EXIM Thailand Alerts Thai Entrepreneurs of Cybercrime Risks

Mr. Pisit Serewiwattana, President of Export-Import Bank of Thailand (EXIM Thailand), said that over the past few years, an increasing number of Thai entrepreneurs, particularly SMEs, engaging in e-commerce have encountered damage caused by a fast-growing cyber menace, seen by a jump in fraudulent transactions such as emails being hacked to masquerade the hackers as an international supplier reaching out to the Thai importers. These Thai importers, on the other hand, will be completely unaware that they are in fact corresponding with a hacker and that their emails are being hacked. When opportunities arise, these hackers will then transform themselves into a trading partner forging changes to the claims on existing trading contracts, substituting the hackers' financial accounts for the actual suppliers'. Meanwhile, the Thai entrepreneurs' email accounts will be blocked and prevented from contacting the actual trading partners directly. The victims' realization of such a forgery will come only too late, with financial losses almost always impossible to recover.

EXIM Thailand President said that cybercrimes can happen to both exporters and importers, particularly SMEs whose computer systems can be hacked more easily than those of large corporates that can better protect their computer systems. Cyberattacks target SMEs and small transaction amounts of about 5,000-50,000 US dollars. From 2015 to present, EXIM Thailand has encountered cyber attack cases and been able to help protect a number of its clients from cyber criminals, mostly from their trade with Asian counterparts in Malaysia, Singapore, South Korea, India, Taiwan and China. Cyber frauds which have been detected included advice of money transfer to countries, towns or persons other than the trading partners, request to change details of money transfer or bank accounts. If these abnormalities are not detected or money transfer cancelled in time, once the money has been funneled to the hackers' accounts, the chance to recoup the lost funds is very slim. Apart from careful precautions of the above incidents, Thai entrepreneurs are advised to contact their trading partners via methods other than emails such as telephone, facsimile etc. as well as setting strong or hard-to-guess passwords and changing passwords frequently. When logging in to an email account, be sure to check that it is the correct URL before filling in the passwords. Never use corporate email accounts to log in to a public website that may not be credible. Business email accounts should be kept separate from personal emails used in day-to-day correspondences while constantly making prudent observation for any abnormalities in business contacts.

/2

"Modern e-commerce relies on email for convenience, speed, and cost savings. This expediency, on the other hand, becomes an invisible trap often catching the unsuspecting Thai entrepreneurs off guard, who are led to take the hackers as genuine trading partners. These hackers will, in turn, take the opportunity to forge payment instructions. Thus, a safer way for the Thai entrepreneurs would be to always try to contact their partners via an alternative channel, prior to finalizing their payment instructions. In addition to keeping informed of the latest developments in modern e-commerce, the entrepreneurs may also solicit advices from financial institutions such as EXIM Thailand to mitigate international trade risks," said Mr. Pisit.

September 12, 2018
Corporate Communication Division
Secretary and Corporate Communication Department

For further information, please contact Corporate Communication Division, Secretary and Corporate Communication Department
Tel. 0 2271 3700, 0 2278 0047, 0 2617 2111 ext. 1141, 1144