Artificial Intelligence and Fraud | Worksheet

Matching
Match the definition in Column A with the term in Column B.

Column A

_____ Fraudulent attempts to steal personal information online.
_____ Scams promoting false or misleading investment opportunities.
_____ Machine-based system performing human-like tasks.
_____ Confirming the accuracy or authenticity of information.
_____ Replicating someone's voice using artificial intelligence.

Column B
a. Artificial Intelligence
b. AI Voice Cloning
c. Phishing
d. Investment Fraud
e. Verification

Multiple Choice

1. **Which of the following is a common tactic used in AI voice cloning scams?**
    a. Sending emails with poor grammar
    b. Using a cloned voice to create urgency
    c. Offering free gifts for clicking a link
    d. Asking for personal information through an online form

2. **AI-enhanced phishing emails are particularly dangerous because:**
    a. They can mimic the tone and style of legitimate messages.
    b. They are always sent by real companies.
    c. They often contain obvious spelling errors.
    d. They are usually sent to a large group of people.

3. **Why should you be cautious about investment opportunities that promise high returns with low risk?**
    a. They are always legitimate and trustworthy.
    b. They may use AI to guarantee profits.
    c. They are generally offered by well-known banks.
    d. They could be scams making false claims.

4. **What is the best first step to take if you receive an unexpected call or email asking for money?**
    a. Send the money immediately to help the person.
    b. Verify the request by contacting the person or institution directly.
    c. Ignore the message completely.
    d. Share the message on social media to warn others.

Application
Imagine you receive a voicemail from someone who sounds exactly like a close family member, urgently asking for money because they've been in an accident. What steps would you take to determine if the request is legitimate, and how would you respond? Explain your reasoning.

Scan to watch episode:

Artificial Intelligence | Answer Key

Matching

Match the definition in Column A with the term in Column B.

Column A
c. Fraudulent attempts to steal personal information online.
d. Scams promoting false or misleading investment opportunities.
a. Machine-based system performing human-like tasks.
e. Confirming the accuracy or authenticity of information.
b. Replicating someone's voice using artificial intelligence.

Column B
a. Artificial Intelligence
b. AI Voice Cloning
c. Phishing
d. Investment Fraud
e. Verification

Multiple Choice

1. **Which of the following is a common tactic used in AI voice cloning scams?**
   a. Sending emails with poor grammar
   b. Using a cloned voice to create urgency
   c. Offering free gifts for clicking a link
   d. Asking for personal information through an online form

2. **AI-enhanced phishing emails are particularly dangerous because:**
   a. They can mimic the tone and style of legitimate messages.
   b. They are always sent by real companies.
   c. They often contain obvious spelling errors.
   d. They are usually sent to a large group of people.

3. **Why should you be cautious about investment opportunities that promise high returns with low risk?**
   a. They are always legitimate and trustworthy.
   b. They may use AI to guarantee profits.
   c. They are generally offered by well-known banks.
   d. They could be scams making false claims.

4. **What is the best first step to take if you receive an unexpected call or email asking for money?**
   a. Send the money immediately to help the person.
   b. Verify the request by contacting the person or institution directly.
   c. Ignore the message completely.
   d. Share the message on social media to warn others.

Application

(Responses may vary.) Here is a sample response:

If I received a voicemail from someone who sounds like a close family member urgently asking for money, my first step would be to stay calm and not act immediately. I would contact the family member directly using a phone number I know is theirs to verify the situation. If I can't reach them, I would reach out to other family members or friends to confirm their safety. By verifying the information through trusted sources, I can ensure I'm not falling victim to a scam before taking any action.