transaction finality can lead to total loss of funds.
- Always double-check transaction details before execution.
- Be cautious of irreversible transactions.
- Educate yourself regularly about transaction processes.

Key Takeaways

- Transaction finality is a critical concept in trading.
- Irreversible transactions can lead to significant losses.
- Awareness is key to preventing costly mistakes.
- Stay informed about transaction processes.
- Implement a personal review process before transactions.

Building a Security Stack

Goal: To understand the components of a personal security stack for safe trading.

Password Managers

Password managers help store and generate strong passwords securely.

> Password Manager: A tool that stores and encrypts passwords.

Using a password manager reduces the risk of weak passwords.

> Hypothetical example
>
> A user can generate complex passwords for each account without needing to remember them.

Why it matters: Strong passwords are essential for protecting accounts.

Understanding these patterns can help you avoid unnecessary losses.

Two-Factor Authentication (2FA)

2FA adds an extra layer of security by requiring a second form of verification.

> Two-Factor Authentication: A security process that requires two forms of identification.

This makes unauthorized access more difficult.

> Hypothetical example
>
> A user must enter a code sent to their phone in addition to their password.

Why it matters: 2FA significantly enhances account security.

Understanding these patterns can help you avoid unnecessary losses.

Hardware Wallets

Hardware wallets store cryptocurrencies offline, providing enhanced security.

> Hardware Wallet: A physical device that securely stores cryptocurrency.

They protect against online hacks.

> Hypothetical example
>
> A user can store their assets in a hardware wallet, making them less vulnerable to online threats.

Why it matters: Using a hardware wallet can prevent unauthorized access to your funds.

Understanding these patterns can help you avoid unnecessary losses.

Security Stack Checklist

- Use a password manager for all accounts.
- Enable 2FA on every platform that offers it.
- Consider investing in a hardware wallet for long-term storage.
- Regularly update your passwords and security settings.
- Educate yourself on the latest security tools and techniques.
- Discuss security practices with peers to reinforce learning.
- Stay informed about new threats and vulnerabilities.

Exercise: Build Your Security Stack

Purpose: To create a personal security stack tailored to your needs.

1. Evaluate your current security practices.
2. Identify gaps in your security stack.
3. Research and select tools to enhance your security.
4. Create a plan to implement these tools.
5. Share your security stack with a peer for feedback.

Expected Output: A comprehensive security stack plan tailored to your needs.

Risk Awareness

- A weak security stack can lead to total loss of funds.
- Always use strong passwords and 2FA.
- Be cautious of sharing access to your accounts.
- Educate yourself regularly about security practices.

Key Takeaways

- A strong security stack is essential for safe trading.
- Password managers and 2FA significantly enhance security.
- Regularly review and update your security practices.
- Stay informed about new security tools and techniques.
- Implement a personal security plan.

Verification Habits

Goal: To develop good verification habits to avoid scams.

Link Verification

Always verify links before clicking to avoid phishing sites.

> Link Verification: The process of checking the authenticity of a URL.

Hovering over links can reveal their true destination.

> Hypothetical example
>
> A user may receive a link that appears legitimate but leads to a fraudulent site.

Why it matters: Verifying links can prevent falling victim to phishing scams.

Understanding these patterns can help you avoid unnecessary losses.

Permissions and Approvals

Always review permissions before granting access to your accounts.

> Permissions: The rights granted to applications or users to access your information.

Be cautious of apps that request excessive permissions.

> Hypothetical example
>
> A legitimate app may request access to your contacts, but a scam app may ask for unnecessary permissions.

Why it matters: Reviewing permissions helps protect your data and assets.

Understanding these patterns can help you avoid unnecessary losses.

Verification Habits Checklist

- Always verify links before clicking.
- Review permissions before granting access.
- Educate yourself on common phishing tactics.
- Be cautious of unsolicited requests for information.
- Discuss verification habits with peers to reinforce learning.
- Stay informed about new verification techniques.
- Regularly review your verification practices.

Exercise: Practice Verification Techniques

Purpose: To reinforce good verification habits in hypothetical scenarios.

1. Review the provided scenarios and identify verification opportunities.
2. Discuss your findings with a partner or write them down.
3. Reflect on how you would respond to each scenario.
4. Consider what preventive measures you could take.
5. Share your insights in a group discussion.

Expected Output: A list of identified verification opportunities and proposed responses.

Risk Awareness

- Poor verification habits can lead to significant losses.
- Always verify links and permissions before acting.
- Be cautious of unsolicited requests for information.
- Educate yourself regularly about verification practices.

Key Takeaways

- Good verification habits are essential for security.
- Always verify links and permissions before acting.
- Awareness is key to preventing scams.
- Stay informed about the latest verification techniques.
- Implement a personal review process for verification.

Personal Security SOP

Goal: To develop a personal security standard operating procedure (SOP).

Creating Your SOP

A personal security SOP outlines your security practices and protocols.

> Standard Operating Procedure (SOP): A set of step-by-step instructions to help achieve a desired outcome.

Your SOP should include guidelines for password management, 2FA, and verification habits.

> Hypothetical example
>
> An SOP might dictate that you always use a password manager and enable 2FA on all accounts.

Why it matters: A clear SOP helps reinforce good security practices.

Understanding these patterns can help you avoid unnecessary losses.

Implementing Your SOP

Implementing your SOP involves putting your guidelines into practice.

Regularly review and update your SOP as needed.

> Hypothetical example
>
> If you adopt a new security tool, update your SOP to include it.

Why it matters: Consistent application of your SOP enhances security.

Understanding these patterns can help you avoid unnecessary losses.

Regularly reviewing your SOP ensures it remains effective.

Personal Security SOP Checklist

- Create a personal security SOP outlining your practices.
- Review and update your SOP regularly.

- Discuss your SOP with peers for feedback.
- Educate yourself on new security practices.
- Stay informed about emerging threats and vulnerabilities.
- Implement your SOP consistently.
- Reflect on your security practices regularly.

Exercise: Develop Your Personal Security SOP

Purpose: To create a tailored personal security SOP.

1. Draft your personal security SOP based on your current practices.
2. Identify areas for improvement in your SOP.
3. Share your SOP with a peer for feedback.
4. Consider what changes you could make to enhance security.
5. Implement your SOP and reflect on its effectiveness.

Expected Output: A comprehensive personal security SOP tailored to your needs.

Risk Awareness

- A lack of a personal security SOP can lead to vulnerabilities.
- Always review and update your SOP as needed.
- Be cautious of emerging threats to your security.
- Educate yourself regularly about security practices.

Key Takeaways

- A personal security SOP is essential for consistent practices.
- Regularly reviewing your SOP enhances security.
- Implementing your SOP can prevent vulnerabilities.
- Stay informed about new security tools and techniques.
- Reflect on your security practices regularly.

Incident Response Checklist

Goal: To develop an incident response plan for potential security breaches.

Creating Your Incident Response Plan

An incident response plan outlines steps to take in case of a security breach.

> Incident Response Plan: A documented strategy for responding to security incidents.

Your plan should include contact information for reporting incidents and steps to mitigate damage.

> Hypothetical example
>
> An incident response plan might include steps to secure accounts and notify relevant parties.

Why it matters: Having a plan in place can minimize damage during a breach.

Understanding these patterns can help you avoid unnecessary losses.

Testing Your Incident Response Plan

Regularly testing your incident response plan ensures its effectiveness.

Conduct drills to practice your response to hypothetical incidents.

> Hypothetical example
>
> Simulate a phishing attack to test your response plan.

Why it matters: Testing helps identify weaknesses in your plan.

Understanding these patterns can help you avoid unnecessary losses.

Regularly reviewing your plan ensures it remains effective.

Incident Response Checklist

- Create an incident response plan outlining your steps.
- Regularly test your incident response plan.
- Educate yourself on common security incidents.

- Discuss your plan with peers for feedback.
- Stay informed about new threats and vulnerabilities.
- Implement your incident response plan consistently.
- Reflect on your incident response practices regularly.

Exercise: Develop Your Incident Response Plan

Purpose: To create a tailored incident response plan for potential breaches.

1. Draft your incident response plan based on your current practices.
2. Identify areas for improvement in your plan.
3. Share your plan with a peer for feedback.
4. Consider what changes you could make to enhance your response.
5. Implement your plan and reflect on its effectiveness.

Expected Output: A comprehensive incident response plan tailored to your needs.

Risk Awareness

- A lack of an incident response plan can lead to severe consequences.
- Always review and update your plan as needed.
- Be cautious of emerging threats to your security.
- Educate yourself regularly about incident response practices.

Key Takeaways

- An incident response plan is essential for managing breaches.
- Regularly testing your plan enhances its effectiveness.
- Implementing your plan can minimize damage during incidents.
- Stay informed about new security tools and techniques.
- Reflect on your incident response practices regularly.

One-Page Rules & Reality Check Summary

Key Security Practices

- Always verify links before clicking.
- Use strong, unique passwords and a password manager.
- Enable 2FA on all accounts.
- Regularly review and update your security practices.

Scam Awareness

- Be cautious of unsolicited communications.
- Recognize common scam patterns.
- Educate yourself on new scams regularly.
- Report suspicious activity.

Incident Response

- Create and test an incident response plan.
- Stay informed about emerging threats.
- Reflect on your security practices regularly.
- Implement your plan consistently.

Final Thoughts

- Security is an ongoing process.
- Stay informed and adaptable.
- Engage with the community for shared learning.
- Prioritize your digital safety.

This summary is designed for quick reference and review.

Glossary

Phishing

A fraudulent attempt to obtain sensitive information by disguising as a trustworthy source.

Recognizing phishing attempts can prevent unauthorized access to your accounts.

Custody

The responsibility for safeguarding assets.

Understanding custody risks helps you take proactive measures to protect your assets.

Two-Factor Authentication (2FA)

A security process that requires two forms of identification.

2FA significantly enhances account security.

Incident Response Plan

A documented strategy for responding to security incidents.

Having a plan in place can minimize damage during a breach.

Attack Surface

The total sum of vulnerabilities in a system.

A smaller attack surface means fewer opportunities for scammers.

Standard Operating Procedure (SOP)

A set of step-by-step instructions to help achieve a desired outcome.

A clear SOP helps reinforce good security practices.

Link Verification

The process of checking the authenticity of a URL.

Verifying links can prevent falling victim to phishing scams.

Permissions

The rights granted to applications or users to access your information.

Reviewing permissions helps protect your data and assets.

Reward Hook

A tactic that offers something desirable to manipulate behavior.

Being aware of these hooks can prevent you from falling for scams.

Irreversible

A state that cannot be undone.

Being aware of transaction finality can prevent costly mistakes.

Security Stack

A combination of tools and practices to enhance security.

A strong security stack is essential for safe trading.

Verification

The process of confirming the authenticity of information or requests.

Good verification habits are essential for security.

Social Engineering

Manipulative tactics used to deceive individuals into providing information.

Awareness is key to preventing social engineering scams.

Custody Hygiene

Practices for securely managing digital assets.

Implementing strong custody hygiene can prevent asset loss.

> **Scam**
>
> A fraudulent scheme designed to deceive individuals for financial gain.
>
> *Recognizing scams can help you avoid significant losses.*

> **Finality**
>
> The irreversible state of a completed transaction.
>
> *Understanding finality helps you make informed decisions before executing transactions.*

Self-Test Quiz

1. What is phishing?

A. A type of investment strategy

B. A fraudulent attempt to obtain sensitive information ✓

C. A method of secure communication

D. A type of cryptocurrency

Explanation: Phishing is a fraudulent attempt to obtain sensitive information by disguising as a trustworthy source.

2. What does custody refer to in the context of digital assets?

A. The process of trading assets

B. The responsibility for safeguarding assets ✓

C. The act of buying and selling cryptocurrencies

D. The management of investment portfolios

Explanation: Custody refers to the responsibility for safeguarding assets.

3. What is the purpose of two-factor authentication (2FA)?

A. To simplify password management

B. To provide an extra layer of security ✓

C. To eliminate the need for passwords

D. To track user activity

Explanation: 2FA provides an extra layer of security by requiring a second form of verification.

4. Why is it important to verify links before clicking?

A. To avoid phishing scams ✓

B. To increase internet speed

C. To enhance user experience

D. To reduce data usage

Explanation: Verifying links can prevent falling victim to phishing scams.

5. What is an incident response plan?

A. A strategy for managing investments

B. A documented strategy for responding to security incidents ✓

C. A method for trading cryptocurrencies

D. A plan for financial growth

Explanation: An incident response plan is a documented strategy for responding to security incidents.

6. What does reducing your attack surface mean?

A. Minimizing vulnerabilities ✓

B. Increasing exposure to threats

C. Enhancing trading strategies

D. Expanding your network

Explanation: Reducing your attack surface means minimizing vulnerabilities.

7. What is a reward hook?

A. A tactic that offers something desirable to manipulate behavior ✓

B. A method for securing accounts

C. A type of phishing attack

D. A strategy for trading

Explanation: A reward hook is a tactic that offers something desirable to manipulate behavior.

8. What is the main purpose of a personal security SOP?

A. To outline your security practices ✓

B. To track your investments

C. To manage your trading portfolio

D. To increase profits

Explanation: A personal security SOP outlines your security practices and protocols.

9. What does transaction finality mean?

A. The ability to reverse a transaction

B. The irreversible state of a completed transaction ✓

C. The process of confirming a transaction

D. The time it takes to complete a transaction

Explanation: Transaction finality refers to the irreversible state of a completed transaction.

10. Why is it important to regularly test your incident response plan?

A. To ensure it remains effective ✓

B. To increase your security risks

C. To reduce your response time

D. To enhance your trading skills

Explanation: Regularly testing your incident response plan ensures its effectiveness.

11. What is the purpose of a password manager?

A. To store and generate strong passwords securely ✓

B. To track your investments

C. To manage your trading portfolio

D. To enhance your trading strategies

Explanation: A password manager helps store and generate strong passwords securely.

12. What should you do if you suspect a phishing attempt?

A. Ignore it and move on

B. Report it to the relevant authorities ✓

C. Click the link to verify

D. Share it with friends

Explanation: If you suspect a phishing attempt, report it to the relevant authorities.

13. What is the best practice for managing permissions for applications?

A. Grant all permissions to avoid issues

B. Review permissions before granting access ✓

C. Ignore permission requests

D. Only grant permissions to trusted applications

Explanation: Reviewing permissions before granting access helps protect your data and assets.

14. What is the significance of understanding custody hygiene?

A. It helps in trading strategies

B. It prevents asset loss through secure management ✓

C. It increases investment returns

D. It simplifies trading processes

Explanation: Understanding custody hygiene helps prevent asset loss through secure management.

15. What should you do before executing a transaction?

A. Double-check transaction details ✓

B. Ignore the details and proceed

C. Rely on others to verify

D. Only check the amount

Explanation: Double-checking transaction details before execution can prevent costly mistakes.