

Co to jest „phishing”?

„Phishing” to określenie działalności przestępczej polegającej na tworzeniu i wykorzystywaniu fałszywych przesylek poczty elektronicznej oraz stron internetowych – zaprojektowanych tak, by nie różniły się one od przesylek i stron dobrze znanych firm, instytucji finansowych czy instytucji publicznych.

Fałszywe wiadomości e-mail, załączniki do nich czy strony internetowe tworzone po to, by w oszukańczy sposób nakłonić użytkowników internetu do ujawnienia swoich danych bankowych, informacji o rachunku, karcie płatniczej oraz poufnych danych osobistych, jak np. nazwisko panięskie matki, adres, nazwa użytkownika czy hasło dostępu. Informacje takie mogą zostać następnie wykorzystane do celów przestępczych, takich jak kradzież informacji potwierdzających tożsamość czy oszustwo finansowe.

Prosimy pamiętać, że SK bank, MasterCard czy inna instytucja finansowa NIGDY nie wysyłają do swoich klientów e-maili z prośbą o podanie wrażliwych danych typu: numer kart czy rachunku bankowego, hasła czy PIN-y lub dane osobowe.

O ile samemu nie jest się inicjatorem korespondencji do Banku, uprzejmie przypominamy użytkownikom kart, że nigdy nie należy ujawniać poniższych informacji w odpowiedzi na wezwania mające jakoby pochodzić z jakichkolwiek instytucji finansowych. Chronić szczególnie:

- numer karty, jej numer CVC2, datę ważności oraz numer PIN,
- login i hasło do systemów bankowości internetowej,
- informacje o charakterze osobistym: nazwisko panięskie matki, pesel, adres zamieszkania,
- listę produktów z których korzystasz w danej instytucji finansowej.

Jak postępować ?

Jeżeli otrzymają Państwo e-mail z prośbą o podanie informacji o Państwa rachunku bankowym lub rachunku Państwa karty – wysłany przez SK bank lub np. płatniczą MasterCard lub jakąkolwiek inną instytucję – **nie należy podawać w odpowiedzi żadnych informacji.**

Należy natychmiast niezwłocznie skontaktować się z Infolinią SK banku i poinformować o otrzymaniu takiego e-maila.

Jeśli otrzymany e-mail z prośbą o dane karty pochodzi z organizacji MasterCard, można również przesłać zgłoszenie do MasterCard, korzystając z adresu mailowego stopit@mastercard.com.

Zagrożenie atakiem tego typu jest realne, dlatego zawsze warto być czujnym!!!