SCB ไทยพาณิชย์

Alert Warning! Trojan / Spyware

attempting to steal your personal information

Fraud websites and e-mails that seek to steal personal information are spreading extensively on online systems. To protect against potential threats, immediately change your SCB Business Net password if you suspect that you may have conducted any transactions on a fake website received via a link in a scam e-mail.

It is important to note that SCB does not request personal information via website links.

What is a Trojan horse?

A Trojan horse, or Trojan, is a hacking program commonly disguised as an attached file in an e-mail message. The term is derived from the story of the Trojan Horse in Greek mythology, whereby a horse was presented to the Trojans as a harmless gift. When night fell, Greek soldiers hidden in the horse came out to open a city gate, allowing the Greek army to easily attack the Trojan city of Troy. Trojan viruses work in the same way. Hackers send them to victims who then unwittingly install them on their computers so they can steal information.

How does a Trojan virus work on your computer?

Unlike other viruses that tend to destroy both the hardware and software of your computer, Trojans do not seek to destroy or damage your computer. Because a Trojan is just a computer program, it is difficult to be captured by virus protection software. Trojans are used by hackers to penetrate systems and detect and record keyboard strokes, enabling them to obtain your user ID and password. The Trojan will then record the information to RAM, CMOS, or a hidden directory on your hard disk and attempt to upload the program to a source targeted by hackers. Hackers will sometimes use other methods to store disguised files. Some Trojan programs can instruct other programs to run systems to destroy or change files.

Prevention

1. Beware of e-mail messages with suspicious contents or containing links that require you to fill in you user name or password. Do not click any link attached to a suspicious e-mail message. Immediately delete any such message, and call the SCB Business Net Call Center at 02-722-2222.

2. For your increased security, when performing financial transactions please type the website name and re-check before filling in your user name and password.

3. Do not disclose your user name and password to anyone. The Bank will never request your password through any banking channel.

4. Install reliable and copyrighted versions of anti-virus programs, always update to the latest version, and use the program to frequently scan your computer.

5. Erase suspicious e-mail messages and do not open any attached file sent from an unknown source or files send from chat programs, and do not download programs or data from unknown websites.