ZWIĄZEK BANKÓW POLSKICH

Warszawa, 31 marca 2022 r.

W związku z coraz większym zapotrzebowaniem na usługi i aktywnością obywateli Ukrainy na rynku bankowym, Związek Banków Polskich i FinCERT.pl - Bankowe Centrum Cyberbezpieczeństwa ZBP przygotowały zbiór najważniejszych informacji i porad, które pozwalają uchronić się przed atakami cyberprzestępców. Porady zostały przygotowane również w języku ukraińskim.

Zasady cyberbezpieczeństwa – bezpieczna bankowość. Chroń swoje pieniądze i tożsamość!

BEZPIECZNE KORZYSTANIE Z BANKOMATU

Na co zwrócić uwagę:

1. Ilość osób zebranych w pobliżu bankomatu i ich zachowanie;
2. dodatkowe/nadmiarowe wyposażenie bankomatu np.: nakładka na klawiaturę lub dodatkowe, ukryte oko kamery lub zainstalowana oszukańcza nakładka na wlot karty;
3. lokalizacja bankomatu w zaułku, miejscu oddalonym od głównych traktów, słabo oświetlona;
4. osoba podążająca za tobą po wypłacie środków.

Jak się chronić:

1. sprawdź czy za Tobą lub w bliskiej okolicy nie stoją osoby obce, które mogą podpatrzeć Twój PIN, lub takie które tworzą sztuczny tłum by odwrócić Twoją uwagę, a następnie ukraść kartę lub gotówkę np. symulując omdlenie czy upuszczenie przedmiotu;
2. jeszcze przed włożeniem karty do bankomatu sprawdź czy w bankomacie lub jego bliskiej okolicy nie zostało zainstalowane dodatkowe „oko kamery" lub czy klawiatura nie jest wypukła lub zniekształcona – za pomocą tych urządzeń oszuści mogą pozyskać PIN do karty;
3. sprawdź czy wlot na kartę nie posiada żadnych dodatkowych nakładek lub elementów działających jak magnes, które można oderwać czy odkleić- umożliwiają one oszustom pozyskanie danych z paska magnetycznego Twojej karty;
4. dokładnie obejrzyj podajnik gotówki, nie powinien mieć doklejonej nietypowej listwy, która uniemożliwi wyciągnięcie banknotów;

5. zwróć uwagę na odstające elementy, różnego rodzaju naklejki, ślady wiercenia, zniszczenia, elementy wyglądające na nieprofesjonalne;
6. wypłacając pieniądze stań blisko maszyny i zasłoń swoim ciałem ekran i klawisze dodatkowo zasłoń też ręką klawiaturę;
7. jeśli wygląd lub funkcjonowanie bankomatu wzbudzi Twoje podejrzenia, nie wykonuj transakcji;
8. korzystaj z bankomatów w miejscach chronionych i dobrze oświetlonych np.: placówki bankowe;
9. wypłacone środki przechowuj w bezpiecznym miejscu. Po ich wypłaceniu upewnij się, że nie idzie za Tobą osoba, która będzie chciała ukraść Ci torebkę lub portfel.

BEZPIECZEŃSTWO KODU PIN LOGINÓW i HASEŁ DO BANKOWOSCI INTERNETOWEJ ORAZ KODÓW AUTORYZACYJNYCH OTRZYMYWANYCH Z BANKU

Na co zwrócić uwagę:

1. stopień skomplikowania PIN- u, loginu i hasła;
2. możliwość ich ujawnienia np.: po kliknięciu w link lub podczas rozmowy telefonicznej.

Jak się chronić:

1. nigdy nie zapisuj PIN-u loginów i haseł do bankowości internetowej, chyba że korzystasz z narzędzi do tego przeznaczonych. Nikomu nie udostępniaj tych informacji – to Twoja tożsamość;
2. wymyśl PIN, login i hasało trudne do odgadnięcia - nie powinna być to data urodzin, powtarzające się po sobie takie same cyfry czy imię i nazwisko;
3. jeśli posiadasz kilka kont, każdemu nadaj inny login i hasło. Dla każdej karty nadaj różny PIN;
4. uważnie czytaj otrzymywane z banku komunikaty (sms/mail) mogą dotyczyć operacji, której faktycznie nie chcesz wykonać, np. zmiany lub nadania haseł lub dodania zaufanych urządzeń;
5. reaguj szybko na otrzymane z banku komunikat o nieautoryzowanej przez Ciebie próbie logowania na Twoje konto lub transakcji, której nie wykonywałeś;
6. zmieniaj te dane co pewien czas np.: co poł roku oraz zawsze, gdy masz podejrzenie, że mogły zostać ujawnione;
7. rozważ, czy warto skorzystać z usług dodatkowych tj.; alert po każdej transakcji lub informacja o stanie konta na koniec dnia;
8. sprawdzaj wyciąg z konta, w przypadku podejrzanych transakcji zgłoś problem swojemu bankowi;
9. nikomu nie pożyczaj swojej karty.

UWAGA!!! STRACIŁEŚ KARTĘ? NIE RYZYKUJ

Skorzystaj z wygodnego systemu do zastrzegania kart bankomatowych. Wprowadź do książki telefonicznej w swoim telefonie numer infolinii międzybankowej (+48) 828-828-828. Jeśli zgubiłeś swoją kartę płatniczą lub została Ci ona skradziona, natychmiast zadzwoń (+48) 828-828-828 i wypowiedz nazwę banku, a system połączy Cię z Twoim bankiem. Następnie odpowiedz na kilka pytań weryfikujących i bezpłatnie zastrzeż swoją kartę.

OFERTY PRACY NA PORTALACH SPOŁECZNNOŚCIOWYCH I SPRZEDAŻOWYCH, CHROŃ SWOJĄ TOŻSAMOŚĆ

Na co zwrócić uwagę:

1. intratne oferty pracy umieszczone w gazetach, portalach społecznościowych czy sprzedażowych, które kuszą wyjątkowym/nierealnym zarobkiem przy jednoczesnym braku wymogu doświadczenia w zawodzie np.: salon masażu, transfer środków pieniężnych;
2. przekazywanie/powierzanie danych zawartych w dokumencie tożsamości, uczciwy pracodawca nigdy nie żąda przekazania dokumentu tożsamości na przechowanie;
3. sposób przechowywania dokumentu tożsamości;
4. zagubienie lub utrata dowodu.

Jak się chronić:

1. nie zostawiaj dokumentów w miejscach publicznych lub w punktach usługowych np.:, agencji nieruchomości czy pośrednictwa pracy, wypożyczalni aut;
2. nie udostępniaj skanu dokumentu potencjalnemu pracodawcy, który proponuje intratną ofertę pracy, może wykorzystać Twój dokument do zaciągnięcia pożyczki lub działalności przestępczej np.: pranie pieniędzy;
3. nigdy nie powierzaj na przechowanie dokumentu tożsamości, osoba może cię szantażować i ograniczyć twoją swobodę.

UWAGA!!! STRACIŁEŚ DOKUMENT TOŻSAMOSCI? NIE RYZYKUJ

W przypadku zagubienia lub utraty dokumentu tożsamości konieczne jest jego ZASTRZEŻENIE. Udaj się do swojego banku lub jeśli to niemożliwe do najbliższej placówki bankowej dowolnego banku. W kilka minut informacja dotrze do wszystkich banków w Polsce, Poczty Polskiej oraz operatorów telefonii komórkowej, a Twoja tożsamość będzie bezpieczna i nikt nie będzie mógł już potwierdzić tożsamości na podstawie Twojego dokumentu. Dokument zastrzegany jest w systemie DOKUMENTY ZASTRZEŻONE. Sprawdź na: www.dokumentyzastrzezone.pl.

BEZPIECZNA ROZMOWA Z PRACOWNIKIEM BANKU LUB INNĄ OSOBĄ PODAJACĄ SIĘ ZA PRACOWNIKA INSTYTUCJI ZAUFANIA PUBLICZNEGO;

Na co zwrócić uwagę:

1. połączenia telefoniczne podczas, których osoba przedstawiająca się informuje, że działa z ramienia instytucji zaufania publicznego np.: policji, straży granicznej, urzędu miasta lub gminy, urzędu do spraw cudzoziemców, ambasady czy pracownika banku (uwaga: na *urządzeniu ofiary może wyświetlić się oficjalny numer telefonu przypisany do danej instytucji*) oraz jednocześnie podczas rozmowy żąda lub intensywnie nalega na przekazanie pieniędzy, numerów PIN, kodów autoryzacyjnych, danych poufnych służących do logowania do bankowości internetowej, kodów służących do dodania urządzenia zaufanego lub nakłania ofiarę do zainstalowania aplikacji dającej przestępcom zdalny dostęp do komputera ofiary;

2. żądanie oszust uwiarygadnia odpowiednią historią np.: udziałem w tajnej akcji związanej z rozbiciem grupy przestępczej, zagrożeniem związanym z kradzieżą środków z konta bankowego czy potrzebą uzupełnienia wniosków urzędowych o dane wrażliwe itp.; ulegając presji atakowane w ten sposób osoby „dobrowolnie" dokonują przelewu środków np.: na rzekome operacyjne konta policji lub udostępniają dane, które oszustom służą do logowania do usług bankowości internetowej i mobilnej, aby przejąć środki osób pokrzywdzonych.

Jak się chronić:

1. nigdy nie ujawniaj kodów do bankowości internetowej oraz kodów 3D Secure wykorzystywanych do autoryzacji transakcji kartowych w Internecie, przychodzących na telefon;
2. zawsze czytaj treść SMS-ów jakie przychodzą na telefon lub komunikatów w aplikacji mobilnej w trakcie połączenia z rzekomym policjantem, urzędnikiem itp.; (z ich treści może wynikać, że akceptuje się transakcję, którą przygotowali przestępcy);
3. jeżeli rozmowa wzbudza jakiekolwiek wątpliwości lub niepokój, rozłącz się, odczekaj minimum 30 sekund, a następnie samodzielnie połączyć się z instytucją, z której telefonował rzekomy przedstawiciel (w takim przypadku koniecznie należy wybrać oficjalny numer na klawiaturze numerycznej zamiast oddzwaniać na wcześniejsze połączenie);
4. zachowaj zdrowy rozsądek i zimną krew, nawet jeżeli zostałeś poinformowany/zostałaś poinformowana o potencjalnym zagrożeniu np.: o utracie środków; należy ze spokojem zastanowić się, czy środki naprawdę mogą być zagrożone, czy może rozmowa prowadzona jest z oszustem, który chce wykorzystać sytuację i skłonić nas do pochopnej decyzji; dobrym krokiem będzie przerwanie połączenia i ponowne jego zainicjowanie zgodnie z zasadą powyżej;
5. należy zawsze mieć świadomość, że wyświetlony numer telefonu lub nazwa banku nie są gwarancją, że rozmawiamy z prawdziwym urzędnikiem; dlatego nie należy podawać żadnych informacji poufnych, w szczególności w sytuacji, kiedy kontakt jest inicjowany z zewnątrz, a nie przez nas samych.

LINKI I WIADOMOŚCI SMS DOTYCZĄCE ZBIÓRKI LUB INFORMUJĄCE O NIEDOPŁACIE LUB PRZESYŁCE POCZTOWEJ

Na co zwrócić uwagę:

1. treść otrzymywanych komunikatów jest emocjonalna, informuje o zbiórce na rzecz uchodźców lub poszkodowanych podczas wojny JEDNOCZEŚNIE wiadomość zawiera aktywny link kierujący do zbiórki;

Jak się chronić:

1. nie klikaj w link z sms lub wiadomości mailowej, gdyż może skutkować to między innymi ujawnieniem danych poufnych służących do logowania się do bankowości internetowej lub mobilnej lub wykonaniem płatności oszukańczej, uruchomieniem szkodliwego oprogramowania, które np. pozwoli przejąć kontrolę nad urządzeniem lub zbierze i przekaże przestępcom nasze dane wrażliwe lub zaszyfrowaniem urządzenia;

2. zgłoszenie podejrzanej wiadomości zawierającej aktywne linki do CSIRT NASK pod numer 799-448-084. wystarczy użyć w telefonie funkcję „przekaż” albo „udostępnij” i wiadomość odesłać pod ww. numer;
3. usuń taką wiadomość (aby w przyszłości uniknąć przypadkowego kliknięcia na niebezpieczny link).

FinCERT.pl - Bankowe Centrum Cyberbezpieczeństwa ZBP - Centrum Wymiany i Analiz Informacji Sektora Finansowego

_____

FinCERT.pl - Bankowe Centrum Cyberbezpieczeństwa ZBP – jednostka operacyjna funkcjonująca w ramach Zespołu Bezpieczeństwa 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 oraz ich klientów.

Правила кібербезпеки - безпечний банкінг. Захистіть свої гроші та свою ідентичність!

БЕЗПЕЧНЕ КОРИСТУВАННЯ БАНКОМАТОМ

На що звернути увагу:

1. Кількість людей, що зібралися біля банкомату, та їх поведінка;
2. додаткове / надмірне і нетипове обладнання банкоматів, наприклад, накладка на клавіатуру або додаткова прихована камера або встановлена шахрайська накладка там, де ви вкладаєте картку;
3. розташування банкомату в провулку, місці, віддаленому від основних шляхів, погано освітленому;
4. особа, яка йде за вами після того, як Ви зняли гроші.

Як захистити себе:

1. перевірте, чи немає позаду Вас чи поблизу незнайомців, які можуть підглянути Ваш ПІН-код, чи тих, хто створює штучний натовп, щоб відвернути Вашу увагу, а потім вкрасти картку чи готівку, наприклад, імітуючи непритомність чи впустивши на землю якийсь предмет;
2. перед тим, як вставити картку в банкомат, перевірте, чи не встановлено додаткове «око камери» в банкоматі або поруч з ним, чи клавіатура не опукла і чи не здеформована – шахраї можуть використовувати різні пристрої для отримання ПІН-коду картки;

3. перевірте, чи немає на вхідному отворі для картки додаткових накладок або елементів, які діють як магніт, які можна відірвати або відклеїти – вони дозволяють шахраям отримати дані з магнітної смужки Вашої картки;
4. уважно огляньте банкомат, на ньому не повинно бути прикріпленої нетипової планки, яка унеможливить вилучення банкнот;
5. зверніть увагу на виступаючі елементи, різні наклейки, , пошкодження, елементи, які виглядають не професійно;
6. під час зняття грошей станьте близько до апарату і закрийте тілом екран і клавіші, додатково прикрийте клавіатуру рукою;
7. якщо у Вас є підозра щодо зовнішнього вигляду або функціонування банкомату, не виконуйте транзакцію;
8. користуйтеся банкоматами, які розташовані в захищених і добре освітлених місцях, наприклад, у відділеннях банків;
9. зберігайте зняті гроші в надійному місці. Після їх зняття, переконайтеся, що за вами не йде особа, яка захоче вкрасти ваш гаманець або сумку.

БЕЗПЕКА ПІН-КОДУ, ЛОГІНІВ, ПАРОЛЕЙ ДО ІНТЕРНЕТ-БАНКІНГУ ТА КОДІВ АВТОРИЗАЦІЇ, ОТРИМАНИХ З БАНКУ

На що звертати увагу:

1. складність ПІН-коду, логіна та пароля;
2. можливість їх розкриття, наприклад, після натискання на посилання або під час телефонної розмови.

Як захистити себе:

1. ніколи не записуйте ПІН-код, логіни і паролі для онлайн-банкінгу, якщо Ви не використовуєте призначені для цього інструменти. Не передавайте цю інформацію нікому – це Ваша конфіденційна інформація;
2. придумайте ПІН-код, логін і пароль, які важко відгадати - це не повинен бути день народження, ланцюг однаковихі цифр або ім'я та прізвище;
3. якщо у Вас кілька рахунків, надайте кожному інший логін і пароль. Дайте кожній картці інший ПІН-код;
4. уважно читайте повідомлення (sms/e-mail), отримані з банку, вони можуть стосуватися операції, яку Ви насправді не бажаєте виконувати, наприклад, зміни або призначення паролів або додавання непотрібних пристроїв;
5. швидко реагуйте на отримане з банку повідомлення про несанкціоновану спробу входження на Ваш рахунок або транзакцію, яку Ви не проводили, або не доручали проводити;
6. змінюйте ці дані час від часу, наприклад, кожні шість місяців і щоразу, коли Ви підозрюєте, що вони могли бути розголошені;
7. подумайте, чи варто користуватися додатковими послугами, такими як сповіщення після кожної операції або інформацією про залишок на рахунку в кінці дня;
8. перевіряйте виписку з рахунку, у разі підозрілих операцій повідомте про проблему у свій банк;
9. нікому не позичайте свою картку.

УВАГА!!! ВИ ВТРАТИЛИ КАРТКУ? НЕ РИЗИКУЙТЕ

Скористайтеся зручною системою блокування карток до банкоматів. Введіть номер міжбанківської гарячої лінії (+48) 828-828-828 в телефонну книгу свого телефону. Якщо Ви згубили свою платіжну картку або її вкрали, негайно зателефонуйте за номером (+48) 828-828-828 і скажіть назву свого банку, система з'єднає Вас із Вашим банком. Потім дайте відповідь на кілька запитань для підтвердження своєї особи і безкоштовно заблокуйте свою картку.

ПРОПОЗИЦІЇ РОБОТИ НА СОЦІАЛЬНИХ ПОРТАЛАХ ТА ПОРТАЛАХ ПРОДАЖІВ, ЗАХИСТІТЬ СВОІ ПЕРСОНАЛЬНІ ДАНІ

На що звернути увагу:

1. вигідні пропозиції роботи, опубліковані в газетах, соціальних мережах або на порталах продажів, які спокушають винятковими / нереальними заробітками без вимог до досвіду роботи за професією, наприклад, масажний кабінет, грошові перекази;
2. передача/довірення даних, що містяться в документі, що посвідчує особу, чесний роботодавець ніколи не Вимагатиме від Вас передати документ, що посвідчує особу, на зберігання;
3. спосіб зберігання документа, що посвідчує особу;
4. загублення або втрата посвідчення особи.

Як захистити себе:

1. не залишайте документи в громадських місцях або в пунктах обслуговування, наприклад, в агентствах нерухомості чи працевлаштування, в пунктах прокату автомобілів;
2. не передавайте скан документу потенційному роботодавцю, який пропонує вигідну роботу, він може використати Ваш документ для отримання позики або здійснення злочинної діяльності, наприклад, відмивання грошей;
3. ніколи не довіряйте іншій особі зберігання Вашого документа, що посвідчує особу, ця особа може шантажувати Вас і обмежити Вашу свободу.

УВАГА!!! ВИ ВТРАТИЛИ ДОКУМЕНТ, ЩО ПОСВІДЧУЄ ОСОБУ? НЕ РИЗКУЙТЕ

У разі загублення або втрати документа, що посвідчує особу, його необхідно ЗАСТЕРЕГТИ Зверніться до свого банку або, якщо це неможливо, до найближчого відділення будь-якого банку. За кілька хвилин інформація надійде до всіх банків Польщі, Польської Пошти та операторів мобільного зв'язку, і Ваша ідентичність (ваші персональні дані) буде в безпеці, і ніхто не зможе підтвердити свою особу на підставі Вашого документа. Документ застерігається в системі ЗАСТЕРЕЖЕНІ ДОКУМЕНТИ. Перевірте: www.dokumentyzastrzezone.pl .

БЕЗПЕЧНА РОЗМОВА З ПРАЦІВНИКОМ БАНКУ АБО ІНШОЮ ОСОБОЮ, ЯКА ПОДАЄ СЕБЕ ЗА ПРАЦІВНИКА УСТАНОВИ ПУБЛІЧНОЇ ДОВІРИ

На що звернути увагу:

1. телефонні дзвінки, під час яких особа, яка представляється, повідомляє, що діє від імені установи публічної довіри, наприклад, поліції, прикордонної служби, міської чи комунальної служби, управління у справах іноземців, посольства чи банку (увага: *на пристрої жертви може відображатися офіційний номер телефону даної установи*) і водночас під час розмови ця особа просить або наполягає на переказі грошей, ПІН-кодів, кодів авторизації, конфіденційних даних, які використовуються для входу в Інтернет-банкінг, кодів, що застосовуються для додавання надійного пристрою (ноутбука, планшета, телефону, веб-браузера, який використовується для входу в інтернет-банкінг) або переконує жертву встановити програму, яка надасть злочинцям віддалений доступ до комп'ютера жертви;
2. свою вимогу шахрай підкріплює відповідною історією, наприклад, участю у таємній операції, пов'язаній з розбиттям злочинної групи, небезпекою викрадення коштів з банківського рахунку або необхідністю доповнити офіційні заяви конфіденційними даними,тощо; піддавшись тиску, люди, атаковані таким чином, «добровільно» перераховують кошти, наприклад, на нібито оперативні рахунки поліції або надають дані, які шахраї використовують для входу до послуг інтернет-банкінгу або мобільного банкінгу, щоб заволодіти грошима жертв.

Як захистити себе:

1. ніколи не розкривати коди для інтернет-банкінгу та коди 3D Secure, які використовуються для авторизації карткових транзакцій в Інтернеті, що надходять на телефон;
2. завжди читайте зміст SMS-повідомлень, які приходять на телефон, або повідомлень в мобільному додатку під час розмови з нібито поліцейським, чиновником тощо; (їх зміст може свідчити, що Ви погоджуєтеся на транзакцію, підготовлену злочинцями);
3. якщо розмова викликає будь-які сумніви чи занепокоєння, покладіть слухавку, зачекайте не менше 30 секунд, а потім самі подзвоніть до установи, з якої дзвонив імовірний представник (у цьому випадку необхідно набрати офіційний номер на цифровій клавіатурі, а не віддзвонювати на вхідний номер);
4. користуйтеся здоровим глуздом і не підходьте до справи емоційно, навіть якщо Вам повідомили про потенційну небезпеку, наприклад, про втрату коштів; слід спокійно подумати, чи дійсно кошти можуть бути під загрозою, чи може розмова ведеться з шахраєм, який хоче скористатися ситуацією і переконати Вас прийняти поспішне рішення; хорошим кроком буде перервати з'єднання та повторно ініціювати його згідно з наведеним вище правилом;
5. Ви завжди повинні пам'ятати про те, що висвітлений на екрані номер телефону або назва банку не є гарантією того, що Ви розмовляєте зі справжнім працівником цієї установи; тому не слід надавати конфіденційну інформацію, особливо коли контакт ініційовано ззовні, а не Вами.

ПОСИЛАННЯ ТА СМС-ПОВІДОМЛЕННЯ, ЩО СТОСУЮТЬСЯ ЗБІРКИ ГРОШЕЙ, ПОВІДОМЛЕННЯ ПРО НЕДОПЛАТУ АБО ПОШТОВУ ДОСТАВКУ

На що звернути увагу:

1. емоційний зміст отриманих повідомлень, інформує про збір коштів для біженців або постраждалих від війни, ОДНОЧАС повідомлення містить активне посилання на збір коштів;

Як захистити себе:

1. не натискайте на посилання з текстового повідомлення або електронної пошти, оскільки це може призвести, серед іншого, до розголошення конфіденційних даних, які використовуються для входу в інтернет або мобільний банкінг, або до здійснення шахрайського платежу, запуску шкідливого програмного забезпечення, яке, наприклад, дозволить взяти під контроль Ваш пристрій або збиратиме та передаватиме злочинцям Ваші конфіденційні дані або приведе до шифрування пристрою ;
2. заявіть про підозріле повідомлення з активними посиланнями до CSIRT NASK за номером 799-448-084, для цього скористайтеся в телефоні функцією «Переслати» або «Поділитися» та відправте це повідомлення на вищезгаданий номер;
3. видаліть таке повідомлення (щоб уникнути випадкового натискання небезпечного посилання в майбутньому).