Bądź mądry przed szkodą.

Wyobraź sobie taką sytuację; siedzisz na ławeczce w parku i dokarmiasz kaczki czy inne ptactwo. W pewnej chwili podchodzi elegancko ubrany mężczyzna (lub kobieta), zwraca się do Ciebie po imieniu i nazwisku i pyta, czy mieszkasz pod adresem, pod którym faktycznie mieszkasz. Nieco zdziwiony, ale i zaciekawiony potwierdzasz i pytasz, o co chodzi. Elegancko ubrany mężczyzna (lub kobieta) informuje Cię, że właśnie przechodził obok Twojego mieszkania, zauważył wyłamany zamek w drzwiach wejściowych oraz usłyszał jakieś podejrzane hałasy dobiegające zza tych drzwi. Od razu też uspokaja, że nie masz powodu do niepokoju, bo złodzieje pewnie jeszcze nie skończyli roboty, więc jeśli dasz mu (lub jej) klucz do mieszkania, to on (lub ona) opanuje sytuację i zażegna niebezpieczeństwo.

Co zrobisz? Podziękujesz za informację i zatelefonujesz do domu, albo zakończysz spacer i wrócisz, żeby sprawdzić jak wygląda sytuacja? Czy też dasz klucz elegancko ubranemu mężczyźnie (lub kobiecie), licząc na jego uczciwość i chęć pomocy.

Nie do wiary, ale są osoby, które co prawda klucza nie dadzą, za to bez większych oporów i bez zastanowienia wpuszczą złodzieja na swój rachunek bankowy, chociaż w obu przypadkach sposób działania sprawcy jest taki sam. Podaje trochę prawdy, trochę nieprawdy, odrobinę niepewności i stawia ofiarę przed wyborem: albo zrobisz **teraz** to, o co Cię poproszę, albo zaraz stracisz wszystkie pieniądze. I niektórzy ulegają temu szantażowi.

Jak więc postępować, żeby pieniędzy nie stracić albo żeby ryzyko ich utraty ograniczyć do minimum? Podpowiedzi znajdziesz tutaj. Dotyczyć będą głównie bankowości internetowej, ale też trochę internetowych zakupów, które również mogą pójść nie po Twojej myśli. Oczywiście, że w Sieci znajduje się mnóstwo literatury na ten temat, może za dużo. Ponadto napisanej niekiedy w sposób trudny do przyswojenia przez osoby, które nigdy nie interesowały się tą tematyką.

Aby obronić się przed oszustem nie potrzebujesz specjalistycznej, informatycznej wiedzy. W zupełności wystarczą Ci: ostrożność, ograniczone zaufanie w stosunku do nieznanego i najważniejsza zasada policyjnej pracy, o której mogłeś zapomnieć - weryfikacja każdej informacji.

To, co przeczytasz dalej to minimum, które powinieneś znać. Bardzo dobrze będzie jeśli uznasz, że to dla Ciebie za mało, bo widać, że poważnie traktujesz swoje cyfrowe bezpieczeństwo i już samodzielnie poszukiwać będziesz odpowiedzi, których tu możesz nie znaleźć.

Na początku musisz uświadomić sobie i przyjąć do wiadomości, że

1) Podpisując umowę z bankiem i uruchamiając usługę bankowości internetowej **zobowiązałeś się** między innymi do tego, żeby danych logowania nie udostępniać innym osobom. To ważne, bo w przypadku skutecznego oszustwa, to Ty nie spełnisz tego warunku, więc bank mieć będzie wszelkie podstawy, żeby nie uznać Twojej reklamacji. Pozostanie Ci więc tylko nadzieja, że sprawca zostanie zatrzymany. Razem z Twoimi pieniędzmi, których nie zdążył wydać.

2) Twoje dane osobowe, które przekazujesz różnym podmiotom, powinny być chronione i dobrze zabezpieczone. Z naciskiem na powinny. Jak jest w rzeczywistości? Różnie, ale **musisz** zało-

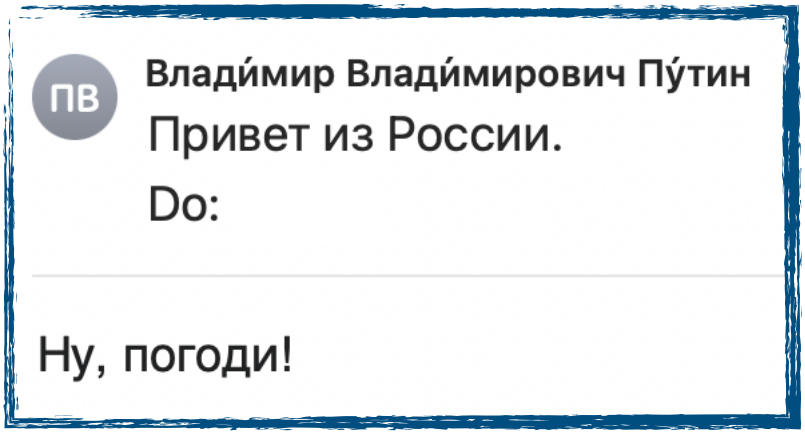
żyć, że oszust może wejść albo już wszedł w ich posiadanie. W jaki sposób? A chociażby:

- Włamując się do baz danych urzędów, instytucji, uczelni, zakładów pracy, w których dane osobowe nie są szyfrowane. To tak zwane „wycieki" danych.
- Odczytując dane znajdujące się w ogólnodostępnych rejestrach publicznych.
- Wykorzystując niechlujstwo organów władzy - do dzisiaj nie wiadomo, czy dane osobowe, krążące w czasie przygotowań do wyborów „kopertowych" między samorządami a Pocztą Polską, wróciły na swoje miejsce i czy wróciły w całości. Nie ma też pewności, czy nie zostały skopiowane i nie czekają na kupca. Albo że już nie zostały sprzedane.
- Wykorzystując to, co pozostawiasz w Internecie; imię i nazwisko, adres e-mail lub pocztowy, numer telefonu. Ale nie tylko w Internecie. Zastanawiasz się, skąd przestępca może znać na przykład Twój numer klienta dostawcy prądu, operatora sieci komórkowej czy cztery ostatnie cyfry Twojej karty płatniczej? A co robisz ze starymi fakturami, rachunkami czy paragonami ze sklepu. Niszczysz je czy tylko mniesz i wszystkie razem wyrzucasz do kosza, albo - co gorsza - do eko-kontenera?

  Sposobów pozyskiwania przez oszusta informacji o Tobie jest więcej. Tu wymienione zostały tylko te najbardziej znane i oczywiste.

3) Jedną z metod kradzieży, niezwykle skuteczną i dotkliwą, jest kradzież z wykorzystaniem duplikatu Twojej karty SIM, w celu autoryzacji przestępczego przelewu. W tym celu oszust przedstawia operatorowi sieci komórkowej sfałszowany dokument, na przykład dowód osobisty z Twoimi danymi czy równie „prawdziwe", notarialne upoważnienie do wydania duplikatu. Ale nie zawsze musi sięgać do tak wyrafinowanych środków, bo lekkość umysłów pracowników niektórych operatorów jest naprawdę zadziwiająca i wystarczy jedna, przekonująca rozmowa telefoniczna, a duplikat karty trafi wprost do oszusta, który oczywiście już wcześniej pozyskał dane służące do jej aktywacji, a tym samym do wyłączenia Twojej karty SIM.

4) Przestępca potrafi podszyć się pod dowolną instytucję czy osobę. Niektóre rzeczy jesteś w stanie sam zweryfikować. Popatrz:



Tego e-maila nie wysłał rzecz jasna Prezydent Federacji Rosyjskiej. Żeby ustalić prawdziwy adres, wystarczy w programie pocztowym lub w przeglądarce (jeśli jej używasz do obsługi poczty) kliknąć w pole nadawcy.

Łatwo możesz też sprawdzić autentyczność przesłanego Ci adresu internetowej witryny, do której chce przekierować Cię oszust. Popatrz: strona logowania do popularnego serwisu aukcyjnego to https://alegro.pl/logowanie?origin_url=%2Fsmart. Jeśli kliknąłeś ten link to już widzisz, że to nieprawda, bo link kieruje Cię do innej witryny. Ponadto nieprawidłowy jest adres, bo powinno być *„allegro”*, przez dwa *„l”*. No to co się stanie, gdy adres logowania będzie prawidłowy, czyli https://allegro.pl/logowanie?origin_url=%2Fsmart. Znowu to samo, prawda? W tym miejscu należy wyjaśnić, że linki w powyższych przykładach oczywiście nie prowadzą do fałszywej strony, a wręcz przeciwnie, do internetowej witryny najbardziej rzetelnej i wiarygodnej stacji informacyjnej.

Ta sztuczka pokazuje, jak łatwo zmanipulować internetowy adres. W rzeczywistości oszust ma trudniej, bo co prawda może przysłać prawdziwy link do fałszywej witryny, ale **nie może** stworzyć fałszywej witryny z identycznym adresem www, jak ta oryginalna, prawdziwa. Adres tej fałszywej będzie łudząco podobny, jednak nie taki sam. Brakować będzie jednej litery, zamiast *„allegro”* będzie *„allergo”*, bądź zamiast *„pl”* będzie *„com”* lub *„eu”*. Jak to sprawdzić? Kliknij w pole adresu przeglądarki.

Przed fałszywym numerem telefonu nie obronisz się jednak, bo oszust ma możliwość wykonania takiego połączenia. Jeśli więc widzisz że ktoś dzwoni do Ciebie z numeru, który zapisałeś jako „Mój bank” licz się z tym, że może dzwonić „Twój oszust”, którego w książce telefonicznej nie masz.

To, co przeczytałeś do tego miejsca pokazuje, że „procedura” kradzieży Twoich pieniędzy może rozpocząć się na wiele sposobów i że to Ty jesteś jej najważniejszym, bo najmniej pewnym elementem. Ale możesz obronić się przed tym. Na początek zrób dwa najbardziej oczywiste i najważniejsze kroki:

Krok nr 1.

Odwiedź swój bank. Ale wizytę poprzedź przeczytaniem informacji i zaleceń dotyczących bezpieczeństwa, które każdy bank powinien udostępniać. Znajdziesz je w zakładce *„Pomoc”* witryny bankowej. Jeśli nie, poszukaj. Wyposażony w taką, chociażby cząstkową wiedzę zapytaj o to:

- W jakich okolicznościach i w jaki sposób pracownik banku skontaktuje się z Tobą?
- O co Cię zapyta i jakie polecenia wyda?
- O co na pewno Cię **nie zapyta** i jakich poleceń **nie wyda**?

Zapytaj również o:

- Usługę *„chargeback”* (obciążenie zwrotne), która może (oby nie) przydać się po nieudanych zakupach internetowych i nie tylko.
- Oferowaną przez niektóre banki możliwość ustawienia „hasła zwrotnego”, w celu identyfikacji dzwoniącego do Ciebie pracownika banku.

Poproś też o pomoc czy wskazówki w ustawieniu optymalnych zabezpieczeń Twojego internetowego profilu i bankowej aplikacji mobilnej.

Krok nr 2.

Odwiedź salon swojego operatora sieci komórkowej. Jeśli używasz karty pre-paid, zatelefonuj lub wyślij korespondencję ze swojego profilu. Zapytaj o to:

- Jak przebiega procedura wydania duplikatu karty SIM?
- W jaki sposób sprawdzana jest osoba wnioskująca o wydanie duplikatu?
- Jak przebiega aktywacja nowej karty? W salonie, telefonicznie, przez Internet?
- W jaki sposób weryfikowana jest tożsamość użytkownika nowej karty?
- Jakie inne środki ma operator, żeby zapobiec wydaniu duplikatu karty SIM innej osobie, bez Twojej wiedzy.

Zapytaj również o możliwość dodatkowego zabezpieczenia, na przykład, wydanie duplikatu tylko w salonie i tylko w zamian za wymienianą, podlegającą natychmiastowemu zniszczeniu kartę, czy ustawienie dodatkowego pytania (kodu, hasła) w procedurze aktywacji nowej karty.

Jeśli nie dostaniesz zadowalających Cię odpowiedzi, albo usłyszysz, że jesteś przewrażliwiony, a zabezpieczenia są super i nie można ich zmieniać czy uzupełniać, rozważ zmianę operatora. Chyba że bardziej niż bezpieczeństwo Twoich pieniędzy cenisz darmowe minuty i megatony Internetu komórkowego.

Uważasz, że powyższych kroków nie musisz robić, bo to strata czasu? Nie trać go też na dalszą lekturę i kolejne czynności do wykonania.

Krok nr 3.

Zrób remanent. Nie od razu, nie w ciągu jednego dnia, ale na spokojnie, żeby niczego nie przegapić lub nie podjąć pochopnej, nieodwracalnej decyzji.

- Sporządź listę wszystkich witryn w Internecie, w których jesteś zarejestrowany. Może to być sklep, portal społecznościowy, firma hotelarska, dostawca prądu, gazu, Internetu, telefonii komórkowej itp.
- Sprawdź, czy potrzebujesz każdej z tych rejestracji. Jeśli nie, usuń zbędne profile (wyrejestruj się) i zażądaj od usługodawcy usunięcia Twoich danych. Masz do tego prawo.
- Jeśli już oczyściłeś przedpole sprawdź, w których pozostałych miejscach dokonujesz płatności kartą bądź przelewem.
- Pozostaw te, które uznasz za niezbędne. Na pewno będą to witryny, w których opłacasz czynsz, nośniki energii czy ubezpieczenia.
- Wyrejestruj się z pozostałych witryn, zwłaszcza z tych, w których płatności dokonujesz okazjonalnie, a możesz z nich korzystać bez konieczności zakładania konta.
- Jeśli do witryny, w której dokonujesz transakcji masz na stałe podpiętą kartę płatniczą, usuń ją jako metodę płatności. W razie konieczności kolejnej transakcji będziesz mógł ją ponownie dodać. Ale działaj rozważnie, bo w niektórych przypadkach taki krok może wiązać się na przykład z anulowaniem subskrybcji albo z utratą bonusów. Decyzja należy do Ciebie.

Jeżeli zastosowałeś się do powyższych wskazówek i zrobiłeś to, o czym przeczytałeś, jesteś już bezpieczniejszy. Powinieneś też zauważyć, że co prawda oszust może znać Twoje imię i nazwisko, PESEL, adres, numer karty czy rachunku bankowego i wiele innych szczegółów, ale **nie zna jednej rzeczy - hasła logowania do Twojego banku**. Nie zna go również bank, bo w przypadku gdy zapomnisz hasła, bank może je jedynie zresetować.

Wniosek stąd taki, że celem działania oszusta będzie zdobycie tego hasła. I nie ma co zawracać Ci głowy, jakich sposobów użyje:

- Czy będzie to e-mail, rozmowa telefoniczna, SMS, a może list polecony.
- Czy oszust podawać się będzie za pracownika banku, gazowni, firmy kurierskiej, sklepu internetowego.
- Czy poinformuje Cię o nieprawidłowości na Twoim rachunku bankowym lub o kradzieży pieniędzy z tego rachunku, o konieczności weryfikacji danych, o jakiejś niezapłaconej należności lub o konieczności uzupełnienia jakiejś płatności.

Celem jego działania będzie przekonanie Cię, że coś jest nie tak, być może nawet z Twojej winy. Na końcu, w tej czy innej formie, w taki czy inny sposób, **zawsze** będzie żądanie podania hasła, najczęściej na podstawionej, fałszywej stronie internetowej. Jeśli więc wykonałeś krok nr 1, jesteś już przygotowany do tego typu podchodów.

Inaczej wygląda sprawa ataku z wykorzystaniem duplikatu karty SIM. Oznacza on, że oszust najpewniej już ma Twoje dane logowania do bankowości elektronicznej (identyfikator i hasło) i „ma" Twój telefon do autoryzacji przelewu. Skąd ma dane logowania? Na przykład:

- Masz komputer zainfekowany oprogramowaniem napisanym do przechwytywania tych danych.
- Logowałeś się do banku na innym niż Twój komputerze, na przykład w kafejce internetowe (karygodne), u znajomego, w hotelu/pensjonacie.
- Logowałeś się do banku ze swojego sprzętu, ale w niezabezpieczonej sieci Wi-Fi.

Jak wygląda taki atak? Pewnego dnia zauważasz, że nie możesz wykonywać/odbierać połączeń i nie masz komórkowego Internetu. Może to być awaria sieci lub usterka telefonu, ale równie dobrze może to oznaczać, że oszust aktywował duplikat karty SIM, a tym samym operator wyłączył Twoją. Jeśli masz szczęście i trafisz na kompetentnych pracowników **dwóch** banków (Twojego i tego banku, do którego sprawca zdążył już przelać pieniądze), jest cień szansy na ich odzyskanie.

Co oznacza „kompetentny"? To, że zauważy on na przykład, że nigdy nie dokonywałeś przelewów dużych kwot do banków, których nie masz w swojej książce zaufanych odbiorców czy na przysłowiowe „kajmany". Oczywiście, że może przelew zauważyć już po jego wykonaniu. Wtedy właśnie potrzebna będzie pomoc i kompetencje pracownika tego drugiego banku, żeby zablokował dalsze transfery.

Ale jak skontaktować się z bankiem, czy też z operatorem sieci komórkowej, gdy telefon nie działa? I o co zapytać? Z drugiego telefonu lub osobiście. A może to bank lub operator pierwszy skontaktuje się z Tobą? Ale jak, gdy telefon nie działa? Jeśli wykonałeś kroki nr 1 i nr 2, będziesz przygotowany na tę okoliczność, bo nie ma tu miejsca na żadne, nawet najmniejsze domysły czy improwizację, więc akurat w tej sprawie wskazówek i porad nie otrzymasz. Przeczytaj za to o tym, co jeszcze powinieneś zrobić, żeby nie być łatwym celem dla oszusta.

Cyfrowe BHP.

- Jeśli Twój telefon służy jednocześnie do wykonywania bądź autoryzowania operacji bankowych i do codziennego użytku, a tym samym jego numer znany jest nie tylko Twoim bliskim, ale i bliżej nieokreślonej grupie osób bądź instytucji, zainwestuj w drugi i w drugą kartę SIM, ale **u innego operatora**. Zainstaluj na nim **tylko** aplikację bankową, a następnie usuń stary i autoryzuj nowy numer w banku.

  Nie musi to wiązać się z kupowaniem drogiego abonamentu. Jeden z operatorów kart prepaid oferuje starter za 5 zł i doładowanie taką samą kwotą w celu przedłużenia ważności konta. o rok.

  Inicjujące połączenie wykonaj na infolinię operatora lub banku. **Nie dzwoń do nikogo innego**. **Nowego numeru nikomu nie udostępniaj!** Ma on służyć **wyłącznie** Tobie i **wyłącznie** do korzystania z aplikacji bankowej i do ewentualnych kontaktów z bankiem. Żadnego przeglądania Internetu, żadnych komunikatorów, żadnych portali społecznościowych. Zapomnij o tym wszystkim. W przeciwnym razie kupowanie drugiego telefonu nie ma sensu.

- Przeglądarki internetowej używaj **tylko** do zmiany ustawień, których nie możesz wykonać w aplikacji mobilnej. Aplikacja mobilna to w zasadzie również przeglądarka, ale napisana tak, że możesz przez nią wejść tylko na specjalnie przygotowane strony Twojego banku. Nie ma więc zagrożenia, że przeglądając te strony zainfekujesz swoje urządzenie złośliwym oprogramowaniem.
- Po zakończeniu sesji, **wyloguj się** z aplikacji mobilnej. Co prawda niektóre z nich mają funkcję auto wylogowania po zamknięciu, ale strzeżonego… . Z przeglądarki internetowej wylogować się musisz sam. Możliwe jest, że po iluś tam minutach bezczynności (w zależności od banku) zostaniesz automatycznie wylogowany, ale również w tym przypadku strzeżonego… . Zwłaszcza gdy bez wylogowania się wejdziesz na inną stronę lub zamkniesz przeglądarkę.
- Tam gdzie to możliwe, zmień sposób autoryzacji bądź powiadomień z SMS-a na „push”. Jeśli uważnie czytałeś to wiesz, że w ten sposób utrudniasz kradzież „na duplikat”, bo powiadomienia „push” przypisane są do urządzenia, a nie do karty SIM. Możesz je równie dobrze odbierać na tablecie bez karty SIM. Musisz mieć tylko dostęp do Wi-Fi.
- Z bankowości internetowej (czyli przez przeglądarkę) korzystaj **tylko** na Twoim komputerze/telefonie/tablecie. **Nigdy** na sprzęcie w pracy (o ile jeszcze masz siły, zdrowie i dorabiasz), na wczasowej kwaterze (hotel, pensjonat), u rodziny, znajomych, jednym słowem, poza domem. W tych miejscach - jeśli już musisz - korzystaj **wyłącznie** z aplikacji mobilnej.
- Ty jesteś suwerenem urządzeń, na których „bankujesz”. **Nie pozwól** wnukowi czy innym osobom instalować żadnych „apek”/programów, przydatnych tylko dla nich.
- Jeśli możesz, zrezygnuj w ogóle z „darmowych” kont pocztowych w popularnych witrynach. Korzystaj z poczty oferowanej przez Twojego dostawcę Internetu.
- Używaj aliasów pocztowych. To nic innego jak dodatkowy adres e-mail, utworzony w tej domenie pocztowej, którą już masz. Jeden alias przypisz **tylko** do banku, drugi, na przykład, **tylko** do odbiorców Twoich stałych zleceń. W ten sposób zorientujesz się, czy e-mail faktycznie pochodzi od przypisanego do aliasu nadawcy, czy też od oszusta, który wysłał na używany przez Ciebie na codzień adres.

- Kontroluj swoje płatności, zwłaszcza te cykliczne, ale też za internetowe zakupy. Gdy otrzymasz jakiś monit o uregulowanie zaległości łatwo ustalisz, czy faktycznie zagapiłeś się i o czymś zapomniałeś, czy też jest to próba oszustwa.

Pominięte tu zostały wskazówki dotyczące komputerowej „higieny", ale o legalności oprogramowania i jego aktualizacjach, zabezpieczeniach antywirusowych, bezpiecznym przeglądaniu Internetu czy korzystaniu z programu pocztowego nie trzeba chyba Ci przypominać.

Kilka zdań o internetowych zakupach. Są sklepy czy portale aukcyjne, w których kupujesz od „zawsze" i do których masz zaufanie. Ale są też takie, w których jeszcze nie gościłeś, a kuszą atrakcyjną ofertą. Przed decyzją o zakupie zrób kilka rzeczy:

- Przede wszystkim **zapomnij** o tym, że „kłódka" i certyfikat przy adresie internetowego sklepu to gwarancje bezpieczeństwa i udanych zakupów. „Kłódka" oznacza tylko tyle, że połączenie jest szyfrowane (dzisiaj prawie wszystkie witryny mają ten symbol) i potwierdza „autentyczność" strony z „kłódką". A certyfikat SSL? Można go legalnie kupić. U nas i za granicą. W Polsce, roczny abonament kosztuje od kilkudziesięciu do kilku tysięcy złotych.

  „Profesjonalny" oszust na pewno zadba o te szczegóły bo wie, że dla znakomitej części potencjalnych ofiar, kliknięcie „kłódki" i rzut oka na certyfikat to początek i koniec sprawdzania wiarygodności sklepu. Dlatego szerokim łukiem omijaj „sklepy" bez tych zabezpieczeń, ale z drugiej strony, jeśli są, nie traktuj ich jako gwarancji bezpiecznych zakupów.

- Czytaj opinie. Te o sklepie też, chociaż licz się z tym, że piszą je nie tylko klienci. Część może być autorstwa samych zainteresowanych, a część mogła napisać zawistna konkurencja.

  Bardziej wartościowe są opinie o kupionych towarach, te pozytywne i te negatywne, bo świadczą o tym, że zamówienie zostało zrealizowane.

- Jeśli sklep oferuje możliwość zakupów bez konieczności rejestracji, skorzystaj z niej. Zawsze to jeden internetowy ślad mniej.
- Gdybyś został „zmuszony" do założenia sklepowego konta i chcesz płacić kartą, nie podpinaj jej na stałe. Jeśli jest to niezbędne, po dokonaniu zakupu usuń kartę jako metodę płatności.
- Nie podawaj innych danych niż teleadresowe i te niezbędne do wykonania płatności. Żądanie numeru PESEL, daty urodzenia czy numeru rachunku bankowego powinno być równoznaczne z Twoim wyjściem z takiego „sklepu".
- Płać kartą płatniczą bądź przy odbiorze przesyłki. W pierwszym przypadku masz możliwość skorzystania z procedury reklamacyjnej *„chargeback"* (kłania się krok nr 1 i samokształcenie) oraz duże szanse na odzyskanie pieniędzy (niemożliwe, gdy oszustowi zapłacisz przelewem). W drugim przypadku, wiadomo.
- Unikaj sklepów, które oferują **tylko** przelew bankowy jako formę zapłaty, za nie wysłany jeszcze towar.
- Zachowaj korespondencję ze sklepem oraz wszelkie dokumenty dotyczące Twojego zamówienia i płatności

W tak krótkim(?) opracowaniu nie sposób wymienić i opisać wszystkich niebezpieczeństw i pułapek, z którymi możesz zetknąć się w Internecie przy okazji zakupów lub w czasie korzystania z internetowej bankowości. Ale stosując się do powyższych wskazówek i poszukując w innych źródłach brakującej, a potrzebnej Ci wiedzy, zmniejszasz prawdopodobieństwo zostania ofiarą oszustów. A ci nie śpią i doskonalą swój fach.

Dlatego, jeśli chcesz być na bieżąco i wiedzieć z czym możesz się spotkać, rozważ zainstalowanie aplikacji *CyberAlerty*, dostępnej w wersji na Android oraz na iOS.

Opracowano w Kole nr 3
SEiRP
w Tychach