

Hong Kong Monetary Authority
Demystifying a Phishing email – Animation Video

Ambassador Kim Demystifying an Online Scam for You

SUPER: Ambassador Kim demystifies an online scam for you

Kim: Ambassador Kim demystifies an online scam for you

SUPER: “Never be deceived!” Smart Sam

Sam: Oh, a bank email!

SUPER: “Get you for sure!” Mr Phisher

Phisher: Dear customers, to strengthen our Internet banking’s security controls, please visit the following website to activate your multi-factor authentication (MFA)
Customers’ accounts without MFA protection will be suspended for funds transfer service

Sam: What? If funds transfer service is suspended, it will be a real hassle!
I need to deal with this immediately

Kim: Wait! This email is highly suspicious!

SUPER: Cybersecurity Ambassador Mr Kim

Sam: Obviously it’s an email from my bank
What’s wrong with it?
By the way, you look more suspicious than this email!

Kim: Hey kid, you’re too naïve
There are many questionable points in this email
Even though the sender and hyperlink appear to be legitimate, the email might still be a phishing email created by swindlers!

SUPER: Phishing emails

Kim: Phishing emails usually use what seems to be a reasonable excuse to lure the email recipients to click the hyperlinks or open the attachments

SUPER: Notification of a huge amount of fund transfer
Activation of a new security function

Kim: For example, notifying you a huge amount of fund transfer in your account, or asking you to activate a new security function, otherwise banking services will be suspended
All these are tricks commonly used by swindlers

Sam: Like my email here?

Kim: Exactly!

Sam: Hmm, so you want to trick me

Phisher: No! No!

Kim: Let's look at this hyperlink
It looks authentic
But actually it links to a fraudulent bank website which will be used to steal your online banking user name, password, and other information

SUPER: Open attachments will cause virus infection to your computer or smartphone

Kim: Swindlers will also lure you to download and open the email attachments which contain viruses that will infect your computer or smartphone
These viruses can record the personal information you enter into your computer or smartphone

Phisher: And when that happens, your money will become mine! Haha!

Sam: Oh no! So, how can I protect myself?

Kim: Generally speaking, banks rarely take the initiative to ask customers for personal information, or request customers to click hyperlinks to update personal information
If you have doubt, definitely don't click the hyperlinks or open the attachments


SUPER: Call bank customer service hotline to verify the email authenticity

Kim: Simply contact your bank's customer service hotline to verify the email authenticity
In this way, the swindlers can't get anything from you

Kim: Never forget!

SUPER: Phishing emails might look real
Handle hyperlinks and attachments with care!

Kim: Phishing emails might look real
Handle hyperlinks and attachments with care!

SUPER: 
www.hkma.gov.hk/cybersecurity