Zasady bezpiecznego korzystania z bankowości elektronicznej

Korzystając z systemu EBO za pośrednictwem Internetu powinniśmy przestrzegać poniższych zasad:

Słownik pojęć:
malware - z angielskiego złośliwe oprogramowanie, czyli wszelkie aplikacje, skrypty itp. Które mają na celu złośliwe, szkodliwe lub przestępcze działanie wobec użytkownika komputera

ransomware - rodzaj oprogramowania malware, które uzyskuje dostęp do zasobów użytkownika, po czym blokuje dostęp do komputera, i szyfruje katalogi z plikami. Użytkownik otrzymuje informację, że dostanie dostęp do swoich zasobów pod warunkiem zapłacenia okupu.

hardening systemu operacyjnego -zespół działań podjętych w celu utwardzenia systemu operacyjnego, czyli mówiąc potocznie zatkaniu dziur. Odbywa się to poprzez wyłączenie usług uznanych za niebezpieczne, zamknięcie niepotrzebnych portów, wyłączenia dostępu niektórym urządzeniom np. pendrive'om, portom USB itp.

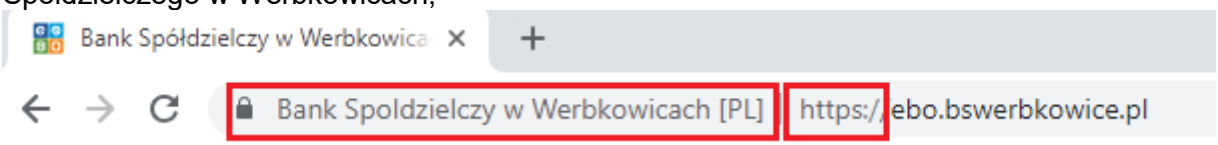
1. Nie podajemy danych do logowania do bankowości elektronicznej - poprzez mail/telefon/list - bank nigdy nie prosi Klienta o takie dane. Jeśli ktoś żąda od nas takich informacji, to powinien to być dla nas sygnał ostrzegawczy. Nie ujawniamy takich danych, a o zaistniałej sytuacji powiadamiamy bank;

2. Zabezpieczamy telefon, komputer, tablet - wszystkie media poprzez które korzystamy z bankowości elektronicznej, powinny być odpowiednio zabezpieczone. Korzystamy z legalnego oprogramowania, które jest na bieżąco aktualizowane. Wykorzystujemy programy antywirusowe. Pamiętamy, że również smartfon powinien mieć zainstalowany program antywirusowy. Postarajmy się o oprogramowanie antymalware, które chroni nas też przed programami typu ransomware, czyli takimi, które zaszyfrują nasze dane i zażądają okupu za ich odblokowanie. Zwracajmy uwagę, aby aplikacje, które ściągamy na smartfon, tablet pochodziły ze sprawdzonego źródła.

3. Nie otwieramy podejrzanych maili i załączników - nie otwieramy załączników nawet od znanych nam osób, jeśli się ich nie spodziewaliśmy. Nie bójmy się tego sprawdzić i skontaktować z nadawcą wiadomości. Może uchronić nas to przed cyberprzestępcą, który przesyłając nam spreparowany załącznik, chce zainfekować nasz komputer;

4. Staramy się bacznie przyglądać stronie banku - warto się jej dobrze przyjrzeć i zapamiętać jej cechy szczególne, aby ustrzec się sytuacji, że zostaniemy przekierowani na łudząco podobną stronę, ale będącą pod kontrolą przestępcy, a nie banku. Taka fałszywa strona może zawierać np. linki bezpośrednio odsyłające do zarażonych plików, które infekują system.

5. Czego musimy przestrzegać przy logowaniu do bankowości elektronicznej – na stronę bankowości nigdy nie wchodzimy korzystając z przesłanych pocztą elektroniczną linków. Zawsze używamy adresu bezpośredniego. Przy logowaniu zwracamy uwagę na dwa elementy: szyfrowanie połączenia i certyfikat bezpieczeństwa. Symbol kłódki w pasku adresu przeglądarki oraz „https" na początku adresu strony, na której się logujemy to elementy, które muszą być na stronie. Klikając na kłódkę możemy sprawdzić certyfikat, jego ważność. Musi być ważny i wydany dla. Banku Spółdzielczego w Werbkowicach,



czyli https://-a nie http://-świadczy o braku szyfrowania, czyli o tym, że dane są transmitowane przez sieć tekstem jawnym, co naraża nas na ogromne niebezpieczeństwo. Odstępujemy wtedy od

logowania. Podobnie robimy, jeśli certyfikat jest nieważny, nie można go zweryfikować lub nie został wydany dla naszego banku.

6. Sprawdzamy datę ostatniego logowania do bankowości elektronicznej - sprawdźmy, czy rzeczywiście w tym terminie korzystaliśmy z bankowości elektronicznej. Jeśli nie powinniśmy zgłosić taki fakt do banku.

7. Tworzymy silne hasło do konta - musi być ono unikalne, możliwie skomplikowane, ale dające się zapamiętać. Pamiętajmy, aby go nikomu nie udostępniać. Zmieniamy je natychmiast, jeśli tylko uważamy, że ktoś mógł je podejrzeć. Aby ułatwić sobie zapamiętanie długich, skomplikowanych haseł można stosować różne sztuczki. Np. bierzemy jakiś tekst, wierszyk, który znamy na pamięć. Wybieramy sobie pierwszą literę z każdego wyrazu i układamy ciąg znaków. Możemy do- łożyć cyfry, zmieniać litery na duże i małe, wykorzystywać znaki alfanumeryczne. Jeśli korzystamy z tego samego hasła na komputerze stacjonarnym i smartfonie musimy sprawdzić, czy znaki, które wprowadzamy z klawiatury komputera, potrafimy wprowadzić też z telefonu.

8. Weryfikujemy kody wysyłane przez SMS - cyberprzestępcy do potwierdzenia operacji potrzebują kodu wysyłanego przez SMS. Należy pamiętać, aby dokładnie czytać takie SMS, zawsze sprawdzać, czy zgadza się numer rachunku odbiorcy oraz kwota operacji.

9. Nie korzystamy z otwartych sieci WIFI - dostęp do sieci WIFI w galeriach handlowych, dworcach, lotniskach jest przeważnie darmowy, ale korzystanie z tego typu sieci do prowadzenia operacji bankowych jest raczej nieodpowiedzialne. Tego rodzaju sieci są stosowane przez cyberprzestępców jako idealne miejsce do roznoszenia różnego rodzaju oprogramowania, które trudno nazwać przyjaznym. Korzystajmy z sieci WIFI, tylko wtedy, gdy gwarantują one odpowiedni poziom bezpieczeństwa.

10. Rozważnie korzystamy z sieci Internet - korzystając ze sklepów internetowych, serwisów aukcyjnych wybierajmy te, które mają dobre opinie, wysokie oceny w rankingach. Także strony zawierające treści pornograficzne, pirackie oprogramowanie są bardzo niebezpieczne. Często korzystanie z dziwnych, podejrzanych (np. sugerujących jakieś wyjątkowe okazje) linków na stronie może doprowadzić do infekcji malwarem, czy nawet ich specyficznym rodzajem, czyli ransomware. Linki są tak skonstruowane, że bezpośrednio odsyłają do zarażonych plików, które infekują system.

11. Uważnie korzystajmy z przeglądarek - zwracajmy uwagę na popularne wtyczki do przeglądarki. Wystarczy zadbać, żeby były one aktualne.

12. Pilnujemy kart - nie zostawiamy kart bankomatowych, kart kredytowych bez kontroli, zwłaszcza w obecności osób trzecich. Nie robimy kartom zdjęć i nie umieszczamy w Sieci, zwłaszcza numerów CVV2 lub CVC2: ostatnich 3 cyfr numeru umieszczonego na pasku do podpisu na odwrocie karty.

13. Sprawdzamy bankomaty - sprawdzamy bankomat, czy czytnik kart nie wygląda podejrzanie (najczęściej w oryginalnych bankomatach wlot na karty płatnicze jest wklęsły), czy klawiatura bankomatu jest równa lub lekko obniżona w stosunku do poziomu obudowy, czy do bankomatu nie są doklejone jakieś podejrzane urządzenia. Wprowadzając PIN, należy zawsze zasłaniać klawiaturę ręką, portfelem i to tak, aby nie można było PIN-u podejrzeć z żadnej strony (przestępcy montują mini kamery). W miarę możliwości korzystamy z bankomatów zlokalizowanych wewnątrz obiektów usługowo-handlowych, które są obciążone mniejszym ryzykiem modyfikacji do celów przestępczych. Często i systematycznie kontrolujemy stan salda rachunku oraz historię transakcji. Ograniczamy liczbę transakcji po zmroku i w nocy. PIN do bankomatu nie powinien składać się z cyfr odpowiadających dacie urodzenia, czy też innym datom łatwym do odgadnięcia.

14. Włączamy powiadomienia SMS - warte rozważenia jest włączenie usługi (przeważnie płatnej) dodatkowych wiadomości od banku, które informują o zmianach na rachunku, wypłatach, wpłatach. W przypadku niepokojących zdarzeń możemy szybko zareagować.

15. Bezpiecznie dokonujemy przelewów internetowych - co jakiś czas sprawdzamy, czy numery rachunków w przelewach zdefiniowanych wcześniej nie zostały zmienione, podmienione; nie kopiujemy numerów rachunków bankowych do przelewów (kopiuj -wklej), ale wpisujemy je samodzielnie i dokładnie weryfikujemy; przed potwierdzeniem transakcji przelewu weryfikujemy zgodność numeru konta odbiorcy oraz numeru, który jest w kodzie potwierdzającym transakcję. Przelewów dokonujemy tylko z pewnych komputerów.

16. Ustawiamy limity dla transakcji kartami płatniczymi - ustawiając zbyt wysokie limity dla kart debetowych i kredytowych, szczególnie z funkcją zbliżeniową, ułatwiamy złodziejom kradzież środków.

17. Dbamy o swój telefon, smartfon - logujemy się do mobilnych aplikacji bankowych tylko wtedy, gdy z nich korzystamy. Po skorzystaniu, wylogowujemy się. Każdy smartfon z uwagi na oprogramowanie, które można na nim zainstalować, ma ogromne możliwości i można na nim przechowywać bardzo różne, wartościowe dane. Warto pamiętać o aplikacji antywirusowej, ochronie przed malware, ściąganiu aplikacji wyłącznie z zaufanych źródeł. Tylko od nas zależy, czy włączymy szyfrowanie telefonu lub usługę zdalnego wyszukiwania telefonu. Ilość opcji zależy od konkretnego modelu telefonu.

18. W miarę potrzeby kontaktujemy się z bankiem - często zdarza się, że w trakcie korzystania z Internetu i konta bankowego, coś nas zaniepokoi: dziwne wiadomości SMS, e-mail, czy komunikat w systemie bankowym. W takiej sytuacji należy bez wahania skontaktować się z bankiem, bo być może ktoś usiłuje dostać się do naszego rachunku. Takich sytuacji nie wolno bagatelizować.

19. Dbamy o dokumenty z naszymi danymi osobowymi - nasze dane osobowe to skarb, który należy chronić za wszelką cenę. Zwracajmy uwagę, komu powierzamy swoje dane: adres, telefon, czy numer i serię dowodu osobistego. Takie informacje są bardzo cenne dla przestępców, bo dzięki nim mogą założyć konto czy uzyskać kredyt. Każde dane można wykorzystać.

WAŻNE !

Po zakończeniu czynności bankowych wylogowujemy się z aplikacji bankowej. Nie zostawiamy komputera zalogowanego do systemu bankowości elektronicznej bez kontroli.