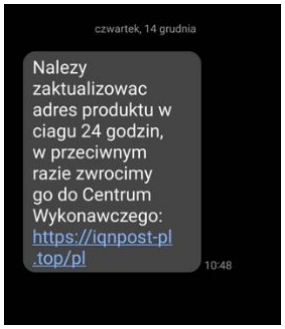
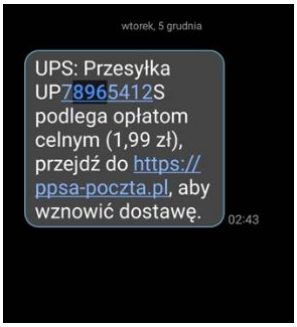
Uważaj na SMS'y dotyczące rzekomych dopłat do przesyłek kurierskich lub zmiany danych adresowych dotyczących przesyłki – Komunikat FinCERT.pl – Bankowego Centrum Cyberbezpieczeństwa ZBP, Centralnego Biura Zwalczania Cyberprzestępczości oraz Komendy Głównej Policji z dnia 20 grudnia 2023 r.

Święta Bożego Narodzenia tuż, tuż... a licho niestety nie śpi.
Ostatnie dni przed Świętami to szczyt szału zakupowego. Kiedy myślisz, że wszystko masz pod kontrolą, nagle dostajesz wiadomość sms. To informacja o nieoczekiwanej dopłacie do przesyłki lub zmianie adresu dostawy… Oblewa cię zimny pot „***przecież teściowa marzyła o szalu, który zamówiłam online***".



Niepokój przeradza się w przerażenie, które zaczyna wyłączać racjonalne myślenie i chłodny osąd sytuacji.



Klikasz w link przesyłany w wiadomości, otwiera się strona, zaczynasz aktualizować dane: adres, e-mail, numer telefonu. Ostatnie kliknięcia, jeszcze tylko podam: imię i nazwisko, numer karty płatniczej, data jej ważności i kod CVV, …uff zaraz będzie można odetchnąć, „ostatnia prosta" – kliknę przycisk „wyślij" i pożar będzie zgaszony, ale czy aby na pewno …?

STOP!!! Zatrzymujesz się na chwilę, czy to na pewno jest bezpieczne? Może to jakieś oszustwo? Szukasz informacji na temat tego rodzaju wiadomości, sprawdzasz, czy inni nie padli ofiarą tego typu przestępstw?

BINGO!!! Docierasz do informacji, że to bardzo popularne oszustwo, którego celem jest wyłudzenie danych z karty płatniczej, danych do logowania w serwisach bankowości internetowej a w konsekwencji można stracić wszystkie pieniądze, a nawet więcej. Inni piszą, że w ten sposób oszuści uzyskali dostęp do ich bankowości elektronicznej, dodali „urządzenie zaufane" przestępców lub utworzyli wirtualną kartę na telefonie – a wszystko to w wyniku ich lekkomyślności!

Ostatnie chwile przed Świętami Bożego Narodzenia generują dodatkowy stres i pośpiech, dlatego zanim wykonasz jakikolwiek krok, szczególnie ten, który może zagrozić Twojemu bezpieczeństwu zatrzymają się, weź 3 głębokie wdechy i:

- **nie klikaj w linki w wiadomości SMS!**
- **przeczytaj bardzo uważnie treść komunikatu SMS, otrzymany z banku!**
- **nie przekazuj kodów otrzymanych od banków w wiadomościach SMS lub kodów BLIK!**
- **nie podawaj danych wrażliwych!**
- **obserwuj zamówiony towar wyłącznie za pomocą oficjalnej strony internetowej firmy kurierskiej lub jej aplikacji!**

Z tego doświadczenia wynosisz ważną lekcję - ostrożność jest równie istotna jak planowanie świątecznych zakupów. Ostatecznie, unikasz przekazania danych wrażliwych, a szal trafia pod choinkę.

Jeśli niestety padł(aś\eś) ofiarą przestępstwa, to w zależności od jego rodzaju natychmiast:

- **skontaktuj się ze swoim bankiem,**
- **zmień hasło do swojej bankowości internetowej i aplikacji mobilnej;**
- **zastrzeż skompromitowaną kartę płatniczą – dzwoniąc na numer 828-828-828;**
- **złóż zawiadomienie o popełnieniu przestępstwa na policji lub w prokuraturze;**
- **zastrzeż skompromitowany dokument potwierdzający Twoją tożsamość i wystąp o wydanie nowego.**

WESOŁYCH ŚWIĄT BOŻEGO NARODZENIA!!!!!

FinCERT.pl - Bankowe Centrum Cyberbezpieczeństwa ZBP - Centrum Wymiany i Analiz Informacji Sektora Finansowego
Centralne Biuro Zwalczania Cyberprzestępczości
Komenda Główna Policji

FinCERT.pl - Bankowe Centrum Cyberbezpieczeństwa ZBP – jednostka operacyjna funkcjonująca w ramach Komitetu Cyberbezpieczeństwa Banków Związku Banków Polskich, która gromadzi, analizuje oraz przekazuje w ramach sektora bankowego i we współpracy z organami ścigania oraz innymi instytucjami informacje dotyczące możliwych zagrożeń oraz o incydentach o charakterze przestępczym, godzących w bezpieczeństwo banków lub ich klientów.