Ulotka składająca się z dwóch stron.

Na stronie pierwszej na granatowym tle czerwony okrąg z białym napisem STOP.

Poniżej biały napis OSZUSTOM W SIECI

Poniżej pomarańczowy napis: Chroń swoje płatności!

Pod napisami na środku grafika przedstawiająca człowieka w kapturze siedzącego przy ekranie laptopa. W lewo od grafiki biała strzałka na pomarańczowym tle wskazująca w lewo na grafikę ekranu komputera. W prawo od grafiki biała strzałka na pomarańczowym tle wskazująca w prawo na grafikę z symbolem komputera.
Na dole na białym tle od lewej pomarańczowe logo rzeszów stolica innowacji, na środku logo (biały napis na czarnym tle z czerwoną kropką) blik oraz po prawej granatowe logo POLICJA z graficznym symbolem policyjnej gwiazdy.

Strona druga.
Na czerwonym tle napis: UWAGA! Oszuści atakują w sieci
Poniżej strona podzielona jest na dwie częście. Po lewej pomarańczowa belka z białym napisem: Podają się za Twoich znajomych
Poniżej na szarym tle czarne napisy wyszczególnione numerami oznaczonymi białą czcionką w pomarańczowym kółku:
1 Przestępcy włamują się na konta
w serwisach społecznościowych.
2 Podszywają się pod Twoich znajomych i rozsyłają prośby o pieniądze.
3 Zwykle jest to uzasadnione nagłą sytuacją, np. „Muszę pilnie coś zapłacić i nie wziąłem ze sobą karty”.
4 Proszą o podanie kodu BLIK.
5 Podajemy kod i akceptujemy płatność w aplikacji naszego banku, bez jej weryfikacji.

Pod spodem biały napis na pomarańczowym tle wyszczególniony białym wykrzynikiem w pomarańczowym kółku:
! JEŻELI TAK ZROBISZ,
STRACISZ PIENIĄDZE!

Po prawej stronie pod czerwoną belką znajduje się granatowa belka z białym napisem:
Podają się za pracowników banków lub portali inwestycyjnych

Poniżej na szarym tle czarne napisy wyszczególnione numerami oznaczonymi białą czcionką w granatowym kółku:

1 Ukrywają numer telefonu i podają się np. za pracownika banku czy portalu.
2 Dzwonią do Ciebie pod pozorem ochrony zgromadzonych na koncie środków lub okazji inwestycyjnej.
3 Proszą o zainstalowanie aplikacji lub oprogramowania typu AnyDesk, TeamViewer, QuickSupport.

4 Dzięki takim programom sprawcy widzą zawartość Twojego urządzenia i mogą się nim zdalnie posługiwać.
5 Pomagają zainstalować takie oprogramowanie, po czym uzyskują dostęp do Twoich danych bankowych.

Pod spodem biały napis na granatowym tle wyszczególniony białym wykrzynikiem w granatowym kółku:

JEŻELI TAK ZROBISZ,
STRACISZ PIENIĄDZE!

Pod spodem na środku czerwony napis na białym tle:
Oszuści, podszywając się pod Ciebie, wypłacają pieniądze, zaciągają pożyczki, dokonują swobodnie płatności, obciążając Twoje konto.

Po prawej w czerwonym kółku biały napis:
JAK NIE DAĆ SIĘ OSZUKAĆ W SIECI

Poniżej biały napis na pomarańczowym tle:
Łatwo możesz uchronić się przed oszustwami – pamiętaj:

Poniżej na ciemno-szarym tle białe napisy wyszczególnione numerami oznaczonymi białą czcionką w czerwonym kółku:

1 ZAWSZE SPRAWDZAJ, komu i jakie dane przekazujesz.
2 ZANIM PRZEKAŻESZ kod BLIK, dane do logowania, dane z kart płatniczych, sprawdź tożsamość odbiorcy – ZADZWOŃ, UPEWNIJ SIĘ, że to Twój znajomy.
3 ZANIM POTWIERDZISZ transakcję, sprawdź jej szczegóły (kwotę i odbiorcę).
4 NIE KORZYSTAJ z podejrzanych formularzy logowania, czy podsyłanych linków. Loguj się tylko przez oficjalne strony banków i ich aplikacje.
5 PAMIĘTAJ – pracownik banku dzwoniąc do Ciebie nigdy nie prosi o instalację dodatkowych aplikacji, podanie pełnego hasła, kodu PIN czy kodów do autoryzacji transakcji.