

## **Teaching Topic: Risks in Cyberspace - Online Scams and Deepfake**

### **Introduction**

Along with the rapid development of technology, criminals begin to commit crimes by various means with the aid of technology. This lesson plan aims at helping teachers to explain to students at class the common risks of online scam, such as “bounced-cheque party” and deepfake technology, so as to enhance their alertness and crime-prevention awareness.

<b>Part 1: Youth Crime Prevention Video</b>	<b>Key Messages</b>
<p>Play the video concerning Risks in Cyberspace - Online Scams and then guide students to discuss.</p> <p>Questions for discussion:</p> <ul style="list-style-type: none"><li>● Which two kinds of scam are mentioned in the video? (e-shopping fraud and “bounced-cheque party” scam)</li><li>● Why would the subjects in the two video stories fall prey to the scams?</li><li>● In face of the scams, how should the subjects respond?</li><li>● How should we respond if we have unluckily fallen prey to a scam?</li></ul>	<ul style="list-style-type: none"><li>● Guide students to enter the characters in the video and rethink why the subjects would fall prey to the scams, so as to understand the modus operandi of online scams and learn how to avoid falling prey to online traps</li></ul>

<b>Part 2: Analysing News Reports</b>	<b>Key Messages</b>
<p>Teacher may present news reports of online scam cases, explain to students the modus operandi of scammers and then guide them to discuss the following questions:</p> <ul style="list-style-type: none"><li>● According to the above two cases, why would youngsters take part in scam activities? What rewards will they receive for participating in the scam activities? What are the liabilities?</li><li>● Will you commit a crime for a reward and then lead a penitential life?</li></ul>	<ul style="list-style-type: none"><li>● Help students to learn the serious consequences of taking part in scam activities, thereby understanding that the gain from committing a crime will certainly be outweighed by the loss</li></ul>

<p>Conclusion: Do not take that you will be given a light sentence because you are a “minor”. The consequences of committing a criminal offence are very serious. Therefore, all of you should learn to protect yourselves and avoid being tempted by criminals!</p>	
--	--

<b>Part 3: How does “deepfake” constitute a scam?</b>	<b>Key Messages</b>
<p>First of all, teacher may give an account of the meaning of “deepfake” techniques. After that, teacher may quote some precedents to explain how deepfake technology have facilitated scams, thereby reminding students to stay alert at all times when receiving or handling any forms of information.</p> <p>References:</p> <ul style="list-style-type: none"> <li>● “Deepfake” refers to the use of deep learning (namely a technique of artificial intelligence (AI)) to synthesise images for the purpose of creating falsified images. The Police have previously noticed a new online deception tactic that involves the use of deepfake technology to impersonate government officials or celebrities for promoting suspicious investment products in fraudulent messages and videos.</li> <li>● In 2023, deepfake video clips were found circulated in the Internet. Scammers made use of deepfake technology to impersonate government officials or celebrities for promoting fictitious investment plan in forged videos. As requested by the Police, the online or social media platforms concerned had already removed those videos to prevent the public from being scammed.</li> </ul> <p>Lastly, teacher may guide students to discuss the following questions:</p>	<ul style="list-style-type: none"> <li>● Help students to understand the background of deepfake technology and its relation with AI</li> <li>● Share with students how criminals have made use of such technology to scam people</li> <li>● Let students know the possible impact on the community if such technology is applied in scam activities</li> </ul>

<ul style="list-style-type: none"> <li>● According to the above incidents, how did scammers make use of deepfake technology to scam people?</li> <li>● Deepfake technology may have a wide impact on the community, including the dissemination of fake news, theft of identity, etc. In your opinion, how would such technology affect public safety?</li> </ul>	
---	--

<b>Part 4: Conclusion</b>	
Use the “Three Don’ts” and “Three Requests” as the conclusion, and share with students the tips against scammers.	
<b>Three Don’ts</b>	<b>Three Requests</b>
Don’t trust information on the Internet easily.	Request assistance from friends, analyse the cause of the incident and judge whether the incidents are reasonable.
Don’t click unknown applications and links.	Request assistance from the elderly or teachers with rich life experience, and listen to their teachings and advices.
Don’t answer unknown calls.	Request assistance from the Police. Call the 24-hour “Anti-Scam Helpline 18222” for consultation. For emergency, call 999.
<p>Other anti-scam information:</p> <ul style="list-style-type: none"> <li>● Patronise reputable sellers, and opt to meet in person for the deal as far as possible.</li> <li>● Buy items through official channels as far as possible.</li> <li>● When selling items, do not take that a payment has been settled simply by the presentation of a deposit receipt. You should check your bank account carefully.</li> <li>● Stop the deal immediately if in doubt.</li> <li>● Make good use of “Scameter” to check the username, number, account for receiving funds, telephone number, e-mail address, website etc. of the platform, so as to assess the deception and cyber security risks.</li> </ul>	

# Part 1: Youth Crime Prevention Video

## Questions for discussion

- Which two kinds of scam are mentioned in the video?
- Why would the subjects in the two stories fall prey to the scams?
- In face of the scams, how should the subjects respond?
- How should we respond if we have unluckily fallen prey to a scam?

Ledger balance  $\neq$  Available Balance



## Part 2: Analysing News Reports

<p><b>Case I</b></p> <p><b>Police smashed “bounced-cheque party” and arrested 21 persons. A 17-year-old student was recruited to commit crime and eventually arrested for involvement in two cases.</b></p> <p>Crime syndicates recruited youngsters who were eager to seek “quick cash opportunities”. They needed to reveal themselves at work, such as depositing cheques and receiving money from victims face to face, and were eventually arrested by the Police.</p>	<p><b>Case II</b></p> <p><b>Two 16-year-old youngsters made false representations regarding payment with a view to deceiving a Pikachu playing card worth of HK\$10,000.</b></p> <p>The two claimed on online social media platforms that they intended to buy a Pikachu special edition playing card which was worth of HK\$10,000 and arranged to meet the victim for the deal.</p> <p>Upon transaction, they falsely claimed that payment had been made by cheque. Being unwary to the fraud, the victim checked his online banking record immediately and found the relevant cheque deposit record. He believed that the transaction was completed and did not realize until later that the cheque could not be honoured. By that time, the two youngsters could no longer be reached.</p>
---	--

## Questions for discussion

- According to the above two cases, why would youngsters take part in scam activities? What rewards will they receive for participating in the scam activities?
- Will you commit a crime for a reward and then lead a penitential life?

Do not take that you will be given a light sentence because you are a “minor”. The consequences of committing a criminal offence are very serious. Therefore, all of you should learn to protect yourselves and avoid being tempted by criminals!

## Part 3: How does “deepfake” constitute a scam?

Online investment  
scams adopting  
“deepfake” technology



- According to the above incident, how did scammers make use of deepfake technology to scam people?
- Deepfake technology may have a wide impact on the community, including the dissemination of fake news, theft of identity, etc. In your opinion, how would such technology affect public safety?

## Conclusion: Tips Against Scammers

<b>Three Don'ts</b>	<b>Three Requests</b>
Don't trust information on the Internet easily.	Request assistance from friends, analyse the cause of the incident and judge whether the incidents are reasonable.
Don't click unknown applications and links.	Request assistance from the elderly or teachers with rich life experience, and listen to their teachings and advices.
Don't answer unknown calls.	Request assistance from the Police. Call the 24-hour "Anti-Scam Helpline 18222" for consultation. For emergency, call 999.