

Zadbaj o bezpieczeństwo swoje i swoich pieniędzy w Internecie

Korzystając z Internetu zawsze przestrzegaj zasad bezpieczeństwa. Oszuści próbują wykorzystać Twoje roztargnienie i nieostrożność. Nie daj się zaskoczyć!

Bądź czujny 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 e-maila od tej osoby - nie otwieraj załącznika. Skontaktuj się z nadawcą wiadomości telefonicznie i wyjaśnij sprawę.
- Nie daj się nabrać, że w Internecie ktoś da Ci coś za darmo lub za drobną przysługę. Może to być próba wykradzenia Twojej tożsamości lub posłużenia się Twoimi danymi do popełnienia przestępstwa – na przykład 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 nieznaney 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 jakiegokolwiek wątpliwości, to zamknij tę stronę.
- Zawsze zwracaj uwagę na komunikaty o błędach certyfikatów wyświetlane przez przeglądarkę - zrezygnuj z autoryzacji transakcji, gdy masz jakiegokolwiek podejrzenia. W razie konieczności, skontaktuj się z Bankiem.
- Nie instaluj programów pochodzących z niezauważanych 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 niezauważanego komputera.

Bezpieczny komputer

- Regularnie aktualizuj system operacyjny i wszystkie zainstalowane programy.
- Zainstaluj renomowany program antywirusowy i regularnie aktualizuj go.
- Zabezpiecz swoją sieć internetową i zainstaluj program typu firewall, który będzie zezwalał na dostęp do/z 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 na komputerze 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 potrzebnej czynności.

- Nie korzystaj z usług „wsparcia” poprzez aplikacje wykorzystujące usługę pulpitu zdalnego. Tego typu narzędzia mogą być wykorzystywane w ramach ataków przeprowadzanych w celu wyłudzenia środków pieniężnych metodami socjotechniki.
- 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 świadomie na włączenie funkcji obniżających bezpieczeństwo (np. makro w pakiecie Office).
- W przypadku wykrycia wirusa lub innego złośliwego oprogramowania usuń go tak szybko jak jest to 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.).

Uwaga! Hasło

- Używaj haseł trudnych do odgadnięcia.
- Nie używaj haseł słownikowych, tzn. haseł zbudowanych z wyrazów, które są potocznie używane lub takich jak imię dziecka, data urodzenia.
- Hasło powinno składać się z co najmniej 8 znaków i zawierać cyfry, małe i wielkie litery oraz znaki specjalne.
- Przykład dobrego hasła: ISwz31g.TpNR Jest to skrót zdania: „Imieniny Sylwestra wypadają zimą 31 grudnia. Tuż przed Nowym Rokiem”.
- Stosuj różne hasła do różnych usług – nie powielaj w bankowości internetowej hasła, którego używasz na przykład do poczty elektronicznej.
- Regularnie zmieniaj hasła.
- Koniecznie zmień hasło, gdy masz podejrzenie, że obecne mogło zostać ujawnione osobom niepowołanym.

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 aktualizuj go.
- Regularnie 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 nieznanymi osób lub firm, i nie klikaj w odsyłacze do stron internetowych.
- Jeżeli nadawca wiadomości jest Ci znany, ale jej treść nie koresponduje z tą osobą, to nie otwieraj załącznika - skontaktuj się z nadawcą i wyjaśnij sprawę.
- Nie instaluj aplikacji pochodzących z niezauważanych źródeł.
- Sprawdź o jaki dostęp do Twoich danych na smartfonie prosi instalowana aplikacja - np. aplikacja „Latarka” nie powinna potrzebować dostępu do SMS-ów, książki adresowej, aparatu fotograficznego, czy sieci Internet.
- 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.

PAMIĘTAJ! Bank Spółdzielczy w Rykach nie świadczy usługi „wsparcia” klientom bankowości internetowej poprzez aplikacje wykorzystujące usługę pulpitu zdalnego.

PAMIĘTAJ! Jeśli ktoś dzwoni do Ciebie podając się za pracownika banku, jeśli otrzymujesz wiadomości, których nadawcy podszywają się pod bank lub po prostu coś Cię zaniepokoiło w związku z przelewami lub stanem Twoich środków pieniężnych, zadzwoń na naszą Infolinię.

PAMIĘTAJ! W przypadku czasowej niedostępności Twojej bankowości elektronicznej zachowaj spokój i nie ulegaj panice. Taki jest właśnie cel cyberprzestępców – wywołanie paniki, strachu i chaosu. Nie wspieraj ich w tym. Nie kieruj się również anonimowymi opiniami czy komentarzami np. z mediów społecznościowych czy forów internetowych. Upewnij się, że to wiarygodne informacje a nie „fake newsy”.