

# 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](mailto:suppinf@ingbank.pl)>  
Data: 21 listopada 2011 10:01:47 CET  
Do:   
Temat: UWAGA : Masz 1 nowa wiadomosc!



**UWAGA : Masz 1 nowa wiadomosc!**

Zaloguj : [ING BankOnLine](#)

**Dziękujemy za korzystanie z ING Bank !**

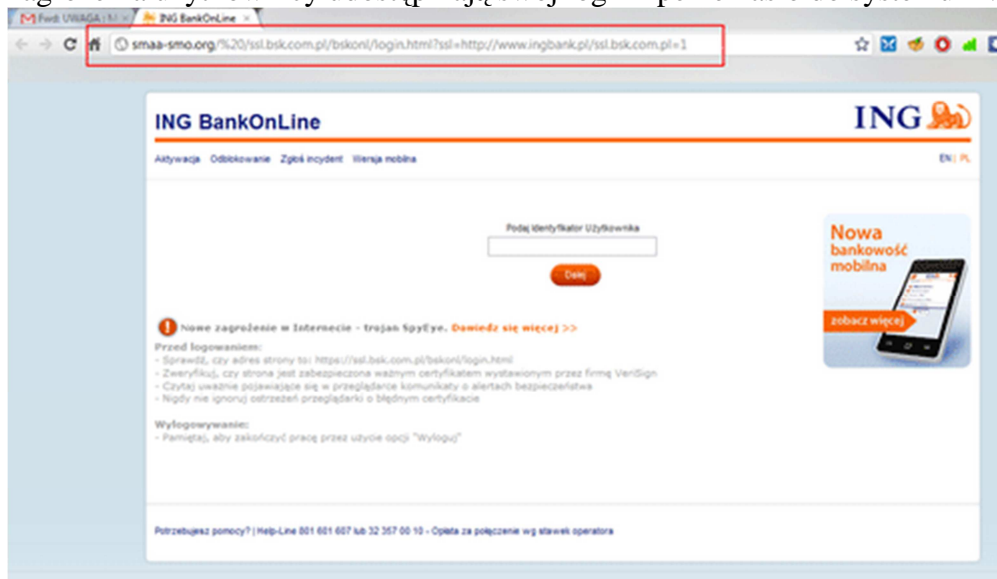
**ING BANK ŚLASKI**

---

2011 ING Bank Śląski S.A. Wszelkie prawa zastrzeżone. Korzystanie z serwisu oznacza akceptację.

Email ID: 469810

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



## ING BankOnLine

Aktywacja Odblokowanie Zgłoś incydent Wersja mobilna

Podaj hasło dla użytkownika

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32

Dalej

! Nowe zagrożenie w Internecie - trojan SpyEye. Dowiedz się więcej >>

### 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/%20ssl.bsk.com.pl/bskonl/login.html](http://smaa-smo.org/%20ssl.bsk.com.pl/bskonl/login.html)

[hxxp://thesaratogaapartments.com/%20ssl.bsk.com.pl/bskonl/login.html?ssl=http://www.ingbank.pl/ssl.bsk.com.pl=1](http://thesaratogaapartments.com/%20ssl.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).