

UWAGA UŻYTKOWNICY APLIKACJI E-KARTOTEKA !!!!!

Informujemy, że pozyskaliśmy z firmy MIESZCZANIN informacje wskazujące na to, że z urządzenia końcowego **jednego z mieszkańców naszej Spółdzielni** zostały wykradzione dane dostępowe do logowania do usług, w tym do usługi e-Kartoteka.

Dotyczy to konta JEDNEGO użytkownika e-kartoteki.

Zapewniono Spółdzielnię, że na podstawie ujawnionych danych dostępowych nie nastąpiło dotychczas żadne podejrzanе logowanie do systemu e-kartoteka.

Firma dostarczająca oprogramowanie pismem z dnia 29.01.2026 r. poinformowała Spółdzielnię, że ujawniono iż w nielegalnych bazach danych znajdują się między innymi dane do logowania do usługi e-kartoteka jednego użytkownika wraz z innymi danymi tego użytkownika. Użytkownik ten został przez Spółdzielnię poinformowany o tym fakcie. Sytuacja ta jest całkowicie niezależna od stale monitorowanych środków bezpieczeństwa, jakie firma Mieszczanin nakłada na usługi i oprogramowanie – dane zostały wykradzione nie z usług firmy Mieszczanin, ale wprost z urządzeń, na których usługi są instalowane, czy to przez przechwytywanie wprowadzanych treści przy pomocy oprogramowania szpiegującego, czy też przez fałszywe strony imitujące strony usług. W/W firma podkreśla, że nie jest w stanie w żaden sposób wpłynąć na zaistniałą sytuację, ani zabezpieczyć przed nią w przyszłości, bo zabezpieczenie dotyczy urządzenia ogółem (**czym zarządza właściciel urządzenia końcowego**), na co żaden z dostawców poszczególnych aplikacji nie ma wpływu.

Górnicza Spółdzielnia Budownictwa Mieszkaniowego im. St. Staszica również nie ma wpływu na sposób zabezpieczenia kont poszczególnych użytkowników systemu E-Kartoteka. Każdy użytkownik we własnym zakresie powinien zadbać o bezpieczeństwo swoich danych znajdujących się na jego urządzeniu.

Z uwagi na to, że możliwe jest, iż poza danymi do logowania do systemu e - kartoteka wykradzono dostępy także do innych serwisów i usług (np. do adresu e. mail) , **zalecamy aby podjąć czynności mające na celu :**

- przeskanowanie Państwa urządzeń oprogramowaniem antywirusowym w szczególności pod kątem złośliwego oprogramowania (**przed zmianą haseł**)
- zmianę haseł do logowania w usłudze e-kartoteka (w szczególności w odniesieniu do użytkowników, którzy nie nadali hasła indywidualnego),
- zmianę haseł w innych usługach celem profilaktycznego podniesienia bezpieczeństwa.

Jako stałe działania profilaktyczne zwiększające bezpieczeństwo sugerujemy ponadto:

- cykliczne skanowanie urządzeń oprogramowaniem antywirusowym
- stałą weryfikację, czy strony usług, do których się Państwo logują, nie są fałszywymi stronami do przechwytywania danych,
- korzystanie tylko z certyfikowanych aplikacji pobieranych bezpośrednio z Google Play czy AppStore.