INFORMACJA O ZAGROŻENIACH ZWIĄZANYCH Z KORZYSTANIEM Z USŁUGI BANKOWOŚCI ELEKTRONICZNEJ

Użytkownicy sieci Internet korzystający z usług bankowości internetowej narażeni są na:

1. Kradzież haseł, co może skutkować całkowitą lub częściową utratą środków zgromadzonych na rachunkach bankowych, a nawet doprowadzić do zaciągnięcia przez przestępców zobowiązań finansowych na koszt niczego nieświadomych użytkowników.
   W celu zmniejszenia prawdopodobieństwa wystąpienia wyżej wskazanych zjawisk zalecamy:
   - **częste zmiany haseł dostępu**
   - **tworzenie haseł długich (co najmniej z ośmiu znaków), zawierających duże i małe litery, cyfry oraz znaki specjalne takie jak ';<>{}/, których przestępca nie będzie mógł się domyślić oraz nie zapisywanie ich, aby nie zostały wykradzione.**
   - **dostęp do hasła powinna mieć wyłącznie osoba, której dane hasło dotyczy.**

2. Instalowanie przez przestępców na komputerach użytkowników sieci internetowej oprogramowania, które może niszczyć zgromadzone dane, jak również wykradać poufne informacje, co prowadzić może nie tylko do strat finansowych, ale dodatkowo służyć przestępcom jako podstawa szantażu.

Z uwagi na fakt, iż najczęstszym sposobem rozprowadzania nielegalnego oprogramowania jest poczta e-mail, zalecamy:

- **nie otwierać wiadomości od nieznanych nadawców oraz zawierających wzbudzające podejrzenia załączników,**
- **zabezpieczyć swój komputer aktualnym oprogramowaniem antywirusowym oraz zaporą (firewall),**
- **regularnie aktualizować system operacyjny, wersje przeglądarki oraz oprogramowanie na komputerze, przy użyciu którego korzystasz z bankowości elektronicznej, używać oprogramowania z legalnego źródła. Oprogramowanie ściągane z Internetu może być zmodyfikowane przez hakerów. Twórcy legalnych systemów tworzą aktualizacje usuwające na bieżąco luki w zabezpieczeniach,**
- **nie korzystać z pośrednictwa linków, znajdujących się w e-mailach w celu zalogowania się na stronę internetową banku.**

Ponadto w celu zwiększenia bezpieczeństwa prosimy aby:

- Zawsze sprawdzać numer rachunku odbiorcy, gdy kopiujemy dane do przelewu. Złośliwe oprogramowanie może spowodować, że wkleimy numer rachunku przestępcy. Najlepiej, aby numer rachunku bankowego był wprowadzany ręcznie.
- Ustalić bezpieczne limity transakcyjne dla przelewów internetowych.
- Swoje konto internetowe najlepiej obsługiwać w domu i na własnym sprzęcie komputerowym.
- Przy korzystaniu z bankowości internetowej unikać miejsc z komputerami i niezabezpieczonymi sieciami Wi-Fi, do których dostęp ma wiele osób (np. kawiarenki internetowe, kina, restauracje, punkty publicznego dostępu tzw. hot-spoty).
- Logując się na naszą stronę bankowości internetowej (**https://ekonto.nbsdzialoszyn.pl/**) weryfikować poprawność adresu oraz sprawdzać czy połączenie jest szyfrowane (świadczy o tym adres witryny rozpoczynający się od „https://" oraz symbol zamkniętej kłódki).
- Zawsze zwracać uwagę na komunikaty o błędach certyfikatów wyświetlanych przez przeglądarkę.
- W przypadku jakiegokolwiek podejrzenia lepiej zrezygnować z autoryzacji transakcji.
- **Zawsze wylogować się** z Internet Bankingu czy serwisu na stronie internetowej banku.
- By być na czasie! Poszerzaj regularnie swoje horyzonty śledząc nasze komunikaty oraz doniesienia dotyczące najnowszych zabezpieczeń oraz narzędzi, dzięki którym możesz się chronić przed atakiem złośliwych oprogramowań.

……
Data i podpis Posiadacza/Użytkownika