Informacja o szczególnych zagrożeniach związanych z korzystaniem przez Klientów z usług świadczonych drogą elektroniczną przez XTB S.A. oraz o funkcji i celu oprogramowania lub danych niebędących składnikami treści usług, wprowadzanych przez XTB S.A. do systemu teleinformatycznego.

XTB S.A. („XTB"), działając stosownie do art. 6 pkt 1. ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną („Ustawy"), informuje o szczególnych zagrożeniach związanych z korzystaniem przez użytkowników z usług świadczonych drogą elektroniczną przez XTB.

Podstawowym zagrożeniem każdego użytkownika Internetu, w tym osób korzystających z usług świadczonych drogą elektroniczną, jest możliwość zarażenia systemu teleinformatycznego przez różnego rodzaju oprogramowanie tworzone głównie w celu wyrządzania szkód, w szczególności takie oprogramowanie jak wirusy, robaki czy konie trojańskie. Bez względu na metody bezpieczeństwa stosowane przez XTB, każdy użytkownik Internetu musi dbać o bezpieczeństwo własnego komputera, poprzez stosowanie programu antywirusowego z aktualną bazą wirusów oraz osobistego firewall'a. Elementy te zabezpieczają komputer przed ingerencją niepożądanych akcji od strony sieci. Zasadnicze znaczenie ma również prawidłowe ustawienie przeglądarki internetowej. Konsekwentne stosowanie przez użytkownika podstawowych środków bezpieczeństwa pozwala uniknąć potencjalnych niebezpieczeństw związanych z korzystaniem z Internetu. Zalecane są programy komercyjne renomowanych producentów, zapewniających szybką reakcję na pojawiające się nowe zagrożenia oraz oferujących wsparcie techniczne. Alternatywnie możliwe jest użycie dostępnych w Internecie bezpłatnych programów antywirusowych. Po upewnieniu się, że w zasobach komputera nie znajduje się żadne niebezpieczeństwo, należy koniecznie zmienić hasło dostępu do serwisu transakcyjnego.

Istnieje cała gama ataków opierających się na technice „phishing" polegającej na próbie wyłudzenia haseł. Ataki te są bardzo popularne – potencjalne ofiary otrzymują listy elektroniczne z prośbą o zalogowanie się do swoich kont pod linkiem podanym w wiadomości. Linki z reguły prowadzą do sfałszowanych stron instytucji finansowych, a podane hasła są przechwytywane z formularzy, a następnie wykorzystywane przez atakującego do zalogowania się do faktycznych kont ofiar.

Aby uniknąć ryzyk związanych z tego typu atakami należy przede wszystkim:

a) Pamiętać, że instytucje finansowe nie wysyłają wiadomości elektronicznych z prośbą o podanie haseł do kont klienckich. Każda taka wiadomość powinna wzbudzić podejrzliwość adresata – wskazane jest wówczas skontaktowanie się z daną instytucją i poinformowanie o zaistniałej sytuacji;
b) nie należy otwierać stron podanych w linkach w tego typu informacjach;
c) nie należy przesyłać mailowo żadnych numerów kont, loginów i haseł;
d) nie należy korzystać z rzekomych stron instytucji finansowych, które nie zawierają w adresie nazwy protokołu HTTPS a wymagają zalogowania;
e) należy stosować program antywirusowy z aktualną bazą wirusów oraz osobisty firewall;
f) Należy regularnie aktualizować używane przeglądarki internetowe, system oraz oprogramowanie (w szczególności antywirusowe). Nasze sugestie należy traktować jedynie jako ogólne, zawsze obowiązujące, podstawowe zalecenia z zakresu bezpieczeństwa, które nie wyczerpują tego obszernego tematu.

XTB, działając stosownie do art. 6 pkt 2. Ustawy, informuje, że funkcja i cel oprogramowania lub danych niebędących składnikiem treści usług wprowadzanych przez XTB do systemu teleinformatycznego, którym posługuje się użytkownik określone zostały w Polityce prywatności, zamieszczonej na stronie internetowej XTB.

XTB S.A.
ul. Prosta 67
00-838 Warszawa

+48 222 019 905
biuro@xtb.pl

www.xtb.com/pl