Uwaga, mieszkańcy Powiatu Kaliskiego! Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa ostrzega przed nasilonymi atakami socjotechnicznymi!

Uwaga, mieszkańcy Powiatu Kaliskiego! Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa ostrzega przed nasilonymi atakami socjotechnicznymi wymierzonymi w obywateli i przedsiębiorców. W okresie rozliczeń podatkowych i wdrożenia Krajowego Systemu e-Faktur grupy cyberprzestępcze podszywają się pod Ministerstwo Finansów i Krajową Administrację Skarbową.

Dalsza część treści komunikatu:

Obserwowana jest kampania phishingowa, w której oszuści podszywają się pod KAS, informując o rzekomej nowej notyfikacji. W wiadomości znajduje się link, który prowadzi do strony zawierającej fałszywy formularz logowania do Profilu Zaufanego. Cyberprzestępcy próbują w ten sposób wyłudzić dane logowania do serwisu.

Zalecamy zachowanie szczególnej ostrożności w internecie, zwłaszcza w przypadku odbierania niepokojących i niestandardowych wiadomości e-mail, SMS czy komunikatów w komunikatorach.

Zanim podasz jakiekolwiek dane:

- sprawdź adres nadawcy wiadomości,
- samodzielnie wyszukaj prawdziwy adres strony internetowej tego podmiotu i zweryfikuj czy link z wiadomości na pewno prowadzi właśnie tam,
- jeśli masz jakiekolwiek wątpliwości skontaktuj się z instytucją, która rzekomo wysłała wiadomość.

W przypadku otrzymania tego rodzaju podejrzanej wiadomości, szczególnie jeśli kliknęliśmy w link i podaliśmy dane, należy zgłosić incydent do zespołu reagowania na incydenty bezpieczeństwa komputerowego CSIRT NASK, który jest właściwy w przypadku osób fizycznych. Incydent można zgłosić poprzez formularz na stronie oraz w usłudze „Bezpiecznie w sieci” w aplikacji mObywatel. Podejrzane wiadomości SMS z linkami można również przesłać na bezpłatny numer 8080.

W przypadku podejrzenia, że padło się ofiarą przestępstwa należy to zgłosić na Policji lub w Prokuraturze.

Przypominamy o stosowaniu podstawowych zasad cyberbezpieczeństwa, które pomogą ochronić nas przed kradzieżą danych osobowych i środków finansowych. Obejmują one m.in.:

- zastrzeżenie numeru PESEL w mObywatelu,

- regularne sprawdzanie wycieków na portalu BezpieczneDane.gov.pl,
- stosowanie dwuskładnikowego uwierzytelniania oraz zasad dotyczących bezpiecznych haseł,
- regularne aktualizowanie oprogramowania,
- instalowanie aplikacji na komputerze i urządzeniach mobilnych tylko ze sprawdzonych źródeł,
- ustawienie możliwie niskich limitów płatności dla kart płatniczych, szybkich przelewów (np. BLIK) oraz przelewów przez internet,

szyfrowanie plików przy przesyłaniu naszych danych osobowych,

- korzystanie z mediów społecznościowych z troską o naszą prywatność (pomogą w tym odpowiednie ustawienia – np. ograniczenie widoczności profilu),
- stosowanie innych podstawowych zasad higieny cyfrowej (zachęcamy do korzystania z Bazy wiedzy na stronie Ministerstwa Cyfryzacji oraz Bazy wiedzy prowadzonej przez CERT Polska).

Bądźmy czujni i dbajmy o bezpieczeństwo swoich danych!