

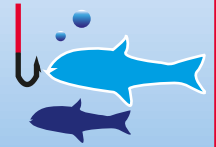
# HOW TO PROTECT YOURSELF AGAINST PHISHING



## What is Phishing?

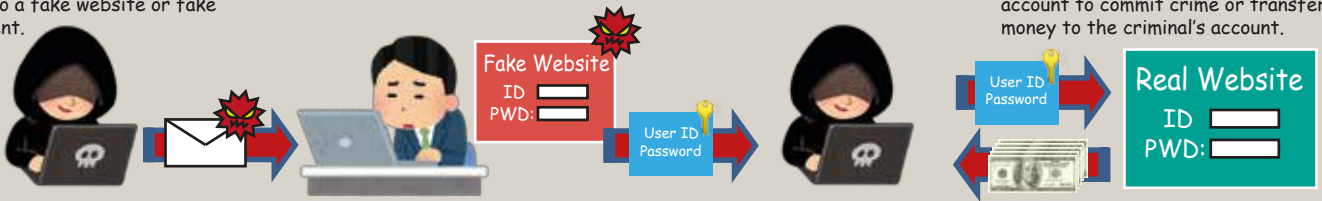
Phishing is the method to steal personal or sensitive information by pretending to be an email from or a website of a trusted organization. Recently, most of the phishing are aiming to steal the user ID and password for internet banking in order to gain access to the victim's account to commit the financial crime

As a result, it is important to protect your organization from phishing. In this document, Mizuho Bank, Ltd., Bangkok Branch would like to introduce some tips on how you can save your organization from being a phishing victim.



## How does the phishing work?

1. The criminal will send fake e-mail that looks like it comes from a bank to the victim. The e-mail contains the link to a fake website or fake attachment.
2. The victim opens the link and login to the fake website, or open the attachment that contains malware.
3. The fake website or malware will capture user ID and password and sends them to the criminal.
4. The criminal will use the victims' user ID and password to login to the real website and gain access to the victim's account to commit crime or transfer money to the criminal's account.



## How do you protect yourself against phishing?

xxx@mizuho-cb.com

xxx@m1zuh0-cb.com

**1. Carefully check the sender's address.**  
Some of fake e-mail use the address with similar spelling that or similar addresses. If you are not sure, contact the sender before opening an e-mail.

Please follow the link below and login to your account and renew your account information

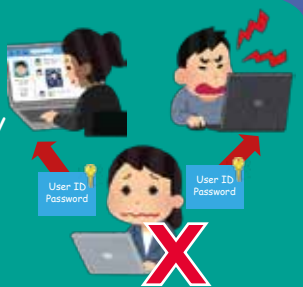
<https://www.paypal.com/cgi-bin/webscr?cmd=login-run>

Sincerely,  
Paypal customer department <http://66.160.154.156/catalog/paypal/>

**2. Don't open the link or attachment from unknown e-mail.** Since links contained in phishing mail are fake or may contain malware that steal your information, please check before clicking.

**3. Don't share your ID or password to anyone.**

The bank does not have a policy to ask for customer's user ID or password. Please keep your user ID and password secret.



**4. Install anti-malware software and keep it up-to-date.**

Anti-malware will help protecting against the malware from stealing your information such as your user ID or password from your PC.



**5. If you received the e-mail that you suspects it to be phishing mail, delete the mail immediately without open the link. If you are not sure, please contact the sender before opening the link.**

