Nowe zagrożenie w Internecie – Phishing - Wyłudzenie danych

W ostatnich dniach odnotowaliśmy próby wyłudzenia danych logowania do bankowości internetowej ING BankOnLine za pośrednictwem fałszywej strony przypominającej stronę ING Banku Śląskiego

Nasi Klienci mogą otrzymać e-mail z informacją o nowej wiadomości pochodzącej z Banku. W wiadomości podany jest link do fałszywej strony zrobionej na wzór oryginalnej strony ING Banku Śląskiego. Wiadomość zachęca do wejścia na tę stronę i zalogowania się do systemu ING BankOnLine.W ten sposób można pozyskać Twój login i hasło dostępu.

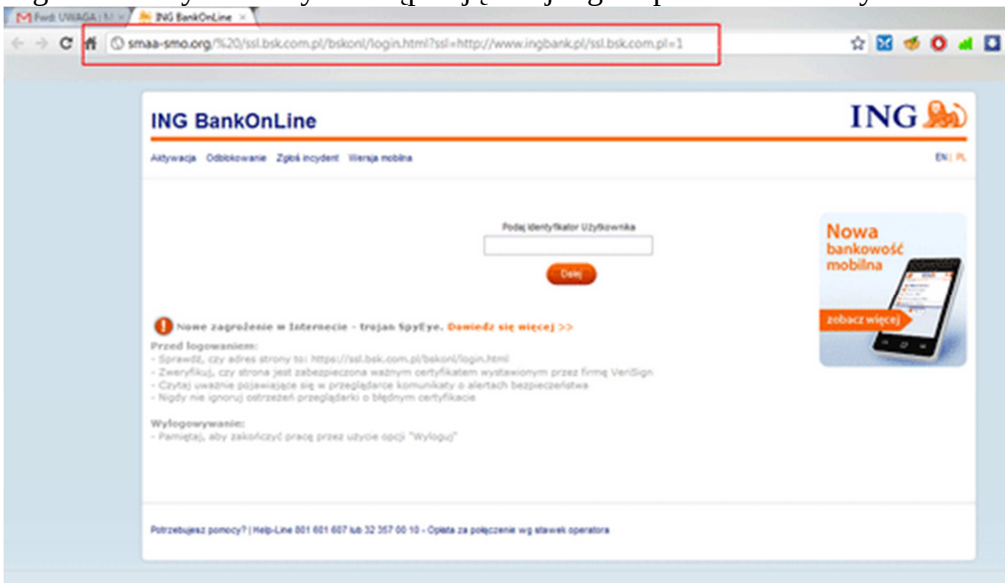
Pamiętaj! Bank nigdy nie prosi o podanie **pełnego hasła dostępu!**

Jak to wygląda?

Przykładowa wiadomość:

Od: ING Bank <suppinf@ingbank.pl>
Data: 21 listopada 2011 10:01:47 CET
Do:
Temat: UWAGA : Masz 1 nowa wiadomosc!

Link podany w wiadomości przekierowuje na fałszywą stronę www, na której nieświadomi zagrożenia użytkownicy udostępniają swój login i pełne hasło do systemu ING BankOnLine!



Jak rozpoznać fałszywą stronę?

Fałszywa strona różni się od prawdziwej strony banku adresem www widocznym w górnym oknie przeglądarki.

Przykładowe adresy fałszywych stron:
hxxp://smaa-smo.org/%20/ssl.bsk.com.pl/bskonl/login.html
hxxp://thesaratogaapartments.com/%20/ssl.bsk.com.pl/bskonl/login.html?ssl=http://www.ingbank.pl/ssl.bsk.com.pl=1

Przypominamy:

Bank nigdy nie prosi o podanie pełnego hasła dostępu do systemu bankowości internetowej

Pamiętaj, aby zachować szczególną ostrożność otwierając linki w e-mailach, które otrzymujesz. W przypadku wątpliwości zweryfikuj autentyczność strony ING Banku Śląskiego. – **zobacz jak**

możesz to zrobić (link do http://www.ingbank.pl/indywidualni/bankowosc-elektroniczna/ing-bankonline/bezpieczenstwo/weryf-sciezki-certyfikacji)

Co powinieneś zrobić?

Każde podejrzenie phishingu powinno wzbudzić Twoją czujność i ostrożność oraz zostać zgłoszone konsultantowi Banku telefonicznie pod nr 801 601 607 (z telefonów stacjonarnych) lub (32) 357 00 10 (z telefonów stacjonarnych i komórkowych).