



POLICE NEWS RELEASE

CRIME ALERT: EMAIL PHISHING SCAMS AND EMAIL SCAMS REQUESTING FOR FINANCIAL ASSISTANCE

1. Police have noted an increase in the number of reported email scams where Internet users are deceived into revealing their email account information. The users' email accounts would then be taken over by the scammers and emails requesting for financial assistance would be sent to the victim's friends and relatives in the victim's name.

Modus Operandi

2. Typically, the victim would receive an email claimed to be sent from his email service provider. The victim is then led to believe that he is required to verify his user account information and email account password with the 'service provider', failing which his email account may be suspended or terminated. Once the victim unwittingly replies with his user information and password, the scammer would take over the email account and change the password to prevent access by the victim.

3. Using the victim's email account, the scammer would then send emails to the victim's email contacts, requesting for financial assistance. These emails, sent out in the victim's name, are intended to deceive the recipients into believing that the victim is stranded overseas e.g. robbed of his valuables, mobile phones, passports, uncontactable via any means other than email, and in urgent need of financial assistance. Typically, the scammers would also request for the money to be remitted urgently to an overseas account via remittance companies.

Crime Prevention Advisory

4. Police advise the public to be wary of such email phishing scams and email scams requesting for financial assistance:

i. No email service providers, banks, financial institutions, or companies would email their customers to reveal or verify their user account information, passwords and / or PIN over the Internet for security reasons. If users receive such emails, they ought to be careful and not respond by clicking on any URL link or opening any file attachments inside the email.

ii. When in doubt about of the genuinity of any information in the 'phishing' email, customers should contact the relevant email service providers, banks, financial institutions or companies for verification. No one should ever release their highly confidential information, such as user account id, password, PIN and credit card details to anyone over email.

iii. Should the public receive any emails from their friends or relatives claiming that they are stranded overseas and requesting for money to be remitted to them, attempt to contact the person in question to verify his whereabouts and authenticate the email request. Should the person be uncontactable via phone, the public should verify the authenticity of the sender by posing some personal questions via email.

5. More details of other scam tactics and the relevant crime prevention advisories can be found at the Singapore Police Force website at www.spf.gov.sg or the Commercial Affairs Department website at www.cad.gov.sg.

**PUBLIC AFFAIRS DEPARTMENT
SINGAPORE POLICE FORCE
29 JANUARY 2010 @ 4.00pm**