13.01.2022 Ostrzegamy o oszustwach na portalach OLX/Vinted/Allegro

Sprzedajesz coś przez OLX, Vinted czy Allegro?
Wystawiasz ogłoszenie o sprzedaży, a kupujący kontaktuje się z Tobą za pomocą komunikatora (np. WhatsApp) i chce kupić przedmiot?
Później możesz dostać od kupującego link na WhatsAppie do rzekomego odbioru pieniędzy:

albo gotową instrukcję finalizacji transakcji:

Uważaj! To oszustwo.
Link prowadzi do fałszywej strony, na której masz ujawnić swoje dane do karty płatniczej lub dane do logowania. Ta strona może łudząco przypominać stronę logowania do Twojego banku. Jeśli ujawnisz na niej swój login, hasło oraz kod SMS, bądź też dane do karty – te dane trafią bezpośrednio do oszusta.

Nie klikaj!
Oszuści wykorzystają każdą okazję, żeby nakłonić Cię do przekazania danych Twojej karty płatniczej czy danych do logowania do bankowości internetowej. Mogą poprosić Cię o hasła, kody z wiadomości SMS od banku. Dla nich nie jest istotne, czy sprzedajesz przedmioty, czy je kupujesz. Przestępcom chodzi o przejęcie Twoich danych, by móc Cię okraść.

Nie podawaj żadnych kodów z wiadomości SMS od banku!
Nie zatwierdzaj żadnych niespodziewanych powiadomień autoryzacyjnych wysyłanych do aplikacji mobilnej!
Możesz dostać wiadomość z kodem SMS lub żądanie autoryzacji mobilnej dotyczące aktywacji aplikacji mobilnej na nowym urządzeniu. To oszust próbuje na swoim urządzeniu aktywować aplikację mobilną. Jeśli mu się to uda – będzie mógł zmienić limity dla Twojej karty, limity przelewów, aktywować usługę BLIK oraz uruchomić autoryzację mobilną i w ten sposób wyprowadzić pieniądze z Twojego konta.

Zadbaj o to, na co masz wpływ
Jeśli Twoja intuicja podpowiada Ci, że przedstawiona okazja jest podejrzana – wycofaj się z niej.
Pamiętaj:

- **czytaj szczegółowo informacje z Banku (w szczególności treść wiadomości SMS, powiadomień i żądań autoryzacyjnych). Zwracaj uwagę na to, co autoryzujesz.** Jeśli w treści SMS-a lub żądania autoryzacji mobilnej informujemy, że aktywujesz aplikację mobilną lub dodajesz nowe urządzenie – a faktycznie tego nie zlecasz, to właściwie pewne, że padłeś ofiarą oszustwa i na Twoim koncie bankowym jest zalogowany oszust.
- **nie otwieraj linków**, które rzekomo mają pozwolić na odbiór pieniędzy za wystawiony przez Ciebie przedmiot.
- rozliczaj się bezpośrednio przez dany portal - **uważaj na próby nawiązania kontaktu poza portalem** czy aplikacją, np. WhatsApp, e-mail.
-

Jeśli podejrzewasz, że padłeś ofiarą oszustwa **przerwij transakcję i skontaktuj się placówką Banku obsługującą rachunek lub infolinią SGB**:

- 800 88 88 88 (bezpłatne połączenie)
- 61 647 28 46 (z zagranicy; opłata zgoda z taryfą operatora).