Jak Chronić Swoje Dane Osobowe?

Ochrona prywatności zaczyna się od codziennych nawyków i ograniczonego zaufania. Ochrona w świecie cyfrowym i analogowym oraz kroki w sytuacjach awaryjnych.

Dane osobowe to informacje pozwalające zidentyfikować konkretną osobę, np. imię i nazwisko, adres, numer telefonu czy PESEL.

Aby je chronić, należy ostrożnie udostępniać dane w Internecie i przez telefon oraz sprawdzać, komu i w jakim celu są przekazywane.

Warto stosować **silne hasła**, **uwierzytelnianie dwuskładnikowe** oraz **unikać klikania w podejrzane linki w e-mailach i SMS-ach**. Należy dbać też o bezpieczeństwo dokumentów papierowych.

Każdy ma prawo wiedzieć, kto przetwarza jego dane i może żądać ich poprawienia lub usunięcia.

W przypadku podejrzenia nadużycia warto szybko zareagować, np. kontaktując się z bankiem lub zgłaszając sprawę odpowiednim instytucjom.

Materiał opracowany w ramach zadania publicznego realizowanego przez Stowarzyszenie Wspierania Aktywności Obywatelskiej CIVIS SUM, finansowane ze środków przekazanych przez Powiat Świebodziński na podstawie umowy o powierzenie realizacji zadania publicznego pn. “Prowadzenie punktu nieodpłatnej pomocy prawnej i nieodpłatnego poradnictwa obywatelskiego oraz realizacja zadań z zakresu edukacji prawnej w powiecie świebodzińskim w 2026 r. ”.

Co musisz chronić?

Twoja Cyfrowa Tożsamość

Dane pod ochroną prawną

Większość informacji, którymi posługujemy się na co dzień, podlega ścisłej ochronie prawnej przed nieuprawnionym wykorzystaniem.

Bezpieczeństwo poza siecią

Dokumenty papierowe

Nie zostawiaj dokumentów z danymi w miejscach publicznie dostępnych i zawsze niszcz je przed wyrzuceniem (np. w niszczarce).

Prawo do bycia zapomnianym

Masz prawo wiedzieć, kto przetwarza Twoje dane, żądać ich poprawienia, usunięcia lub ograniczenia ich przetwarzania.

Twoja tarcza w internecie

Silne i unikalne hasła

Stosuj skomplikowane hasła i nigdy nie używaj tego samego klucza do wielu różnych serwisów internetowych.

Uwierzytelnianie dwuskładnikowe (2FA)

Włącz dodatkową warstwę ochrony, która wymaga potwierdzenia logowania kodem wysłanym na Twój telefon.

Weryfikuj źródło kontaktu

Zanim podasz dane, sprawdź, czy osoba po drugiej stronie słuchawki lub monitora faktycznie reprezentuje bank, kuriera lub urząd.

Uwaga na pułapki!

Fałszywe e-maile i SMS-y

Przestępcy tworzą strony ludząco podobne do witryn banków lub sklepów, aby wyłodzić Twoje dane logowania i numery kart.

Nie klikaj w podejrzane linki

Zawsze sprawdzaj adres URL strony, na której się znajdujesz, i unikaj otwierania linków z niepewnych wiadomości.

Co robić w razie kłopotów?

Szybka reakcja to podstawa

Jeśli podejrzewasz wyciek danych, natychmiast skontaktuj się z bankiem, zastrzeż dokumenty tożzamości i zgłoś sprawę odpowiednim służbom.