Warszawa, 13.03.2026 r.

Jak rozpoznać próbę wyłudzenia danych (phishing) i jak się przed nią bronić?

Może się wydawać, że oszustwa w sieci dotyczą tylko osób nieostrożnych (np. takich, które zostawiają swoje dane „nie wiadomo gdzie"). Niestety, cyberprzestępcy doskonalą swoje metody każdego dnia. Phishing, czyli technika wyłudzania naszych haseł, danych osobowych czy pieniędzy poprzez podszywanie się pod osoby lub firmy, to dziś jedno z największych zagrożeń.

Jak nie dać się złapać na haczyk? Wystarczy odrobina czujności i znajomość kilku podstawowych mechanizmów.

Dwa oblicza phishingu: od widocznego gołym okiem oszustwa po mistrzowski kamuflaż

Wiele prób wyłudzenia danych dociera do nas kanałami, z których korzystamy najczęściej: przez e-maile, SMS-y (tzw. *smishing*) lub bezpośrednią rozmowę telefoniczną (tzw. *vishing*).

Phishing łatwy do wykrycia

Wielu oszustów idzie na ilość, wysyłając masowe wiadomości lub wykonując masowe połączenia. W takich przypadkach często już na pierwszy rzut oka widać, że coś jest nie tak. Zazwyczaj zdradzają ich:

- adres nadawcy – może do złudzenia przypominać prawdziwy, ale zawiera drobną literówkę (np. zamiast @nasza-firma.com widzisz @nasza-firnna.com albo dziwną domenę typu @gmail.com.biz),
- błędy językowe – dziwne konstrukcje gramatyczne, brak polskich znaków, tekst wyglądający jak kalka z translatora, w dodatku nieudolnie przetłumaczonego,
- presja czasu – wiadomość krzyczy: "Twoje konto zostanie zablokowane za 2 godziny!", aby wywołać w Tobie panikę i wymusić szybkie, nieprzemyślane kliknięcie,
- temat, który nas nie dotyczy – wiadomość od kuriera informuje Cię o wstrzymaniu paczki w sortowni z powodu błędnego adresu odbiorcy, podczas gdy Ty w ogóle niczego nie zamawiałaś/zamawiałeś,
- granie na emocjach, wzbudzenie strachu i wywołanie stresu – dzwoni do Ciebie „konsultant" z banku, że rzekomo ktoś złożył wniosek pożyczkowy na Twoje dane

Phishing „zaawansowany"

Niestety, musimy być przygotowani na znacznie sprytniejsze scenariusze. Hakerzy potrafią włamać się na prawdziwe konto e-mail (np. naszego kontrahenta lub pracownika innej firmy) i wysyłać wiadomości bezpośrednio z niego. Znika problem podejrzanego adresu nadawcy. Tak samo potrafią podrobić numer, kiedy dzwonią jako „konsultant" z banku (tzw. *spoofing*) – odbierając telefon widzisz nazwę swojego banku.

Złote zasady: jak zachować ostrożność?

Jeśli zastosujesz te kilka prostych zasad, drastycznie zmniejszysz ryzyko udanego (dla hakera) ataku:

Zasada nr 1 – nie klikaj w linki odruchowo

Jeśli dostajesz maila z prośbą o zalogowanie się do banku, systemu firmowego czy na pocztę – nie klikaj w przycisk w wiadomości. Otwórz przeglądarkę i wpisz adres strony ręcznie (lub skorzystaj z własnej zakładki). Jeśli na Twoim koncie faktycznie jest jakiś alert, zobaczysz go po bezpiecznym, samodzielnym zalogowaniu.

Zasada nr 2 – weryfikuj innym kanałem

Dostałeś nietypową prośbę od kolegi z pracy, przełożonego lub kontrahenta (np. o pilny przelew, udostępnienie wrażliwych danych, zakup kart podarunkowych)? Zadzwoń do tej osoby lub wyślij

wiadomość na komunikatorze, by potwierdzić, że to faktycznie ona.
Dostałeś telefon z banku o pożyczce na Twoje dane lub konieczności autoryzacji przelewu? Rozłącz się i sam zadzwoń do banku.

Zasada nr 3 – zwracaj uwagę na załączniki

Nie pobieraj plików (szczególnie .zip, .exe, ale też niespodziewanych dokumentów Office) z podejrzanych wiadomości.

Zasada nr 4 – nie panikuj

Nie daj się ponieść panice i podejmowaniu pochopnych działań w stresie, bo najczęściej oszuści chcą uzyskać dokładnie ten efekt. Dokładnie sprawdź maila/SMSa, zastanów się, czy na pewno zamawiałaś/zamawiałeś coś ostatnio, czy faktycznie masz do opłacenia usługę, której rzekomo dotyczy faktura, czy nie masz zastrzeżonego numeru PESEL, co ma Cię chronić przed niechcianymi pożyczkami na Twoje dane.

Zasada nr 5 – zgłaszaj wątpliwości

Jeśli coś wzbudziło Twój niepokój, nie ignoruj tego i nie usuwaj po prostu wiadomości. Zgłoś sprawę do swojego działu IT i Inspektora Ochrony Danych. Lepiej zgłosić o jeden fałszywy alarm za dużo niż zignorować prawdziwe zagrożenie.

Pamiętajcie, w cyfrowym świecie zdrowa podejrzliwość to Wasz najlepszy obrońca. Zanim klikniesz – weź głęboki oddech i zastanów się dwa razy.

Katarzyna Ułasiuk-Delamare, Członek Zarządu iSecure Sp. z o.o.