JAK DBAĆ O BEZPIECZEŃSTWO?

I. BEZPIECZNE URZĄDZENIA

a) Z serwisów transakcyjnych należy korzystać tylko na sprawdzonych urządzeniach. Należy unikać logowania do aplikacji i stron z cudzych komputerów i urządzeń mobilnych
b) Należy korzystać z dodatkowych programów (np. antywirus, firewall), które chronią komputery i urządzenia mobilne
c) Należy regularnie aktualizować system operacyjny na komputerze
d) Nie należy zmieniać ustawień bezpieczeństwa urządzenia, a w szczególności nie należy usuwać ograniczeń, które narzucił producent
e) Aplikacje i programy należy pobierać wyłącznie z oficjalnych źródeł
f) Należy blokować ekran urządzenia za pomocą dodatkowego zabezpieczenia (np. hasło, PIN).

1. Urządzenia mobilne

Smartfony i tablety coraz częściej zastępują inne urządzenia osobiste. Podobnie jak komputery, urządzenia mobilne wymagają odpowiedniej ochrony przed wirusami.
Wielu użytkowników, myśląc o bezpieczeństwie telefonu lub tabletu, obawia się, że go zgubi, lub ktoś go ukradnie. Tymczasem bardziej powinniśmy się obawiać, że ktoś przejmie nad nim kontrolę.
O czym pamiętać, żeby bezpiecznie korzystać z aplikacji na urządzeniu mobilnym:

a) Należy używać oprogramowania antywirusowego
b) Należy blokować ekran hasłem lub PIN-em
c) Należy instalować aktualizacje aplikacji i systemu operacyjnego
d) Należy pobierać i instalować aplikacje wyłącznie z oficjalnych sklepów z aplikacjami
e) Nie należy uruchamiać linków z wiadomości SMS lub e-mail, jeśli istnieje wątpliwość, że pochodzą z niebezpiecznego i niezaufanego źródła
f) Nie należy łączyć aplikacji mobilnej ze swoim kontem na obcych urządzeniach
g) Nie należy odczytywać kodów QR nieznanego pochodzenia
h) Należy ostrożnie podchodzić do instalacji aplikacji, które wymagają uprawnień do odczytywania i wysyłania wiadomości SMS
i) Jeśli nie korzystają Państwo w danej chwili z Wi-Fi lub Bluetooth, należy je wyłączyć.

Uwaga! Żadna instytucja nigdy nie prosi, abyś instalował dodatkowe aplikacje lub certyfikaty.

2. Komputer

Bezpieczny komputer powinien mieć:

a) aktualizowany i legalny system operacyjny
b) oprogramowanie typu firewall
Firewall (zapora sieciowa) to jeden ze sposobów zabezpieczania komputerów, sieci i serwerów przed intruzami. Firewall stał się nieodzownym oprogramowaniem każdego komputera podłączonego do sieci. Zapora na domowym komputerze sprawdza cały ruch w sieci oraz ogranicza dostęp nieznanym programom lub użytkownikom
c) oprogramowanie antywirusowe oraz zabezpieczające przed spyware i adware
To oprogramowanie, które wykrywa, zabezpiecza, zwalcza, usuwa i naprawia szkody, które powodują wirusy. Jeśli aplikacja zawiera szkodliwe oprogramowanie, program antywirusowy wykonuje odpowiedni ruch, który wyklucza wirusa i pozwala na bezpieczny dostęp do uruchamianego programu. Ważne jest, aby każdego antywirusa odpowiednio często aktualizować. Pozwala mu to „być na bieżąco” w świecie wirusów. Dzięki aktualizacji program zbiera informacje o najnowszych wirusach i dostaje instrukcje, które pozwalają mu je zwalczać i naprawiać. Cenione na rynku firmy, które produkują oprogramowanie antywirusowe, codziennie aktualizują definicje wirusów
d) oprogramowanie antyspamowe
To rodzaj oprogramowania, które blokuje niechcianą korespondencję mailową. Programy filtrują wiadomości i wykorzystują tak zwane czarne listy adresów i domen używanych przez spamerów. W większości tego typu oprogramowania możemy

zmieniać ustawienia reguł (np. określać słowa klucze, występujące w materiałach reklamowych). Pozwala to zablokować naszą skrzynkę pocztową na wiadomości, które zawierają te słowa w tytule przesyłki. Jednak programy te nie są bezbłędne i potrafią czasem zablokować korespondencję, która powinna być dostarczona, dlatego warto sprawdzać folder spam i weryfikować, czy wszystkie wiadomości, które do niego trafiły, rzeczywiście powinny się w nim znaleźć.

II. BEZPIECZNE HASŁA

a) Należy stosować skomplikowane hasła i zadbać o to, aby trudno było je odgadnąć (minimum osiem znaków, w tym znaki specjalne, liczby, duże i małe litery)
b) Nie należy używać w haśle trywialnych zwrotów oraz informacji, które łatwo powiązać (np. imię czy nazwisko) lub odgadnąć (np. aktualny miesiąc, rok)
c) Należy regularnie zmieniać hasła i nie udostępniać ich nikomu
d) Należy używać unikalnych haseł do serwisów www. Nie należy wykorzystywać tych samych haseł, które stosuje się w innych systemach, na forach czy portalach.

III. BEZPIECZNE LOGOWANIE DO E-BOK

a) Nigdy nie należy udostępniać osobom trzecim identyfikatora (loginu) ani hasła dostępu. Hasło do logowania w serwisie ustalają Państwo samodzielnie
b) Wpisując identyfikator (login) i hasło należy się upewnić, że nikt ich nie podpatruje
c) Nie należy logować się do aplikacji na komputerach dostępnych w miejscach publicznych
d) Należy stosować bezpieczne hasła i starać się nie używać prostych do odgadnięcia haseł
e) Nie należy zapisywać nigdzie haseł i pamiętać o ich regularnej zmianie
f) Przed odejściem od komputeranależy się wylogować i zamknąć przeglądarkę
g) Należy sprawdzać datę ostatniego poprawnego oraz niepoprawnego logowania
h) Jeśli na stronie logowania pojawią się dodatkowe pola, które należy uzupełnić np. wpisać dane osobowe lub hasło jednorazowe, lub zauważą Państwo jakiekolwiek nieprawidłowości, nie należy podawać danych i natychmiast zgłosić problem do Biura Obsługi Klienta.

IV. BEZPIECZNA INSTALACJA APLIKACJI

Jeśli zdecydują się Państwo pobrać jakiekolwiek oprogramowanie na swoje urządzenie, należy pamiętać:

a) aplikacje powinny być pobierane z autoryzowanych sklepów. autoryzowane sklepy to: App Store (iOS – Apple), Google Play (Android), Windows Phone Store (Windows Phone) oraz Windows Store (Windows 8.1) – należy korzystać tylko z tych sklepów, ponieważ znajdujące się tam programy są cyfrowo podpisane i są sprawdzane pod kątem bezpieczeństwa
b) nigdy nie należy pobierać aplikacji z niezaufanych źródeł oraz należy unikać pobierania aplikacji od osób trzecich (np. przesyłanych przez Bluetooth lub w SMSie)
c) należy ostrożnie podchodzić do instalowania aplikacji, które żądają od Państwa nadania uprawnień do odczytywania lub wysyłania wiadomości SMS.

V. BEZPIECZNE MAILE

a) Nie należy otwierać podejrzanych maili i załączników
b) Należy zwracać szczególną uwagę na załączniki posiadające kilka rozszerzeń plików jednocześnie, np. przelew.pdf.zip, wyplata.jar.doc
c) Należy sprawdzać, czy rzeczywisty adres odnośnika (link) jest spójny z tym, który widzą Państwo w treści maila

d) Należy zwrócić uwagę na wiarygodność nadawcy oraz sposób w jaki zwraca się do Państwa
e) Nigdy nie należy logować się do serwisu transakcyjnego z linka, który otrzymali Państwo w mailu
f) Nie należy realizować transakcji na podstawie maila. Należy sprawdzić dokładnie tego typu dyspozycje.

VI. BEZPIECZNE STRONY WWW

a) Należy sprawdzić poprawność witryny serwisu www, z którym się Państwo łączą (certyfikat oraz połączenie HTTPS)
b) Nie należy wchodzić na podejrzane i nieznane witryny - należy zwracać uwagę na adresy URL stron, które Państwo odwiedzają, zwłaszcza na tzw. skrócone adresy URL. Takie strony mogą zainfekować Państwa urządzenie złośliwym oprogramowaniem
c) Nie należy podawać danych osobowych na niezaufanych witrynach, w szczególności loginu i hasła na stronach obcych serwisów
d) Logując się do serwisów, należy wpisywać stronę logowania samodzielnie lub używać przycisku „Zaloguj” po ręcznym wpisaniu adresu strony. Nigdy:
   - nie wolno korzystać z linków do logowania, które otrzymują Państwo mailem czy w portalach społecznościowych
   - nie powinno się szukać strony do logowania w wyszukiwarce internetowej – można trafić na fałszywe strony, które udają stronę, na którą chcą się Państwo zalogować.

VII. BEZPIECZNE PROFILE I OFERTY

a) Jeżeli dostali Państwo prośbę od znajomego, aby zrobić mu przelew uważaj – możliwe, że piszesz z oszustem. Należy skontaktować się ze znajomym w inny sposób i potwierdzić, że faktycznie to on prosi Państwa o przelew
b) Przed zakupem należy sprawdzić, od kogo kupuje się towar: jak długo istnieje dana firma, gdzie ma siedzibę, czy można się do niej dodzwonić oraz jakie opinie wystawili inni kupujący
c) Nie należy ufać ofertom pracy, które przychodzą bezpośrednio na Państwa skrzynkę pocztową, szczególnie tym wyjątkowo atrakcyjnym. Gdy szukają Państwo pracy, należy korzystać wyłącznie ze znanych portali.

VIII. BEZPIECZNE ROZMOWY TELEFONICZNE

a) Nie należy ujawniać prywatnych danych, dopóki nie ma się pewności się, z kim się rozmawia. Pracownika instytucji zawsze można sprawdzić oddzwaniając do Biura Obsługi Klienta i potwierdzając jego tożsamość
b) Nie należy ufać nieznanemu rozmówcy, który chce, aby podać mu poufne dane (hasła, PIN-y).