Aim: • Learn about types and countermeasures for financial cybercrimes.

Answers

Saitama Prefectural Police Cyber Bureau

Crime Prevention

Stay Safe from Online Crimes

Financial Crime

Grade: Class: Student No.:

Name:

Points:

1 This question is about financial crimes on the internet. Draw a line to match the description in ☐ with ☐.

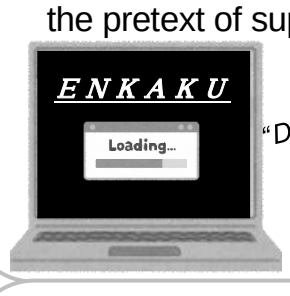
(5pts x 4 = 20pts)

Opening an online bank account using someone else's or fake identity, or for the purpose of selling it to another person.	Phishing
Illegally withdrawing or transferring funds from someone else's bank account.	Illegal Account Opening
Sending emails or social-media messages and directing people to fake websites to steal personal information and bank account details.	Fake Online Store
Pretending to be a real online shop or brand and stealing money from fake sales.	Unauthorized Transaction

2 Arrange the sequence of events in this tech support scam, where the scammer tricks the victim into paying for fake virus removal.

(5pts x 4 = 20pts)

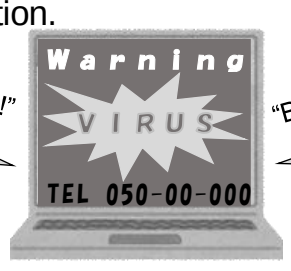
A. The victim installs remote-access software under the pretext of support.



"Downloading now!"

B. Fake popup alert appears, claiming a virus infection.

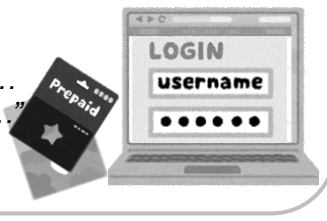
"Beep!"



"Beep!"

C. The victim is required to buy prepaid cards or enter bank account details.

"¥50K twice… That's a lot…"



D. The victim calls the number displayed on the screen.

"Hello. This is the support desk!"

"Hi, My computer is…"

Ⓑ ⇨ Ⓓ ⇨ Ⓐ ⇨ Ⓒ

3 Read the reactions to suspicious cases. In the ☐, mark "○" for correct responses, "×" for incorrect, and write an appropriate countermeasure for each case in the ___.

(☐=5pts x 6, ___=10pts x 3/ 60pts)

① **You received an email with the subject: "[Important] Request to Update Your Online Bank Account", containing a link to an update page.**

"Isn't this phishing? But you should still check the attached link just in case it's real and to avoid trouble."

"I heard that if you fall for phishing, your account will be hacked and money will be stolen!"

×

○

Example: Do not directly access the URL in the email. Set up spam filter.

② **You received a direct message (DM) on social media saying: "We will buy your internet banking ID and password."**

"You can give your ID and password as long as it's not for the account itself! Besides, you can just change the account holder information later!"

"The sender must be a criminal, so I can help the police catch them by replying to get their information!"

×

○

Example: Set your account so strangers cannot send DMs to you.

③ **A person claiming to be a police officer contacts you via social media video call, saying: "Your account has been misused. Please transfer the money through online banking for fund investigation."**

"If they show a police badge or an arrest warrant, or a prosecutor appears with them, it might be a real police officer!"

"Sometimes they tell you to take off your clothes to check your body — even real police are warning people not to follow such instructions."

×

○

Example: Call your nearest police station to confirm. (Police officers or prosecutors will never video-call individuals on their personal smartphones.)

Back

Aim: • Learn about types and countermeasures for financial cybercrimes.

Answers

Saitama Prefectural Police Cyber Bureau

Crime Prevention

Stay Safe from Online Crimes

Financial Crime

Grade: Class: Student No.:

Points:

4 **Read the following statements, and mark "O" if correct, and "×" if incorrect.** (5pts x 5 = 25pts)

① Phishing victims are mostly in their 50s, so people in their 20s and 30s don't need to worry as much. (×)

② Phishing methods evolve by incorporating social trends and become more sophisticated, so it's important to regularly research the latest techniques. (○)

③ You won't be a victim of fraud on Japanese language websites because they are authentic sites hosted on Japanese servers. (×)

④ Using system-based measures like multifactor authentication with one-time passwords completely eliminates the risk of un-authorized transfers or unauthorized access. (×)

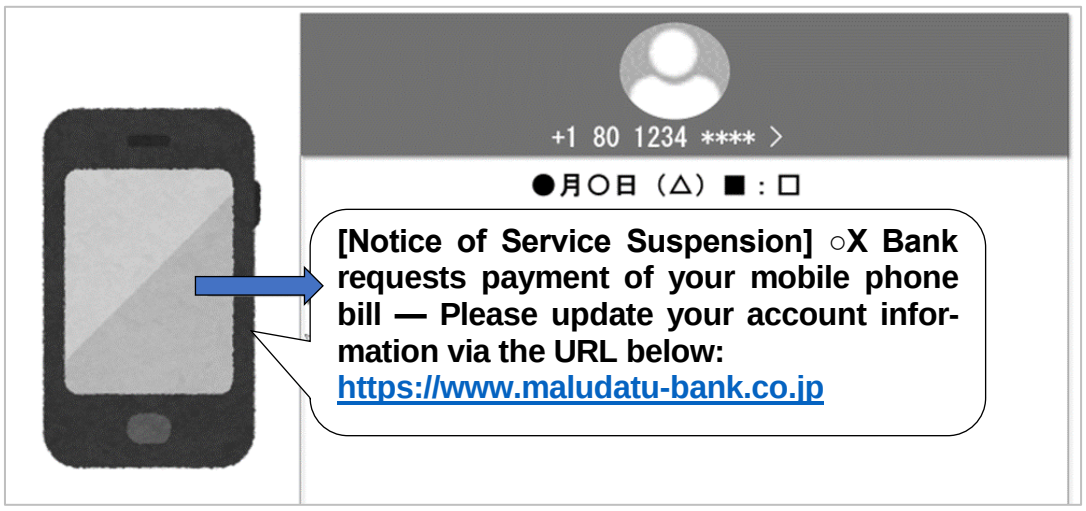
⑤ If someone steals money from your bank account, the bank might not give it back. So be careful of phishing emails and other types of scams – it's better to avoid the problem before it happens. (○)

5 **The figure below is an example of a phishing message (SMS):**

Q1) Explain why this email is suspicious.

Q2) Write what you know about phishing (such as different types).

(Q1=15pts, Q2=10pts)



Answer for Q1: (Example) The sender's phone number is from a foreign country, which seems suspicious. The URL shows 'maludatu' instead of the correct bank name, which is also strange. Banks would not contact customers about mobile phone bills.

Answer for Q2: (Example) Some phishing attacks use phone calls (voice phishing) or QR codes (quishing). Phishing emails come in many forms, including impersonating electric companies or delivery services.

To Protect Yourself from Cybercrime

- While the Internet enriches our lives, criminals are constantly exploiting new services and technologies for cybercrime.
- In addition to phishing and tech support scams covered in this test, there are other scams — such as side hustle scams or ticket scams via social media DMs — that are getting increasingly malicious and sophisticated. You need to be extra cautious. Also, getting involved in criminal activities through "Yami Baito" (illegal part-time jobs), such as buying or selling bank accounts, can seriously harm you and your family. Never participate in these activities.
- Today, smartphones are widely used across all ages, from elementary students to the elderly. To protect yourself from online threats, everyone must properly understand the risks and issues of the Internet. Let's stay interested in cybersecurity and use the Internet safely and securely.
- For more information about cybersecurity, please use the following websites, which include resources related to this cyber test.

Saitama Prefectural Police Website

Cyber Test: Check the answers here!

Official X account @spp_cyber