Dobre praktyki w zakresie bezpieczeństwa teleinformatycznego

AKTUALIZACJE SYSTEMÓW I BEZPIECZEŃSTWO SPRZĘTU

- Korzystaj z aktualnego oprogramowania: Regularnie **aktualizuj system operacyjny, program antywirusowy**, przeglądarkę internetową. Dzięki aktualizacjom łatwiej ustrzeżesz się przed szkodliwym oprogramowaniem i innymi zagrożeniami obecnymi w sieci.
- Włącz aktualizacje automatyczne: Wiele aplikacji oferuje możliwość automatycznego pobierania aktualizacji, w celu ochrony przed nowymi zagrożeniami. Skorzystaj z tego rozwiązania wszędzie tam, gdzie to możliwe.
- Chroń urządzenia podłączane do sieci: Nie tylko komputery, ale także smartfony, tablety i inne podłączane do Internetu urządzenia, potrzebują ochrony przed wirusami i złośliwym oprogramowaniem.
- Skanuj przed użyciem: Nie podłączaj do komputera nośników, których pochodzenie nie jest Ci znane. Dyski zewnętrzne, pendrive'y, czy inne nośniki danych mogą być niebezpieczne (zainfekowane przez szkodliwe oprogramowanie). Zanim otworzysz ich zawartość skorzystaj ze skanera antywirusowego.

ZABEZPIECZ DOSTĘP

- Dwuskładnikowe uwierzytelnianie: Zadbaj o swoje konta w sieci. Logowanie oparte wyłącznie o nazwę użytkownika i hasło nie jest wystarczająco bezpieczne (szczególnie w przypadku konta e-mail, portalu społecznościowego czy bankowości internetowej). Aktywuj weryfikację tożsamości opartą o dodatkowy składnik, np. kod SMS, token, czy klucz sprzętowy.
- Stwórz mocne hasło: Dobre hasło składa się przynajmniej z 12 znaków. Skup się na pozytywnych zdaniach lub zwrotach, o których lubisz myśleć i które łatwo zapamiętasz (np. „Lubię chodzić do kina"). Na wielu stronach internetowych, możesz przy wprowadzaniu hasła używać spacji.
- Jedno hasło, jedno konto: Jeżeli chcesz utrudnić działania przestępcom, dla każdego konta przypisz oddzielne hasło. Niezbędne minimum, to rozdzielenie kont używanych do pracy i celów prywatnych. Zadbaj o silne hasło do najistotniejszych serwisów (bankowość, poczta elektroniczna, portale społecznościowe)
- Przechowuj bezpiecznie: Każdy może zapomnieć swojego hasła. W celu ułatwienia nam życia stworzono aplikacje zwane menadżerami haseł. Służą do bezpiecznego przechowywania danych dostępowych. Możesz z nich korzystać. Jeżeli zapisałeś hasło na kartce (lepiej tego nie rób), postaraj się umieścić ją w bezpiecznym miejscu, z dala od komputera.

ROZWAGA I ŚWIADOME UŻYTKOWANIE

- Zatrzymaj się, jeśli masz wątpliwości: Linki i załączniki w wiadomościach e-mail, spreparowane posty w mediach społecznościowych oraz reklamy - to częste metody używane przez przestępców w celu kradzieży danych. Jeżeli wydają Ci się podejrzane, po prostu je zignoruj. Nawet, jeżeli źródło wygląda na zaufane.
- Uważaj na hotspoty Wi-Fi: Ogranicz aktywność w publicznie dostępnych sieciach Wi-Fi. Używając poza domem kluczowych serwisów (poczta e-mail, bankowość internetowa, portale społecznościowe) bezpieczniej będzie użyć własnego modemu LTE lub połączenia VPN. Pamiętaj o wyłączaniu transmisji Wi-Fi i Bluetooth, kiedy z niej nie korzystasz.
- Chroń swoje finanse: Korzystając z bankowości internetowej i sklepów online, upewnij się, że połączenie jest objęte szyfrowaniem (zielona kłódka oraz prefiks „https://" w pasku adresu). Odczytując kod SMS uwierzytelniający transakcję, zweryfikuj kwotę przelewu i numer rachunku odbiorcy!
- Nie lekceważ informacji ze świata bezpieczeństwa IT - Jeśli coś podawane jest do publicznej wiadomości, najczęściej dotyczy także Ciebie.

- Pomyśl, zanim zadziałasz: Bądź ostrożny wobec korespondencji zachęcającej do natychmiastowych działań. Szczególnie, jeśli ktoś oferuje Ci łatwy zysk lub próbuje nakłonić do podania prywatnych danych. Robiąc zakupy w sieci, weryfikuj reputacje sklepów. Dziel się wiedzą z rodziną i znajomymi.
- Zadbaj o kopie zapasowe: Zabezpiecz efekty swojej pracy, muzykę, zdjęcia, cenne dokumenty. Twórz kopie zapasowe i przechowuj je w bezpiecznym miejscu.

OCHRONA PRYWATNOŚCI

- **Informacje mają wartość:** Dane na Twój temat, takie jak historia zakupów czy historia lokalizacji są cenne. Zwracaj uwagę kto i co (aplikacje, strony internetowe) próbuje uzyskać do nich dostęp.
- **Dostosuj ustawienia prywatności w serwisach online i na urządzeniach:** Dzięki nim, możesz lepiej chronić Twoje dane. Sam decyduj, jak wiele informacji na swój temat chcesz udostępnić innym.
- **Pomyśl, zanim udostępnisz:** Zwracaj uwagę na przesyłaną do sieci treść, zasięg komunikatu, a także sposób, w jaki może zostać odebrany.

PRACA ZDALNA

- **Korzystaj tylko z zaufanego połączenia z siecią:** Jeśli wraz z laptopem zapewniono Ci także dodatkowe urządzenie umożliwiające połączenie z internetem lub wyposażyła Twój komputer w kartę SIM, to do pracy korzystaj wyłącznie z takiego dostępu do sieci. Szczególnie w sytuacji, gdy Twoja sieć domowa jest współdzielona z innymi użytkownikami (np. z bloku lub osiedla). Nie łącz się z innymi otwartymi sieciami bezprzewodowymi, choćby ich zasięg w Twoim mieszkaniu był wyśmienity. Jeśli z jakiegoś powodu służbowy dostęp do internetu zawiedzie, to najbezpieczniej zastąpić go siecią udostępnioną z telefonu (tzw. hotspot).
- **Podczas pracy nie wychodź z tunelu VPN**: tunel VPN nie tylko szyfruje Twoje połączenie z siecią bankową, ale może zapewniać Ci także dodatkową ochronę przed zagrożeniami pochodzącymi z sieci, np. przed stronami internetowymi zaatakowanymi przez malware. Dlatego w czasie pracy zdalnej nie wyłączaj VPN, nawet jeśli zechcesz sprawdzić coś niezwiązanego z Twoimi obowiązkami.
- **Daj o bezpieczeństwo danych podczas ich przesyłania:** Pamiętaj o tym, aby nigdy nie wysyłać wrażliwych danych bez szyfrowania. Jeśli przekazujesz komuś cenne dane jako załącznik do wiadomości email, to dodatkowo zabezpiecz taki plik hasłem. Jeśli program, którego używasz nie ma takiej funkcjonalności, to zawsze możesz spakować plik np. programem „ZIP" z użyciem hasła i dopiero w takiej postaci dołączyć go do wiadomości. Hasło do pliku przekaż odbiorcy najlepiej w inny sposób, np. za pomocą SMS. I co najważniejsze – przed wysłaniem pliku upewnij się, czy adres odbiorcy jest poprawny!

ETYKA, DOBRE PRAKTYKI

- **Twoje zachowanie w sieci ma znaczenie:** Stosowanie dobrych praktyk buduje kulturę bezpiecznej sieci. To, co robisz, ma znaczenie (w domu, w pracy, gdziekolwiek jesteś).
- **Traktuj innych tak, jak sam chciałbyś być traktowany.**
- **Wspieraj walkę z cyberprzestępczością:** Jeżeli zaobserwujesz niepokojące zjawiska, nie wahaj się o tym poinformować.

P A M I Ę T A J:

- **Nigdy nie odpowiadaj na e-maile zachęcające do ujawnienia danych i haseł!!!**
- **Bank nigdy nie wykorzystuje usługi pulpitu zdalnego jako narzędzia wsparcia i pomocy Klientom Banku korzystającym z bankowości internetowej.**
- **Nigdy nie wyrzucaj hasła pierwotnego, które otrzymałeś z Banku, gdyż na jego podstawie będziesz mógł się odblokować, składając dyspozycję w Banku/ poprzez kontakt z pracownikami zespołu księgowego w Centrali Banku, pod numerem: 68 3564104.**

BEZPIECZNY KOMPUTER

- Regularnie aktualizuj system operacyjny i wszystkie zainstalowane programy.
- Zainstaluj renomowany program antywirusowy i regularnie go aktualizuj.
- Zabezpiecz swoją sieć internetową i zainstaluj program typu Firewall, który będzie zezwalał na dostęp do internetu tylko zaufanym usługom i aplikacjom.
- Regularnie sporządzaj kopie zapasowe swoich danych zapisanych na komputerze i przechowuj je w bezpiecznym miejscu, np. na dodatkowym zewnętrznym dysku.
- Konta administracyjnego używaj tylko do konfiguracji systemu – na co dzień pracuj na koncie bez uprawnień administracyjnych.
- Nie udostępniaj komputera osobom trzecim. Jeśli jednak zajdzie taka konieczność – utwórz dodatkowe konto dla tej osoby na czas wykonywania przez nią potrzebnej czynności.
- Dbaj o fizyczne bezpieczeństwo swojego laptopa - chroń go przed uszkodzeniami mechanicznymi, używaj zabezpieczeń przed kradzieżą, a także nie pozostawiaj bez nadzoru.
- Szyfruj ważne dane, czyli takie, które powinny być znane tylko Tobie lub których ujawnienie może narazić Cię np. na straty finansowe lub kradzież tożsamości.
- Włącz opcję wyświetlania rozszerzeń nazw typów plików w systemie i zwracaj uwagę, czy rozszerzenia odpowiadają typom plików, np. czy dokument Word ma rozszerzenie .doc, a plik Excel .xls .
- Dokładnie czytaj komunikaty, które wyświetla komputer – nie zezwalaj na włączenie funkcji obniżających bezpieczeństwo (np. makro w pakiecie Office).
- W przypadku wykrycia wirusa lub innego złośliwego oprogramowania – usuń go tak szybko, jak to jest możliwe, a w przypadku problemów z usunięciem – zainstaluj ponownie system operacyjny, dane odtwórz z kopii zapasowej i koniecznie zmień hasła do usług internetowych (bankowość elektroniczna, poczta, serwisy społecznościowe itp.).
- W sytuacji, gdy przypadkiem autoryzowałeś transakcję, która Twoim zdaniem jest podejrzana, w trybie pilnym powiadom infolinię swojego Banku.
- Nie odchodź od komputera będąc zalogowany do systemu!
- Wyloguj się i zamknij przeglądarkę po zakończeniu pracy.
- Nie korzystaj z nieznanych sieci bezprzewodowych oraz usług bankowości internetowej na ogólnie dostępnych komputerach np. kawiarenki internetowe/
- Nie wchodź na stronę internetową Banku za pośrednictwem linków znajdujących się w przychodzacych mailach.
- Zweryfikuj certyfikat strony (np. klikając na kłódkę).

CZUJNOŚĆ W INTERNECIE

- Nie otwieraj załączników poczty elektronicznej od nieznanych Ci osób lub firm i nie klikaj w zawarte w załącznikach lub e-mailach odsyłacze do stron internetowych.
- Jeżeli nadawca wiadomości pocztowej jest Ci znany, ale treść e-maila nie koresponduje z tą osobą lub nie oczekiwałeś listu od tej osoby - nie otwieraj załącznika. Skontaktuj się telefonicznie z nadawcą wiadomości i wyjaśnij sprawę.
- Nie daj się nabrać, że w internecie ktoś da Ci coś za darmo lub za drobną przysługę. Może to być próba kradzieży Twojej tożsamości lub posłużenia się Twoimi danymi do popełnienia przestępstwa – np. próba wykorzystania Twojego rachunku bankowego w procederze prania pieniędzy.
- Zastanów się, dlaczego ktoś w e-mailu skłania Cię do szybkiego niestandardowego działania - czy przypadkiem nie jest to atak socjotechniczny.
- Zastanów się, zanim podasz swój adres e-mail lub numer telefonu komórkowego w formularzu nieznanej Ci witryny internetowej. Nie działaj pod wpływem impulsu.
- Jeśli link, w który kliknąłeś, przenosi Cię na stronę logowania do usługi - upewnij się, że jesteś na właściwej stronie logowania, a nie zostałeś przekierowany na przestępczą stronę, która chce wyłudzić Twoje dane osobowe. Jeżeli masz jakiekolwiek wątpliwości, zamknij tę stronę.
- Zawsze zwracaj uwagę na komunikaty o błędach certyfikatów wyświetlane przez przeglądarkę - zrezygnuj z autoryzacji transakcji, gdy masz jakiekolwiek podejrzenia. W razie konieczności skontaktuj się z Bankiem.
- Nie instaluj programów pochodzących z niezaufanych źródeł. Pamiętaj, że Bank nie wysyła SMS-ów lub innych wiadomości z odsyłaczem do zainstalowania „certyfikatów bezpieczeństwa”.

- Nie korzystaj z nieznanych lub publicznych sieci (np. hotspot, Wi-Fi).
- Nie podawaj ważnych danych (np. login i hasło), gdy korzystasz z obcej sieci lub niezaufanego komputera.
- Przestępcy mogą próbować wykorzystywać usługi pulpitu zdalnego w ramach ataków przepropwadzanych w celu wyłudzenia Twoich środków metodami socjotechniki. Bank Spółdzielczy w Nowej Soli nigdy nie wykorzystuje usługi pulpitu zdalnego jako narzędzia do wsparcia i pomocy Klientom Banku korzystającym z bankowości internetowej.

HASŁO

- Używaj haseł trudnych do odgadnięcia.
- Nie używaj haseł słownikowych, tzn. haseł zbudowanych z wyrazów, które są potocznie używane, lub takich jak imię dziecka czy data urodzenia.
- Hasło powinno się składać z co najmniej 8 znaków i zawierać cyfry, małe i wielkie litery oraz znaki specjalne. Przykład dobrego hasła: Aoi30l.WlbsnaA. Jest to skrót zdania: *Andrzej obchodzi imieniny 30 listopada. Wtedy ludzie bawią się na Andrzejkach*. – jego pierwsze litery, cyfry i znaki:
- Stosuj różne hasła do różnych usług – nie powielaj w bankowości internetowej hasła, którego używasz np. do poczty elektronicznej.
- Regularnie zmieniaj hasła. Koniecznie zmień hasło, gdy masz podejrzenie, że obecne mogło zostać ujawnione osobom niepowołanym.
- Zapamiętaj hasło. Nie ujawniaj hasła. Nie przechowuj hasła razem z loginem.

BEZPIECZNY SMARTFON

- Jeżeli kupiłeś używany telefon – przed instalacją karty SIM usuń dane z urządzenia i przywróć ustawienia fabryczne
- Jeżeli masz zamiar sprzedać swój telefon – usuń dane, zaszyfruj telefon i przywróć ustawienia fabryczne.
- Nie udostępniaj urządzenia mobilnego swoim dzieciom lub osobom trzecim. Jeśli jednak zajdzie taka konieczność, utwórz dodatkowe konto dla tej osoby, o ile jest taka możliwość.
- Ustaw kod PIN lub symbol odblokowujący telefon.
- Zainstaluj renomowany program antywirusowy i regularnie go aktualizuj.
- Systematycznie sporządzaj kopie zapasowe danych i przechowuj je w bezpiecznym miejscu.
- Kontroluj na bieżąco koszty lub liczbę połączeń i wiadomości SMS oraz wielkość transmisji danych – zwiększone koszty lub ilość przesyłanych danych może sugerować działanie niechcianych, groźnych aplikacji na urządzeniu. Nie otwieraj załączników, które otrzymałeś w wiadomościach od nieznanych osób lub firm, i nie klikaj w odsyłacze do stron internetowych
- Nie instaluj aplikacji pochodzących z niezaufanych źródeł.
- Sprawdź, o jaki dostęp do Twoich danych na smartfonie prosi instalowana aplikacja - np. aplikacja „LUSTERKO" nie powinna potrzebować dostępu do SMS-ów, książki adresowej, aparatu fotograficznego czy internetu.
- Sprawdź i ewentualnie zablokuj dostęp do funkcjonalności telefonu aplikacjom, które ich nie wymagają do prawidłowego działania
- Nie podawaj ważnych danych (np. login i hasło), gdy korzystasz z obcej sieci lub cudzego telefonu
- Jeżeli otrzymałeś wiadomość SMS od Banku z kodem autoryzacyjnym do potwierdzenia zleconego przelewu, dokładnie sprawdź treść wiadomości - czy zawiera właściwy numer rachunku odbiorcy i kwotę przelewu

---