U góry strony na niebieskim tle napis: JAK TO Możliwe. Poniżej na niebieskim tle po lewej stronie znajdują się emotikony a po prawej tekst:

Emotikona dymku konwersacji, a obok napis: 1. Kontakt z ofiarą

Oszust kontaktuje się ze sprzedającym, podając się za zainteresowanego kupca. Sprawca preferuje kontakt telefoniczny.

Emotikona portfela z wystającym banknotem i napis: 2. Rzekoma opłata za przesyłkę

Informuje, że opłacił firmę kurierską, która odbierze przesyłkę.

Emotikona koperty i e-maila, a obok napis: 3. Fałszywy e-mail

Pokrzywdzony otrzymuje wiadomość e-mail z linkiem do rzekomego potwierdzenia transakcji.

4. FAŁSZYWA strona banku

Po kliknięciu w link następuje przekierowanie na FAŁSZYWĄ stronę banku.

Emotikonka do wpisania haseł i napis: 5. Logowanie SPRZEDAJĄCEGO na FAŁSZYWEJ stronie

Sprzedający loguje się na FAŁSZYWEJ stronie banku, wpisując poufne dane do logowania.

Emotikona linii papilarnych i otwartej kłódki, a obok napis: 6. OSZUST prosi o kody SMS

Kolejny rozmówca podaje się za pracownika firmy kurierskiej i prosi o podanie kodów SMS. UWAGA!!! TO SĄ KODY Z BANKU.

Emotikona dymku konwersacji, z boku osoby oraz napis: 7. Zatwierdzenie przelewu przez ofiarę

Sprzedający podaje kody autoryzacyjne, tym samym zatwierdza przelewy wykonane przez oszusta, który wcześniej uzyskał dostęp do konta po zalogowaniu się przez ofiarę na fałszywej stronie banku.

Poniżej z lewej strony emotikona dzwoniącego telefonu.