Magiczny Kraków

Nadchodzi „Cyfrowa Tarcza Seniora”

2026-09-22

Drodzy Seniorzy. Dzisiaj rozpoczynamy cykl artykułów: „Cyfrowa Tarcza Seniora”. Prostym i zrozumiałym językiem będziemy wyjaśniać, jak bezpiecznie korzystać z telefonu, komputera i internetu, rozpoznawać próby oszustwa oraz chronić swoje dane i pieniądze. Bez straszenia i trudnych pojęć. Za to z konkretnymi przykładami i praktycznymi wskazówkami. Dzisiaj prezentujemy pierwszy artykuł wspomnianego cyklu.

Fot. Canva Photos

Bezpieczne hasło – pierwsza linia obrony

Z poczty elektronicznej, bankowości internetowej, mediów społecznościowych, Profilu Zaufanego czy Internetowego Konta Pacjenta korzystamy dziś niemal codziennie. Przechowujemy tam wiele prywatnych i ważnych informacji, dlatego dostęp do każdego z tych miejsc powinien być odpowiednio chroniony. Pierwszym zabezpieczeniem jest zazwyczaj hasło. Warto więc zadbać, aby było naprawdę skuteczne.

Przez lata zalecano tworzenie skomplikowanych haseł zawierających wielkie i małe litery, cyfry oraz znaki specjalne. W efekcie powstawały krótkie kombinacje podobne do „Kasia123!” albo „Wakacje2026!”. Takie hasła tylko sprawiają wrażenie bezpiecznych. Imię bliskiej osoby, popularne słowo czy aktualny rok można stosunkowo łatwo przewidzieć.

Obecnie eksperci zwracają uwagę przede wszystkim na długość hasła. CERT Polska rekomenduje, aby miało ono co najmniej 14 znaków, a najlepiej jeszcze więcej. Dobrym rozwiązaniem może być hasło zbudowane z kilku przypadkowych słów. Powinny one tworzyć nietypowy, łatwy do wyobrażenia obraz. Na przykład:

CzarnyRowerWiezie3Chmury!

Takie zdanie jest długie, a jednocześnie można je stosunkowo łatwo zapamiętać. Możemy wyobrazić sobie czarny rower przewożący chmury i dzięki temu odtworzyć hasło w pamięci. To tylko przykład i nie należy go kopiować. Każdy powinien stworzyć własną, niepowtarzalną kombinację. Najlepiej wykorzystać kilka słów, które nie tworzą znanego powiedzenia, cytatu ani popularnego zwrotu.

Czego nie umieszczać w haśle?

Hasło nie powinno zawierać informacji, które ktoś może znaleźć w internecie albo poznać podczas zwykłej rozmowy. Nie używajmy więc:

- imienia lub nazwiska,
- daty urodzenia,

- imienia dziecka, wnuka albo domowego zwierzęcia,
- numeru telefonu,
- nazwy ulicy lub miejscowości,
- ulubionej drużyny sportowej,
- prostych ciągów znaków, takich jak „123456” czy „qwerty”,
- słowa „hasło” z dodaną cyfrą lub wykrzyknikiem.

Nie warto również tworzyć hasła przez przesuwanie palca po kolejnych klawiszach klawiatury. Takie układy są dobrze znane przestępcom i programom służącym do odgadywania haseł.

Jedno hasło do wszystkich kont?

Używanie jednego hasła w wielu miejscach jest wygodne, ale może mieć poważne konsekwencje. Wystarczy, że dane wyciekną z jednego sklepu internetowego lub portalu, aby przestępcy spróbowali zalogować się tym samym hasłem do naszej poczty, mediów społecznościowych, a nawet innych ważnych usług. Można porównać to do używania jednego klucza do mieszkania, samochodu, garażu i skrzynki pocztowej. Jeśli ktoś zdobędzie ten klucz, od razu uzyska dostęp do wielu miejsc.

Dlatego każde konto powinno mieć inne hasło. Szczególnej ochrony wymaga poczta elektroniczna. To właśnie na nią trafiają wiadomości umożliwiające zmianę haseł w innych serwisach. Przejęcie skrzynki może więc otworzyć przestępcy drogę do kolejnych kont. CERT Polska podkreśla, że dwie najważniejsze zasady to odpowiednia długość hasła oraz stosowanie innego hasła w każdym serwisie.

Czy trzeba regularnie zmieniać hasła?

Nie ma potrzeby zmieniania dobrego hasła co kilka tygodni wyłącznie „na wszelki wypadek”. Częste zmiany mogą prowadzić do tworzenia coraz prostszych kombinacji, na przykład „Jesien2026!”, a następnie „Zima2026!”.

Hasło należy zmienić niezwłocznie, gdy:

- otrzymamy informację o wycieku danych z serwisu,
- zauważymy nieznane logowanie lub podejrzaną aktywność,
- wpisaliśmy je na stronie, która mogła być fałszywa,
- przekazaliśmy je innej osobie,
- używaliśmy go również na koncie, którego bezpieczeństwo zostało naruszone.

Aktualne rekomendacje nie zalecają profilaktycznej, okresowej zmiany silnych haseł, jeśli nic nie wskazuje na ich ujawnienie.

Jak zapamiętać wiele różnych haseł?

Magiczny Kraków

Kilka długich i niepowtarzalnych haseł trudno utrzymać w pamięci. Pomocny może być menedżer haseł, czyli program działający jak cyfrowy sejf.

Menedżer może:

- tworzyć długie, przypadkowe hasła,
- przechowywać je w zaszyfrowanej bazie,
- automatycznie uzupełniać dane podczas logowania,
- synchronizować hasła między telefonem a komputerem.

Użytkownik nie musi pamiętać wszystkich kombinacji. Wystarczy jedno bardzo dobre hasło główne, które otwiera menedżer. Powinno być wyjątkowo długie, niepowtarzalne i nieużywane w żadnym innym miejscu.

Prosty menedżer haseł jest już dostępny w wielu przeglądarkach internetowych oraz telefonach. Istnieją również osobne aplikacje oferujące taką funkcję. Warto korzystać wyłącznie z rozwiązań pochodzących z oficjalnego sklepu z aplikacjami lub strony znanego dostawcy. Menedżery mogą nie tylko przechowywać dane, lecz także generować bezpieczne hasła i uzupełniać je na stronach logowania.

Czy hasła na kartce to błąd?

Jeżeli jednak ktoś nie czuje się jeszcze pewnie w korzystaniu z menedżera, zapisanie haseł na kartce przechowywanej w zamkniętym, bezpiecznym miejscu w domu może być rozsądniejszym rozwiązaniem niż używanie jednego prostego hasła do wszystkich kont.

Na kartce nie trzeba podawać pełnej nazwy serwisu ani loginu, jeśli mogłoby to ułatwić dostęp do konta osobie postronnej. **Nie należy natomiast przechowywać haseł w niezabezpieczonym pliku na pulpicie, w wiadomości e-mail czy w notatce zatytułowanej „Moje hasła”.**

Hasło to nie wszystko

Nawet bardzo dobre hasło może zostać wykradzione, na przykład po wpisaniu go na fałszywej stronie. Dlatego warto włączyć **weryfikację dwuetapową, nazywaną również 2FA.** Wtedy do zalogowania potrzebne jest nie tylko hasło, ale również dodatkowe potwierdzenie, na przykład w aplikacji, kodem jednorazowym albo przy użyciu odcisku palca.

Jeżeli przestępca pozna hasło, nadal nie powinien dostać się do konta bez drugiego zabezpieczenia. Weryfikację dwuetapową warto uruchomić przede wszystkim na poczcie elektronicznej, profilach w mediach społecznościowych i innych najważniejszych kontach.

Marcin Majerek