Jak rozpoznac phishing? 7 sygnalow ostrzegawczych

Praktyczny przewodnik po najczestszych technikach oszustow internetowych

Tomasz Grabowski · 09.11.2026

W czwartek rano Agnieszka ze Szczecina otworzyla e-mail od "banku". Wiadomosc mowila o problemach z jej kontem i prosila o klikniecie linku w celu weryfikacji danych. Wygladalo profesjonalnie, mialo nawet logo banku. Kliknela. Po trzech miesiacach odkryla, ze z jej konta zniknelo 4500 zlotych. Nie pamietala, kiedy doszlo do tego pierwszego klikniecia.

Historia Agnieszki to jedna z wielu. Raport Instytutu Badan Policyjna Polska z 2025 roku pokazuje, ze co czwarty uzytkownik Internetu w Polsce doswiadczyl proby phishingu w ostatnim roku. To nie jest problem marginalny - to jest problem kazdego, kto ma e-mail i konto bankowe online.

Phishing to technika oszustwa polegajaca na wysylaniu falszywych wiadomosci, ktore wygladaja jak pochodzace od zaufanych zrodel - bankow, sklepow, uslug pocztowych, mediow spolecznosciowych. Celem jest sklonienie cie do ujawnienia hasel, numerow kart, a nawet pesel-u. Dziala, bo oszusci sa coraz bardziej wyrafinowani.

Chociaz pracuje w branzy cyberbezpieczenstwa od dekady, widze, ze ludzie maja wrazenie, iz phishing to cos abstrakcyjnego. "Ja bym na to nie wpadl" - slysze to wciaz. Ale statystyki mowia inaczej. Sama Microsoft raportuje, ze phishing odpowiada za 90 procent wszystkich naruszen bezpieczenstwa. To nie jest kwestia inteligencji, ale edukacji i uwagi.

Sygnal 1: Nagly pospiech i grozby

Pierwszy i najczestszy trik to stworzenie paniki. E-mail mowi: "Twoje konto zostanie zablokowane za 24 godziny", "Wykrylismy podejrzana aktywnosc", "Natychmiast zweryfikuj swoje dane". Wszystko ma jeden cel - zmuszic cie do impulsywnego dzialania bez zastanowienia.

Poznalem to na wlasnej skorze. Kilka lat temu dostalem wiadomosc od "PayPal", ze moja platnosc nie powiodla sie i konto bedzie zamkniete. Powiedze szczerze - przez sekunde sie przestraszylem. Ale zaraz pomyslalem: czemu bank wysyla e-mail z takim tonem? Rzeczywiste instytucje sa ostrozne w komunikacji. Oszusci nie sa.

Obserwuj siebie, kiedy czytasz takie e-maile. Jesli czujesz pospiech, strach, potrzebe natychmiastowego dzialania - to pierwszy sygnal ostrzegawczy. Autentyczne banki i serwisy czekaja. Moga czekac godziny, dni. Phishingowe e-maile nie.

Konkretny przyklad: otrzymujesz wiadomosc, ze "Twoja subskrypcja Spotify wkrotce wygasnie". Tak naprawde mozesz zalogowac sie do Spotify bezposrednio (wpisujac adres w przegladarce) i sprawdzic stan konta. Nigdy nie klikaj linku z e-maila w takich sytuacjach.

Sygnal 2: Adres e-maila wysylajacego - maly szczegol, duza roznica

Tu zaczyna sie detektywistyka. Spojrz na adres e-maila, z ktorego przyszla wiadomosc.

Nie na nazwe wyswietlana (bo te mozna latwo sfalszowac), ale na faktyczny adres e-maila.

Jesli otrzymujesz e-mail "od banku", ale adres to cos w stylu support.bankname.service@gmail.com, to oszustwo. Zaden profesjonalny bank nie wysyla e-maili z konta Gmail. Wszyscy maja wlasne domeny.

Przyklady, ktore widzialem w szkoleniach:

- Falszywy: mbank-potwierdzenie@mbank.pl - prawie identyczny z prawdziwym, ale ostateczna czesc domeny to mbank.pl zamiast rzeczywistej
- Falszywy: support@amazonn.com - jedna litera zbyt wiele (dwie "n")
- Falszywy: verification-paypal@paypal-security.info - domena konczy sie na .info zamiast .com
- Prawdziwy: noreply@mbank.pl - zaden linkow do klikniecia, tylko informacja

Jak to sprawdzic? W Gmailu klikni na strzalke obok "Pokaz szczegoly" lub "Pokaz oryginalna wiadomosc". W Outlooku to "Akcje" > "Wyswietl wiadomosc". Zobaczysz dokladnie, skad przyszla wiadomosc.

Oszusci czasem zmieniaja serwer pocztowy, ale domena zawsze cos zdradza. Jesli wiadomosc rzekomo od mBanku, ale serwer to mbank-update@o2.pl, to falsz. mBank ma wlasne serwery.

Sygnal 3: Logi i linki - gdzie rzeczywiscie Cie kieruja

Nawet jesli e-mail wyglada profesjonalnie i ma logo banku, logo mozna skopiowac. Prawdziwa wskazowke daje link.

Nie klikaj od razu. Zamiast tego przesunac kursor myszy nad linkiem (bez klikania) i spojrz, gdzie rzeczywiscie Cie kieruje. W wiekszosci programow pocztowych pojawi sie podglad adresu docelowego. Moze to wygladac tak:

Wyswietlony tekst: "Kliknij tutaj aby zweryfikowac dane" Rzeczywisty URL: http://verify-your-bank-now.xyz/update?id=5f8d9c

Widac? Tekst mowi o banku, ale link kieruje na podejrzana strone z dziwnym adresem. To klasyczna taktyka phishingowa.

Dodatkowo zwroc uwage na:

- Czy adres zaczyna sie od https:// (bezpieczny) czy http:// (niezabezpieczony) - banki zawsze uzywaja https
- Czy w URL-u jest dziwne kodowanie, np. %2F zamiast /
- Czy domena rzeczywiscie nalezy do instytucji, ktora twierdzi, ze wysyla e-mail

Moja rada: jesli masz watpliwosci, nigdy nie klikaj linku z e-maila. Zamiast tego wpisz adres strony bezposrednio w przegladarce. Jesli chodzi o bank, otworz aplikacje mobilna lub wejdz na strone przez zakladki, ktore masz zapisane. To zajmie 30 sekund wiecej, ale bedzie bezpieczniej.

Sygnal 4: Bledy ortograficzne i dziwna gramatyka

Oszusci czesto pracuja szybko i z dala od Polski. Efekt? E-maile pelne bledow.

Rzeczywiste banki maja zespoly redakcyjne. Jesli otrzymasz e-mail od "PKO BP" z napisem

"Potwierdzic Twoje dane w ciagu 2 godzin", to juz dziwnie brzmi. PKO BP by napisal "Potwierdz swoje dane". Bledy gramatyczne to czerwona flaga.

Szukaj:

- Bledow ortograficznych - "Twoje konto zostal zablokowany"
- Dziwnych czasow gramatycznych - "Bank wysyla Ci wiadomosc"
- Zbyt oficjalnego lub zbyt swobodnego tonu - banki sa neutralne, phishingowe e-maile oscyluja miedzy tymi ekstremami
- Zmieszanych jezykow - np. polski slowo w angielskim zdaniu

Kiedy prowadzilem szkolenia dla pracownikow biura rachunkowego, pokazalem im kilka autentycznych e-maili od banku i kilka phishingowych. Wszyscy od razu wychwycili te drugie. Nie dlatego, ze byli geniuszami, ale dlatego, ze bledy byly oczywiste, gdy sie ich szukalo.

Sygnal 5: Prosby o dane, ktore zadna instytucja nie pyta

To moze byc najwazniejszy sygnal. Zapamietaj sobie prosta regule: zaden bank, zaden serwis, zadna instytucja nie prosi Cie o haslo, PIN czy PESEL przez e-mail.

Nigdy.

Jesli e-mail prosi o:

- Haslo do konta bankowego
- Numer karty kredytowej
- Kod CVV (trzy cyfry z tylu karty)
- PESEL
- Dane logowania do portalu

To jest phishing. Punkt.

Autentyczne instytucje wiedza, ze ty posiadasz te dane. Oni nigdy cie nie beda prosic o ich ujawnienie. To podstawowa zasada bezpieczenstwa. Jesli nawet strona wyglada identycznie jak serwis banku, ale prosi o haslo - to oszustwo.

Trafilem na przypadek, gdzie oszusci stworzyli strone, ktora byla praktycznie klona mBanku. Wszystko wygladalo profesjonalnie. Ale kiedy uzytkownik wpisal login i haslo, pojawil sie komunikat o bledzie, a nastepnie prosba o wpisanie kodow z karty graficznej. To byla wskazowka, ze cos jest nie tak - mBank nigdy nie prosi o wszystkie kody naraz.

Sygnal 6: Zalaczniki, ktore powinny cie zaniepokoic

Zalaczniki to paliwo phishingu. Oszusci wysylaja pliki z nazwami takimi jak "Potwierdzenie_transakcji.pdf" czy "Rachunek_2026.zip".

Nie otwieraj zalacznikow z e-maili, ktorych sie nie spodziewasz. Nawet jesli wydaja sie pochodzic od znanej osoby. Nawet jesli wiadomosc wyglada profesjonalnie.

Dlaczego? Zalacznik moze zawierac oprogramowanie zlosliwe (malware). Kiedy go otworzysz, malware zainstaluje sie na twoim komputerze lub telefonie. Od tego momentu, oszusci moga miec dostep do twoich danych.

Jak to wyglada praktycznie? Otrzymujesz e-mail "od Paczkomatu InPost" z informacja, ze

masz paczke do odebrania. W zalaczniku plik PDF. Klikasz, otwiera sie, ale zaraz pojawia sie komunikat o bledzie. Nic sie nie stalo, myslisz. Ale w tle, malware juz pracuje. Po kilku dniach odkrywasz, ze twoje hasla zostaly zmienione.

Zasada bezpiecznosci: jesli spodziewasz sie zalacznika (np. zamowiles cos i czekasz na fakture), sprawdz najpierw, czy e-mail jest autentyczny. Zrob to metoda z punktu drugiego - sprawdz adres nadawcy. Jesli wciaz masz watpliwosci, zaloguj sie do konta na stronie i pobierz dokument bezposrednio stamtad.

Sygnal 7: Brak personalizacji - ogolne pozdrowienia i adresy

Ostatni sygnal to brak personalizacji. Autentyczne wiadomosci od banku zawieraja twoje imie, numer konta, ostatnie cztery cyfry karty. Phishingowe e-maile mowia "Szanowny Panie/Pani" lub "Drogi Kliencie".

Dlaczego? Oszusci wysylaja masowo tysiace e-maili. Nie maja czasu na personalizacje. Banki maja dostep do twoich danych i je uzywaja.

Porownaj:

Pamietaj: personalizacja to koszt. Oszusci oszczedzaja na wszystkim. Jesli e-mail traktuje cie generycznie, to prawdopodobnie nie pochodzi od instytucji, w ktorej masz konto.

Co zrobic, jesli juz kliknales podejrzany link?

Nie panikuj. Klikniecie linku to jeszcze nie koniec swiata. Gorzej jest, jesli wpisales dane.

Wykonaj nastepujace kroki:

- Zamknij przegladarke - jesli link otworzyl sie w nowej karcie, zamknij ja. Nie klikaj nic wiecej na tej stronie
- Odlacz sie od Internetu - jesli chcesz byc ostrozny, odlacz WiFi na kilka minut. To uniemozliwi zlosliwemu oprogramowaniu wyslanie danych
- Sprawdz, czy wpisales dane - jesli nie wpisales hasla ani zadnych danych osobowych, jestes bezpieczny. Klikniecie linku samo w sobie zwykle nie stanowi zagrozenia
- Jesli wpisales haslo - zmien je natychmiast. Zaloguj sie bezposrednio na stronie (nie przez link z e-maila) i zmien haslo na nowe, silne
- Jesli wpisales dane karty - skontaktuj sie z bankiem. Powiedz, kiedy podejrzewasz, ze dane mogly byc skompromitowane. Bank moze zablokowac karte i wydac nowa
- Uruchom skaner antywirusowy - jesli obawiasz sie, ze kliknal cos niebezpiecznego, uruchom pelny skans komputera programem takim jak Windows Defender (wbudowany) lub Avast (darmowy)

Rzeczywisty scenariusz z mojej praktyki: ktos kliknal link, ale zaraz zdal sobie sprawe, ze to phishing. Strona nie zaladowala sie prawidlowo. Osoba natychmiast zamknela przegladarke, nic nie wpisala. Wynik? Nic sie nie stalo. Klikniecie linku bez wpisania danych to naprawde minimalne ryzyko.

Inny scenariusz: osoba wpisala login i haslo. Zaraz potem pojawil sie komunikat o

bledzie. Natychmiast zmienila haslo. Bank nie zaraportowal zadnych podejrzanych transakcji. Szybka reakcja uratowala jej konto.

Jak sie bronic - proaktywne kroki

Oprocz uczenia sie rozpoznawac phishing, mozesz podjac konkretne kroki, aby zredukowac ryzyko.

Najpierw: wlacz uwierzytelnianie dwuetapowe (2FA) na wszystkich waznych kontach. Nawet jesli oszust zdobedzie twoje haslo, nie bedzie mogl zalogowac sie bez drugiego kodu (z aplikacji jak Google Authenticator lub SMS-u). To zmienia cala gre.

Drugie: zainstaluj rozszerzenie przegladarki, ktore ostrzega przed phishingowymi stronami. Wiele przegladarek (Chrome, Firefox, Edge) ma to wbudowane. Moga one zablokowac dostep do znanych zlosliwych stron przed tym, zanim sie zaloguja.

Trzecie: regularnie aktualizuj oprogramowanie. Oszusci szukaja luk w starych wersjach przegladarek i systemow operacyjnych. Aktualizacje je zamykaja.

Czwarte: nigdy nie uzywaj tego samego hasla na wielu stronach. Jesli jedno haslo wycieknie, wszystkie konta sa zagrozone. Uzyj menadzera hasel (np. Bitwarden, ktore sa darmowe) do przechowywania roznych hasel.

Te kroki zajma ci godzine, ale zaoszczedza wiele bolu glowy pozniej.