Security Alert

At AmBank, we are always concerned about your online banking safety. Kindly be reminded to take necessary precautions in safekeeping your computers and mobile devices from malwares, viruses and trojans. Only perform AmOnline related activities or any transactions if you have logged directly onto the website and sighted the security icon and phrase.

Rest assured that AmOnline is safe for your usage and we will always guarantee the security of your information in our system. Keep yourself updated with the latest online security alerts and advisories at www.mycert.org.my.

3 Most Common Types of e-Banking Scams

Email Scam

An email scam is a type of scam more widely known as ‘phishing‘. An email scam involves a fraudster randomly sending forged emails purportedly from financial institutions or publicly known organisations to lure victims into revealing their internet banking login credentials, email credentials, credit card numbers, bank account numbers and/or passwords which are then used to perform transactions not authorised by the victims.

These emails are designed to appear legitimate to gain the trust of the recipient. The content of the email typically attempts to inflict a sense of urgency and panic in order to trick customers into revealing confidential information on a fake website/popup.

To know how to protect yourself against Email scams, click here.

Phone Scam

In such cases, the fraudster usually attempts to obtain sensitive information over a voice call. The fraudster normally tries to gain the victim’s trust by impersonating a credible individual such as a banking authority or a police investigation officer. Victims may not verify the received calls purportedly made by such persons thinking that the calls are from regulators so called, to avoid embarrassment or as a result of “warnings” given by the “officer.

SMS Scam

A SMS scam usually involves SMS-es initiated by a fraudster to trick victims into believing that they have won a contest/reward and which attempt to lead them into compromising their banking information and/or create an internet banking facility without the victim even realising it.

This type of scam may also involve ‘identity theft’ since an unauthorised person usually pretends to be a valid account holder and accesses the customer’s account (usually through the internet), unbeknown to the account holder.

Fake phone calls/SMS have been on the rise whereby scammers would trick customers into revealing their confidential banking credentials (such as login ID/password/TAC number/NRIC/ ATM Card Number/ ATM PIN, etc) by following given instructions.We would like to kindly remind you NOT to entertain such requests.

To know how to protect yourself against Phone/SMS scams, please read the below notices.

Notice from Bank Negara.

Notice from PDRM