

Kradzież tożsamości to sytuacja, w której (cyber)przestępca pozyskuje informacje o Tobie i wykorzystuje je w niepożądany sposób. Przykłady? Wyłudzenie pożyczki, fałszywe transakcje bankowe, podszywanie się w korespondencji – można je mnożyć. Można również się przed nimi chronić. Jak to zrobić?

Cyfrowy ślad – zostawiaj go ostrożnie

Wg danych zawartych w raporcie GUS „[Społeczeństwo informacyjne w Polsce w 2020 roku](#)”, ponad 90% gospodarstw domowych w Polsce ma dostęp do internetu, a z sieci korzysta regularnie (co najmniej raz w tygodniu) 81,4% osób w wieku 16-74 lata. Każda z nich, bez wyjątku, zostawia swój cyfrowy ślad - Ty też.

Za każdym razem, kiedy przeglądasz strony internetowe, robisz zakupy online, korzystasz z poczty elektronicznej, mediów społecznościowych, czy komunikatorów – zbierane są pewne informacje na Twój temat. Wykorzystuje się je na różne sposoby, np. do zapamiętywania Twoich preferencji, czy tworzenia anonimowych statystyk odwiedzanych serwisów.

- Poruszając się w cyberprzestrzeni nie da się uniknąć pozostawiania po sobie cyfrowych śladów. Warto jednak wiedzieć, gdzie i jakie swoje dane zostawiamy oraz jak to ograniczać. W ten sposób zminimalizujemy prawdopodobieństwo, że nasze dane osobowe, czy informacje o naszej aktywności staną się narzędziem w rękach cyberprzestępców – mówi Marek Zagórski, sekretarz stanu w KPRM i pełnomocnik rządu ds. cyberbezpieczeństwa.

Ogranicz ryzyko

Ochrona prywatności w sieci to coś, o czym musimy pamiętać codziennie, podczas każdej aktywności podejmowanej online. Oto kilka wskazówek, jak zwiększyć bezpieczeństwo swoich danych:

- **Publikuj mniej.** Pamiętaj, że treści udostępniane na forach, czy w mediach społecznościowych - również w grupach prywatnych - stają się publiczne.
- **Ostrożnie dobieraj zdjęcia.** Źródłem cyberataku może być np. widoczny w kadrze dokument, czy choćby fragment numeru karty kredytowej.
- **Używaj unikalnych haseł.** Do każdego z kont/kanałów loguj się za pomocą innych danych. Dodatkowo - ustaw uwierzytelnianie dwuskładnikowe.
- **Czytaj politykę prywatności.** Jeśli tworzysz jakiegokolwiek konto internetowe, zwróć uwagę, jakie dane są zbierane przez serwis/portal, z którego korzystasz – podaj tylko te niezbędne. **Masz wątpliwości? Zrezygnuj.**
- **Korzystaj z pewnych/wiarygodnych aplikacji.** Zanim pobierzesz apkę – dokładnie ją sprawdź. Czy pochodzi od zaufanego wydawcy? Jakie ma wymagania dotyczące uprawnień (np. dostęp do lokalizacji, kontaktów)? Jeśli cokolwiek budzi Twoje obawy – wybierz inną aplikację.
- **Zmień ustawienia przeglądarki.** Wybierz opcję „prywatne” lub włącz tryb incognito. Dzięki temu ograniczysz zakres udostępnianych informacji, a także sposób używania i przechowywania plików cookies.

Stosowanie się do tych zasad skutecznie utrudni cyberprzestępcom dostęp do informacji na Twój temat. Mimo to – zwracaj uwagę na wszelkie niepokojące sygnały.

Włącz czujność

Chroń swoje Ja, czyli jak nie stracić tożsamości w sieci

Kategoria: Styl życia

Opublikowano: środa, 21, kwiecień 2021 11:23

Artur Duda

Odśłony: 610

Jeśli już niestety staniesz się ofiarą kradzieży tożsamości, kluczowa jest szybka reakcja, która pozwoli zminimalizować straty. Co powinno wzbudzić Twoje obawy?

- **Podejrzane transakcje.** Sprawdzaj regularnie wyciągi z kont i kart bankowych. Upewnij się, że to Ty dokonałeś/-eś wszystkich odnotowanych tam operacji.
- **Odrzucenie karty i/lub nieuzasadniona windykacja.** Masz problem z płatnością, zdarzyło Ci się odebrać list lub telefon w sprawie długu, o którym nie masz pojęcia? Wyjaśnij to.

Ostrożności nigdy za wiele!

Nie wahaj się – reaguj

Twoja tożsamość została skradziona? Nie czekaj, zgłoś sprawę organom ścigania. Możesz to zrobić online.

Podejrzewasz, że ktoś złożył w Twoim imieniu wniosek o kredyt, albo o dowolne świadczenie? Poinformuj o tym bank lub odpowiednią instytucję.

Jeśli trafisz w internecie na stronę, która wyłudza dane osobowe lub informacje uwierzytelniające, również możesz i powinnaś/powinieneś zareagować. Zgłoś to za pomocą dostępnego internetowego [formularza](#).

W ten sposób możesz ostrzec innych przed zagrożeniem.

- *W walce z cyberprzestępczością, tak samo ważne jak zapobieganie jest odpowiednie reagowanie* – dodaje minister Marek Zagórski.

Więcej informacji o tym, jak dbać o bezpieczeństwo w internecie znajdziesz na naszej stronie GOV.pl/cyfrizacja oraz w dostępnej na GOV.pl [bazie wiedzy](#) na temat cyberbezpieczeństwa.

Źródło: MC