Information about specific risks associated with the use of electronic services as well as function and purpose of Thulium Agent software

Fulfilling obligation specified in Article 6 paragraph 1 of the Act of 18 July 2002 on providing electronic services ("Act"), Thulium LLC ("Thulium") informs about specific risks associated with using electronic services provided by Thulium.

The main risk Internet users face, users of electronic services including, is the possibility of infecting the electronic system by software devised to cause harm, in particular software like viruses, bugs or trojans. Irrespective of security measures implemented by Thulium, every Internet user has to protect their computer by means of installing and running anti-virus software with an up-to-date definition file and putting up a personal firewall. These elements shield the computer from dangers coming from the network. Correct browser settings are also essential. Commercial software provided by renowned companies which react quickly to potential new threats and offer technical support is recommended.

There is a whole range of attacks deploying phishing technique relying on attempts of taking over a password. These attacks are prevalent - potential victims receive e-mails containing a plea to log in to their accounts through the link mentioned in the e-mails. Links usually lead to faux websites of financial institutions. passwords are intercepted via forms, and later utilised by attackers to log in to victims' accounts.

To avoid risks associated with attacks of this kind it is best:

1. to remember that financial institutions do not send e-mails containing requests for submission of passwords to client accounts. Every single message like that should raise suspicion - it is advisable to contact a given institution and inform about the ensuing situation
2. not to click on links listed in that type of communication
3. not to send any bank account numbers, logins or passwords by e-mail
4. not to use faux websites of financial institutions lacking the HTTPS protocol in the location bar which demand logging in
5. to use anti-virus software with an up-to-date definition file and a personal firewall
6. to regularly update internet browsers, computer system and software (particularly of the anti-virus kind)

Our suggestions should be treated only as basic, general and always binding recommendations regarding security, which do not exhaust this vast subject.
Thulium, acting pursuant to Article 6 paragraph 2, informs that function and aim of software or data which are not an element of service contents, and which are introduced by Thulium into a teleinformation system used by the service recipient, have been defined in the privacy policy, available at thulium.io/termsofuse.