BANK SPÓŁDZIELCZY ZIEMI KRAŚNICKIEJ W KRAŚNIKU

ZASADY BEZPIECZEŃSTWA

DLA KLIENTÓW

KORZYSTAJĄCYCH Z BANKOWOŚCI INTERNETOWEJ

Bank Spółdzielczy Ziemi Kraśnickiej w Kraśniku
23-200 Kraśnik ul. Ogrodowa 5
Sąd Rejonowy w Lublinie, XI Wydział Gospodarczy KRS,
KRS 0000087630, NIP 715-000-00-92
tel. (0-81) 884-06-00, fax. (0-81) 884-04-44

Bank Spółdzielczy Ziemi Kraśnickiej umożliwia swoim Klientom dostęp do usług związanych z prowadzeniem rachunków z wykorzystaniem elektronicznych kanałów informacji. To wygodne rozwiązanie pozwalające na obsługę rachunków niemal z każdego miejsca na świecie. Równolegle z tym komfortem podąża jednak ryzyko związane z niebezpieczeństwami czyhającymi na osoby, które nie zdają sobie sprawy z zagrożeń związanych z korzystaniem z Internetu.

Niniejszy dokument ma zwrócić Państwa uwagę na najczęstsze zagrożenia i wyjaśnić, w jaki sposób uchronić się przed nadużyciami. Pragniemy wraz z Państwem minimalizować ryzyko wystąpienia sytuacji kryzysowych poprzez budowanie świadomości zagrożeń. Zagrożeń, które ewoluują wraz z udoskonalaniem systemów zabezpieczeń.

W przeszłości przestępcy korzystali zwykle z rozwiązań technicznych, aby „dobrać się" do środków finansowych. Do dziś zresztą tego typu zagrożenia istnieją. Często w ten sposób okrada się konta poprzez nieuprawnione wejście w posiadanie danych kart płatniczych poprzez najróżniejsze nakładki na bankomatach.

Jeśli jednak chodzi o nadużycia dnia dzisiejszego, to najczęściej jesteśmy – jako klienci banków – narażeni na ataki socjotechniczne. Nie opłaca się bowiem w wielu przypadkach stosować rozwiązań technologicznych, skoro o wiele łatwiej wzbudzić w potencjalnej ofierze ataku zaufanie. I właśnie z tego typu zagrożeniami jest dziś w skali globalnej najwięcej problemów.

Jak więc bezpiecznie korzystać z bankowości internetowej minimalizując ryzyko ataku? Trzeba się stosować do kilku prostych zasad, które można streścić jednym sformułowaniem – **ograniczone zaufanie**. Przecież nie zaniosą Państwo swoich pieniędzy do śmierdzącego typa w łachmanach siedzącego w obskurnej bramie gdzieś w szemranej dzielnicy, prawda? Poszukają Państwo normalnego banku, często z tradycjami, z siecią placówek, z gwarancjami Bankowego Funduszu Gwarancyjnego. I tak samo należy postępować z bankowością internetową – wybierać zaufanych dostawców i nie dać się naciągać na dziwne propozycje.

Bank Spółdzielczy Ziemi Kraśnickiej ze swojej strony zapewnia możliwie bezpieczne rozwiązania stosując światowej klasy technologie. Korzystając z oferowanej przez nas bankowości internetowej i stosując się do kilku zasad zapewniają Państwo wysoki poziom bezpieczeństwa swoich transakcji. Na następnych stronach omówimy najistotniejsze kwestie pozwalające na bezpieczne i rozważne korzystanie z nowych technologii.

OCHRONA ŚRODOWISKA PRACY

Bardzo ważne jest zapewnienie bezpiecznego środowiska, z którego dokonują Państwo logowania się do systemu bankowości internetowej oraz przeprowadzają tam Państwo swoje transakcje. Podstawowe elementy, na które trzeba zwrócić uwagę, to:

- **aktualny i wspierany system operacyjny** (z reguły Windows) z wgranymi aktualizacjami i zabezpieczeniami przygotowanymi przez twórców owego systemu; należy instalować wszystkie niezbędne łatki, aktualizacje i zabezpieczenia – można ustawić automatyczne aktualizacje; nie należy korzystać z systemów, dla których skończyło się tzw. wsparcie, czyli nie są już przygotowywane wspomniane wcześniej aktualizacje i łatki;
- **aktualna wersja przeglądarki internetowej** z wgranymi aktualizacjami i zabezpieczeniami; w przypadku bankowości dla klientów korporacyjnych system operacyjny i przeglądarka muszą umożliwiać obsługę środowiska Java;
- **aktualny program antywirusowy**; zalecamy korzystanie z płatnych wersji, a nie darmowych rozwiązań; ważne, żeby program automatycznie i często aktualizował sygnatury wirusów – im bardziej aktualną ma ich bazę, tym lepiej; dobry program antywirusowy powinien też być wyposażony w mechanizmy wykrywające nieznane jeszcze zagrożenia, a także w filtrowanie poczty elektronicznej pod kątem zagrożeń; program antywirusowy powinien działać przez cały czas, a nie tylko na żądanie;
- **firewall**, zwany też zaporą ogniową – oprogramowanie, bądź urządzenie zabezpieczające system komputerowy przed niepożądanym ruchem sieciowym; jest w stanie wyfiltrować niewłaściwe zachowania i chroni komputer przed wieloma zagrożeniami z Internetu; dobrze skonfigurowany firewall analizuje i filtruje zarówno ruch przychodzący z Internetu, jak i wychodzący z komputera;
- **ważność certyfikatów**; jeśli przeglądarka wyświetla komunikaty o błędach certyfikatów, to nie należy kontynuować pracy na takiej stronie; w przypadku wątpliwości należy się skontaktować z Bankiem, o ile oczywiście komunikaty byłyby wyświetlane przez stronę BSZK lub naszą stronę bankowości internetowej;
- **rozsądna obsługa poczty elektronicznej**; nie należy otwierać poczty z nieznanych źródeł, zwłaszcza, jeśli dołączono do niej jakiekolwiek załączniki; nie powinno się też klikać na odsyłacze (linki) w takiej korespondencji; nie należy podawać jakichkolwiek danych wrażliwych osobom nieznanym, które nawiązały z Państwem nieoczekiwany kontakt;

- **instalacja oprogramowania**; nie należy instalować oprogramowania pochodzącego z nieznanych źródeł; po instalacji jakichkolwiek aplikacji warto zawsze uruchomić skanowanie systemu programem antywirusowym;
- **sieci Wi-Fi i sieci publiczne**; nie należy korzystać z bankowości elektronicznej poprzez sieci Wi-Fi i sieci publiczne; nie należy też korzystać z obcych, niezaufanych komputerów;
- **korzystanie z komputera na systemowym koncie użytkownika bez praw administratora**; kont z prawem administratora systemu operacyjnego należy używać jedynie do konfiguracji systemu, codzienna praca powinna się odbywać na koncie użytkownika, który nie posiada uprawnień administracyjnych systemu operacyjnego;
- **zapewnienie prywatności**; komputera, z którego dokonują Państwo logowania i obsługi bankowości elektronicznej nie należy udostępniać osobom trzecim; nie powinien to też być komputer wykorzystywany przez dzieci, zwłaszcza jeśli korzystają z gier internetowych i przeglądają Internet; jeśli takie współużytkowanie jest nieuniknione, należy dla takiego użytkownika stworzyć konto w systemie operacyjnym z bardzo ograniczonymi prawami;
-- **czytanie komunikatów generowanych przez system i aplikacje**; obserwuje się powszechne zatwierdzanie pojawiających się w systemie komunikatów, nie tylko bez próby ich zrozumienia, ale nawet bez czytania! to niedopuszczalne! należy przeczytać i zrozumieć komunikat, a w przypadku jakichkolwiek wątpliwości skontaktować się z osobą, która wyjaśni wyświetlony przekaz;

OCHRONA DANYCH WRAŻLIWYCH

W dobie ataków socjotechnicznych szalenie istotne jest zachowanie wysokiej poufności wszelkich danych wrażliwych. Do takich niewątpliwie należą elementy dostępowe uzyskane z banku – w naszym przypadku identyfikatory, hasła, tokeny, czy karty chipowe. Stosowane przez Bank Spółdzielczy Ziemi Kraśnickiej rozwiązania zapewniają wielowątkowe potwierdzanie tożsamości osoby korzystającej z bankowości internetowej. Są to:

- <u>w przypadku rozwiązań z tokenem lub autoryzacją przez SMS:</u> identyfikator użytkownika, indywidualnie przez niego ustawiane i regularnie zmieniane hasło; hasło maskowane, token lub autoryzacja przez SMS;
- <u>w przypadku rozwiązań z kartą:</u> identyfikator użytkownika, indywidualnie przez niego ustawiane i regularnie zmieniane hasło; karta chipowa, PIN do karty.

Podkreślmy tu istotność konieczności regularnej zmiany hasła oraz jego złożoność. Zaleca się, aby hasło było zmieniane nie rzadziej, niż raz na miesiąc, by było ono możliwie długie, by składało się z liter (małych i dużych), cyfr i znaków specjalnych oraz należy unikać haseł prostych do zgadnięcia – imion, nazwisk, dat, nazw własnych. I – oczywiście – w żadnym razie nie należy haseł zapisywać w miejscach dostępnych dla osób postronnych! Nie należy stosować takich samych lub podobnych haseł do różnych celów, różnych aplikacji.

Prosimy pamiętać o konieczności zachowania pełnej poufności haseł, PIN-ów i identyfikatorów oraz o bezpiecznym przechowywaniu tokenów, telefonu komórkowego, kart i czytników do nich. Wszak aby zalogować się do bankowości internetowej i zrealizować polecenie przelewu, potrzebne są zarówno wiedza o identyfikatorach, hasłach i PIN-ach, jak i fizyczne elementy dostępu – w przypadku naszego Banku tokeny, telefon komórkowy, bądź karty chipowe z ich czytnikami. Zabezpieczając dostęp do tych elementów w dużej mierze dbają Państwo o bezpieczeństwo swoich środków.

WIEDZA O ZAGROŻENIACH

Jak wspominaliśmy, wiele ataków w ostatnich czasach odbywa się z zastosowaniem rozwiązań socjotechnicznych. Pomysłowość przestępców jest nieograniczona, a znajomość socjotechniki momentami zdumiewająca. Za to odporność na takie ataki nie wymaga od użytkownika bankowości internetowej praktycznie żadnych nakładów – wystarczy odpowiednia wiedza i rozsądny brak zaufania. Niestety w naszym kraju wciąż bywa z tym różnie – mimo wieloletniego informowania przez media wciąż wiele osób daje się oszukać metodami „na wnuczka", „na policjanta", „na inkasenta" itp. Wciąż wiele osób okazuje nadmierne zaufanie ludziom, których nie tylko nie zapraszali, ale których widzą/słyszą pierwszy raz w życiu. I podobnie jest z bankowością internetową: wysoki poziom czujności, zwracanie uwagi na to, co dzieje się na ekranie, czytanie komunikatów przed ich zatwierdzeniem, ignorowanie niechcianych e-maili – to wszystko pozwala wyeliminować zdecydowaną większość zagrożeń socjotechnicznych.

Prosimy pamiętać, że **nasz Bank nigdy nie wysyła powiadomień mailowych ani SMS-owych o jakichkolwiek pracach serwisowych, czy problemach z dostępem do konta internetowego. Nie prosimy też w ten sposób o instalację jakichkolwiek certyfikatów**. Możemy Państwa informować o planowanych pracach serwisowych wewnętrzną korespondencją, czyli przez pocztę stanowiącą moduł bankowości internetowej. Te wiadomości jednak otrzymują Państwo już po zalogowaniu się

do bankowości internetowej. Nigdy nie prowadzimy mailingu na adresy e-mail, których podawania zresztą od Państwa nie oczekujemy.

Niezależnie od tego zawsze należy zachować szczególną ostrożność. Nie powinno się otwierać e-maili od nieznajomych osób/instytucji, zwłaszcza takich przesyłek, których się Państwo nie spodziewają. Najlepiej od razu usunąć takie e-maile bez otwierania. Sugerujemy nie ustawiać programu pocztowego w trybie automatycznego podglądu maili, bo to równa się otwarciu takich listów elektronicznych, a stąd do zawirusowania komputera jest już bardzo blisko.

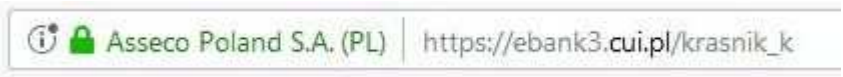
Nie powinni też Państwo klikać na odnośniki (linki) w takich e-mailach, bo mogą one prowadzić do serwisów, które błyskawicznie zainfekują Państwa system operacyjny. Również otwieranie załączników, nawet tak z pozoru niewinnych, jak dokumenty pakietów biurowych, może być niebezpieczne. Nie należy też włączać obsługi makr w takich dokumentach, jeśli nie są Państwo całkowicie pewni, że dokument pochodzi z zaufanego źródła.

Proszę też pamiętać, że dzisiejsze **smartfony**, to w istocie także komputery. Na nich też – niezależnie od tego, czy korzystają Państwo w ten sposób z bankowości elektronicznej, czy też nie – należy mieć zainstalowane oprogramowanie antywirusowe.

BEZPIECZNE ZACHOWANIA PODCZAS OBSŁUGI BANKOWOŚCI INTERNETOWEJ

Zawsze logując się do bankowości internetowej należy sprawdzać, czy połączenie jest szyfrowane, czy certyfikat jest wystawiony dla naszego Banku (lub firmy Asseco), a w przypadku niestandardowych sytuacji (np. strona internetowa oczekuje na powtórne podanie identyfikatora lub hasła, lub po nieudanej próbie logowania pojawia się komunikat, że trwają prace serwisowe i należy powrócić na stronę za kilka godzin) należy jak najszybciej skontaktować się z naszym Bankiem.

Jeśli chodzi o **połączenia szyfrowane i właściwe certyfikaty**, to bardzo ważne jest sprawdzenie, czy w pasku adresu zaznaczony jest szyfrowany protokół https, a sesja ma odpowiedni status potwierdzony zamkniętą kłódeczką. Warto sprawdzić, czy adres strony jest taki sam, jak zawsze.



Certyfikaty – zależnie od tego, czy jest to bankowość detaliczna, czy korporacyjna, są wystawione bądź na Bank Spółdzielczy Ziemi Kraśnickiej, bądź na Asseco Poland S.A. – naszego integratora,

dostawcę usługi i jednocześnie jedną z największych informatycznych firm w Europie działającą także na rynkach zagranicznych. Dodajmy, że Asseco jest polskim przedsiębiorstwem.

Jakiekolwiek identyfikatory, hasła, kody z tokenów itp. należy wpisywać tylko w wyznaczone, standardowe miejsca. Jeśli żądanie wpisania któregoś z elementów dostępu pojawia się w miejscu niestandardowym, należy natychmiast skontaktować się z Bankiem. Podobnie należy zachować się w przypadku wszelkich nietypowych komunikatów i poleceń.

Prosimy też zwrócić uwagę na fakt, że szyfrowanie połączenia odbywa się jedynie pomiędzy systemem operacyjnym Państwa komputera, a systemami bankowymi. To znaczy, że jeśli ktoś przejmie – za pośrednictwem odpowiedniego oprogramowania – kontrolę nad Państwa przeglądarką, to tutaj będzie możliwość wystąpienia nadużycia. Dlatego tak ważne jest posiadanie i używanie aktualnego oprogramowania antywirusowego dobrze radzącego sobie z różnego rodzaju zagrożeniami, m.in. z tzw. malware'em. To jednak nie wszystko. Trzeba zachować daleko idącą ostrożność podczas potwierdzania wykonania przelewów: **należy bezwzględnie sprawdzać, czy potwierdza się zlecenie wysłania pieniędzy we właściwej kwocie, na właściwy rachunek i do właściwego odbiorcy**. Oczywiście w przypadku rozbieżności nie wolno autoryzować operacji i jak najszybciej sprawdzić system pod kątem wirusów.

Należy pamiętać, że zlecenie wystawione w bankowości elektronicznej jest takim samym zleceniem, jak złożenie przelewu papierowego w placówce banku. Poprawność wprowadzonych danych klient potwierdza osobiście i bierze za to pełną odpowiedzialność. W przypadku, gdy dojdzie do nieautoryzowanej przez klienta transakcji trzeba się liczyć z tym, że to po stronie Klienta leży zapewnienie poufności i integralności środków dostępu. Zalicza się tu także zapewnienie odpowiednich zabezpieczeń po stronie Klienta – oprogramowania antywirusowego, czy aktualności systemu operacyjnego. To Klient ma też potwierdzać przelew pod względem jego poprawności – kwoty i rachunku, na który są przekazywane środki.