PIGUŁKA WIEDZY

Bądź bezpieczny(a)

w Internecie

Autorka: Małgorzata Szlendak

Opracowanie graficzne: Małgorzata Szlendak

Publikacja powstała w ramach projektu: „Senioralne Grupy Rozwijania Kompetencji Cyfrowych: dofinansowanego ze środków programu wieloletniego na rzecz Osób Starszych „Aktywni+" na lata 2021-2025.

Publikacja dostępna jest bezpłatnie na stronie: www.pro-cultura.pl

Materiał opracowany ze wsparciem sztucznej inteligencji.

Warszawa, wrzesień 2025.

Słowniczek

1. **Aktualizacja** – wgranie nowej wersji programu lub systemu, która naprawia błędy i zwiększa bezpieczeństwo.
2. **Antywirus** – program chroniący komputer lub telefon przed wirusami i złośliwym oprogramowaniem.
3. **CERT Polska** – instytucja w Polsce, która pomaga w przypadku zagrożeń i oszustw w Internecie https://cert.pl/
4. **Certyfikat bezpieczeństwa (https)** – kłódka w pasku adresu przeglądarki oznaczająca, że połączenie ze stroną jest szyfrowane i bezpieczniejsze.
5. **Cookies** (ciasteczka) – małe pliki zapisywane przez strony, które zapamiętują nasze ustawienia i historię.
6. **Deepfake (czyt: dip-fejk)** – przerobione zdjęcie, film lub nagranie głosu, które wygląda jak prawdziwe.
7. **Fake news (czyt: fejk njus)** fałszywa wiadomość podawana w Internecie lub mediach tak, by wyglądała na prawdziwą; najczęściej służy manipulacji lub wywołaniu emocji.
8. **Kradzież tożsamości** – sytuacja, gdy ktoś podszywa się pod nas, aby np. wziąć kredyt.
9. **Malware (czyt: „malwer”)** - złośliwe oprogramowanie – ogólna nazwa dla wirusów, trojanów i innych programów, które robią coś złego na urządzeniu.
10. **Menedżer haseł** – program, który przechowuje wszystkie hasła w bezpiecznym miejscu.

11. **Phishing (czyt.: piszing)** – fałszywe e-maile, SMS-y lub strony internetowe udające prawdziwe, które mają nas skłonić do podania danych lub kliknięcia w link.

12. **Ransomware (czyt.: ransomwer)** – wirus, który blokuje komputer lub pliki i żąda okupu za ich odblokowanie.

13. **Silne hasło** – hasło trudne do odgadnięcia, składające się z liter, cyfr i znaków specjalnych.

14. **SIM swapping (czyt: sim słoping)** (podmiana karty SIM) – przejęcie numeru telefonu ofiary, aby dostać się np. do bankowości internetowej.

15. **Smishing (smiszing)** – oszustwo przez SMS (np. wiadomość o paczce lub konieczności dopłaty).

16. **Spam** – niechciane wiadomości, najczęściej reklamy, wysyłane masowo.

17. **Tożsamość cyfrowa** – nasze dane w Internecie, np. imię, e-mail, PESEL, loginy do kont.

18. **Trojan** – program podszywający się pod coś pożytecznego (np. grę), a w tle robiący coś złego.

19. **Uwierzytelnianie dwuskładnikowe** (2FA) – dodatkowe zabezpieczenie logowania, np. kod SMS oprócz hasła.

20. **Vishing (czyt: wiszing)** – oszustwo przez telefon (np. fałszywy „wnuczek” albo „pracownik banku”).

Tożsamość cyfrowa i internetowa

Kiedy korzystamy z telefonu czy komputera, zostawiamy w sieci różne informacje o sobie. Tworzą one **naszą tożsamość cyfrową** – czyli obraz tego, kim jesteśmy w świecie komputerów i Internetu. Dotyczy to m.in naszych oficjalnych spraw obywatelskich.

Część tej tożsamości, którą widać publicznie, nazywa się **tożsamością internetową**. To np. Twój profil na Facebooku, adres e-mail, zdjęcia, które wrzucasz, czy komentarze, które zostawiasz pod artykułami.

Ślad internetowy

Za każdym razem, kiedy korzystasz z Internetu, zostawiasz po sobie **ślad internetowy** – trochę jak ślady butów na piasku. Może to być wyszukiwane hasło w Google, odwiedzona strona albo zdjęcie wnuka wrzucone na Facebooka. Czasem wydaje się, że jak coś usuniemy, to ślad znika. Ale w rzeczywistości w sieci wiele rzeczy zostaje – ktoś mógł skopiować zdjęcie, zapisać nasz post albo przesłać go dalej. Dlatego mówi się, że **„w Internecie nic nie ginie”**.

Czy to znaczy, że trzeba się bać? Absolutnie nie! To oznacza tylko, że warto **korzystać z sieci z głową** – tak, jak w codziennym życiu. Nie dajemy obcemu kluczy do mieszkania, nie opowiadamy każdemu w kolejce w sklepie o swoich problemach i nie zostawiamy portfela na ławce w parku.

W Internecie obowiązują podobne zasady – uważność i rozsądek to najlepsza ochrona.

Podstawy bezpieczeństwa

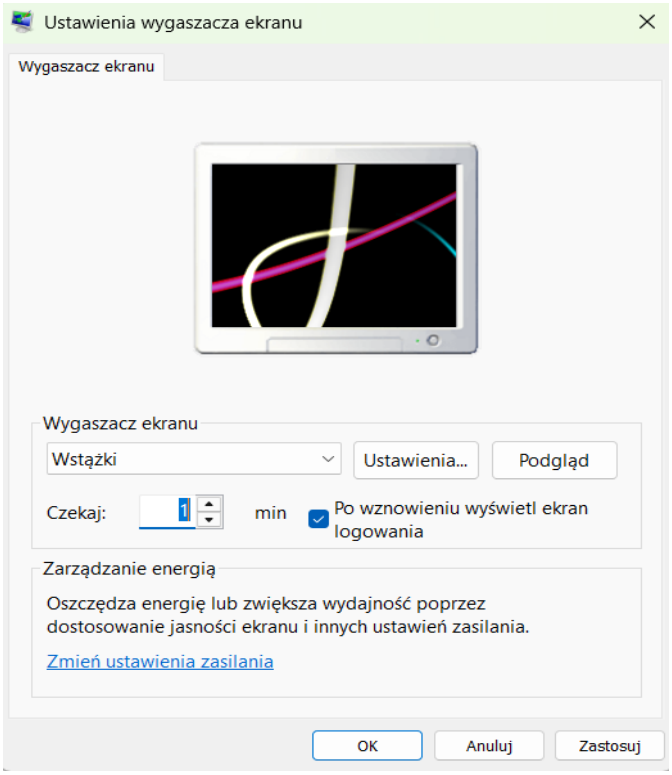
Aktualizuj i blokuj – to Twoja tarcza

Telefon i komputer to dziś nasze podręczne centra informacji – trzymamy w nich zdjęcia, kontakty, hasła i dostęp do banku. Warto o nie dbać tak samo, jak o inne ważne rzeczy. Regularne **aktualizacje**, program **antywirusowy** i blokada ekranu to proste kroki, które zwiększają bezpieczeństwo i sprawiają, że urządzenia działają sprawniej.

W praktyce:

Na telefonie i komputerze pojawia się czasem komunikat „dostępna aktualizacja". Sprawdź, co domaga się Twojej uwagi. Jeśli to program antywirusowy, kliknij: „Zainstaluj teraz" zamiast odkładać. W większości komputerów z systemem Windows działa już darmowy *Microsoft Defender*. Wystarczy, że system jest aktualny.

Na smartfonie ustaw PIN, wzór lub odcisk palca (taką możliwość znajdziesz w „Ustawienia → Zabezpieczenia" lub „Ustawienia → Ekran blokady"). Na komputerze ustaw hasło logowania oraz blokuj ekran, gdy odchodzisz od biurka. Możesz ustawić automatyczny wygaszacz ekranu z funkcją logowania. (Ustawienia → Personalizacja → Ekran blokady)



Silne hasło = spokój

Hasła to pierwsza linia obrony w sieci. Krótkie i powtarzalne są łatwe do złamania, dlatego warto wybierać dłuższe, składające się z liter, cyfr i znaków specjalnych. Dobrze też, aby do każdego konta było inne hasło – wtedy przejęcie jednego nie oznacza od razu kłopotów wszędzie. Jeśli trudno je zapamiętać – rozważ prosty **menedżer haseł** albo zapisz w bezpiecznym miejscu poza komputerem. Nie bój się **uwierzytelniania dwuskładnikowego**. Proces sprawdzania naszej tożsamości jest dłuższy, ale przez to – bezpieczniejszy.

Pomyśl dwa razy, zanim coś pokażesz światu

Każde zdjęcie, komentarz czy wpis pozostają w Internecie dłużej, niż się wydaje. Nawet jeśli coś usuniemy, ktoś mógł to wcześniej skopiować lub przesłać dalej. Dlatego publikuj tylko to, czym naprawdę chcesz się dzielić – dla własnego spokoju i bezpieczeństwa. Zanim opublikujesz zdjęcie lub wpis zastanów się, kto może to zobaczyć? Na Facebooku i w innych serwisach możesz zmieniać **ustawienia prywatności**. Naucz się to robić.

Powyższe zasady są uniwersalne i stanowią absolutną podstawę bezpiecznego zachowania w cyfrowym świecie. Jeśli o nią nie zadbamy, możemy stać się łatwym celem dla przestępców. Należy ponadto pamiętać, że w Internecie nie tylko nic nie ginie, ale ...

 nie zawsze wszystko jest takim, jakim się zdaje

Niestety, wraz z rozwojem nowych technologii, rozszerzył się także wachlarz sposobów na oszukiwanie. I chodzi tu nie tylko o działanie na szkodę pojedynczych osób (wyłudzanie pieniędzy, szkalowanie, czy hejt), ale także o manipulacje całymi grupami społecznymi - m.in. w celu zdobycia wpływów

politycznych i gospodarczych. Prawdopodobieństwo, że znajdziemy się w zasięgu tego rodzaju manipulacji jest w dzisiejszych czasach bardzo duże.

Stosuj zasadę ograniczonego zaufania

Zasada ograniczonego zaufania jest stara, jak świat ale obecnie trzeba mieć się na baczności także w sieci. Co zatem robić, a czego nie? Oto krótki poradnik:

- Nie ufaj w 100% SMS-om, e-mailom i telefonom od „instytucji", „rodziny w potrzebie", czy „bogatego szejka". Przestępcy często wykorzystują dobre serce, chwilę nieuwagi, rutynę lub zaskoczenie. ZAWSZE DOKŁADNIE czytaj wiadomości i nie działaj impulsywnie. Nie klikaj w podejrzane linki i nie otwieraj załączników od nieznanych nadawców.

- Zawsze sprawdzaj informacje w kilku źródłach. Pamiętaj, że wiarygodnie wyglądające wiadomości, zdjęcia i filmy mogą być w łatwy sposób sfabrykowane. Dzisiejsza technologia pozwala na podmienianie twarzy lub całych sylwetek, „produkowanie" dowolnego głosu z niewielkiej próbki i tworzenie dowolnych iluzji. Nie daj się dezinformacji (patrz: **deep fake** i **fake news** w Słowniczku).
- Jeśli coś budzi Twoje wątpliwości – **porozmawiaj z rodziną lub znajomymi**. W razie podejrzenia oszustwa – **skontaktuj się z bankiem, operatorem lub policją** poprzez oficjalną infolinię.
  Zawsze lepiej zapytać, niż żałować.