

Mesaj anti-phishing

ING depune toate eforturile necesare pentru a asigura confidentialitatea datelor clientilor sai si a tranzactiilor acestora. Totusi, indiferent cate eforturi se depun la nivel global pentru securizarea datelor, cresc riscurile privind atacurile ilegale (phishing), atat online cat si prin alte mijloace, iar metodele de atac sunt din ce in ce mai sofisticate.

Prin acest mesaj dorim sa va oferim informatiile-cheie despre cum pot fi identificate tentativele de phishing si sa va informam cu privire la masurile pe care ING le-a luat pentru a evita astfel de atacuri.

Phishing-ul este un proces prin care clientii unei organizatii sunt determinati sa dezvaluie date personale sau confidentiale care ulterior sunt folosite ilegal pentru a efectua tranzactii in contul clientului respectiv. Atacurile de phishing pot fi realizate prin **e-mail**: un mesaj electronic este trimis clientilor, pretinzand a fi din partea unei surse legitime (banca) si prin care se solicita introducerea de date confidentiale intr-un link catre un site falsificat, indicat in textul mesajului. Atacul de tip phishing poate fi realizat si prin **telefon**: o persoana pretinde ca suna din partea bancii si, invocand probleme tehnice (de ex. in sistemul de plati), solicita informatii confidentiale cum sunt codul PIN, numarul contului, parola.

Datorita cresterii incidentei atacurilor de tip phishing la nivel global, ING Bank Romania a introdus o procedura standard anti-phishing care presupune un sistem complet de masuri preventive, de detectare si de raspuns. Prin acest sistem dorim sa ne asiguram ca toti clientii ING sunt in masura sa recunoasca si sa evite un atac de tip phishing.

Practica standard in domeniul Anti-Phishing consta in:

1. Masuri tehnice

- **Masuri de securizare a datelor si sisteme de avertizare**: detectarea in timp real a abuzului de identitate; inspectii ale mesajelor e-mail; sectiune de web dedicata clientilor pentru a raporta atacurile de tip phishing.
- **Aplicatii de internet securizate**: autentificarea multi-factor; securizarea browser-ului si a configuratiei e-mail-urilor; software impotriva furtului de identitate.

2. Masuri non-tehnice

- Informarea clientilor; comunicarea online; afisarea termenilor si conditiilor; aplicarea procedurii de raspuns in cazul incidentelor de tip phishing.

Practica standard ING Anti-Phishing mai include:

- ING va trimite intotdeauna un mesaj personalizat (care include numele Dvs.) atunci cand mesajul implica **informatii confidentiale**
- ING **nu va trimite niciodata** mesaje e-mail in care sa fie incluse link-uri catre site-uri unde Dvs. va trebui sa introduceti informatii personale
- ING **nu va solicita niciodata** sa confirmati detalii personale (de ex. numarul cardului, data la care expira, PIN-ul, parola) intr-un mesaj e-mail

- ING foloseste cele mai noi sisteme si tehnologii de criptare si autentificare pentru a securiza toate tranzactiile

Oricand aveti dubii cu privire la un mesaj e-mail pe care l-ati primit, pretinzand a fi din partea ING, va rog sa sunati la serviciul My'Line: 021 402 83 91 sau sa trimiteti un mesaj la contact@ingromania.ro.

Cu stima,

ING Bank N.V. Amsterdam, Sucursala Bucuresti