XIX Dzień Ochrony Danych Osobowych

28 stycznia 2025r.

Jak cyberprzestępcy wykradają hasła?

Cyberprzestępcy stosują różnorodne techniki, aby zdobyć Twoje dane logowania.

Oto pięć najczęściej używanych metod:

Ataki socjotechniczne (phishing):

Ataki socjotechniczne (phishing): Przestępcy podszywają się pod zaufane osoby lub instytucje, wysyłając wiadomości e-mail lub SMS-y, które wyglądają na autentyczne. Często wywołują poczucie pilności, strachu lub ciekawości, aby skłonić Cię do podjęcia niepożądanych działań.

Złośliwe oprogramowanie (malware):

Programy takie jak keyloggery rejestrują każde naciśnięcie klawisza na Twoim urządzeniu, umożliwiając przestępcom przechwycenie loginów, haseł i innych wrażliwych danych.

Ataki brute force:

Cyberprzestępcy używają zautomatyzowanych narzędzi do odgadywania haseł, próbując wielu kombinacji. Słabe lub popularne hasła są szczególnie podatne na tego typu ataki.

Wyciek danych:

Gdy serwis internetowy zostanie zhakowany, dane użytkowników mogą zostać ujawnione. Jeśli używasz tego samego hasła w wielu miejscach, jedno naruszenie może zagrozić wszystkim Twoim kontom.

Zakup skradzionych danych:

Przestępcy mogą nabywać dane logowania na czarnym rynku od innych hakerów, którzy wcześniej je wykradli.

Jak się chronić?

Stosuj długie, unikalne hasła

dla każdego konta. Najlepiej używać haseł w formie zdań.

Korzystaj z menedżera haseł

aby bezpiecznie przechowywać i zarządzać swoimi hasłami.

Włączaj uwierzytelnianie wieloskładnikowe (MFA)

tam, gdzie to możliwe, aby dodać dodatkową warstwę zabezpieczeń.

Pamiętaj: Twoje dane są cennym zasobem.
Świadome i ostrożne działanie w sieci to klucz do ich ochrony.

XIX Dzień Ochrony Danych Osobowych

28 stycznia 2025r.

Czy kserowanie dowodu osobistego jest legalne?

Kiedy kopiowanie dowodu jest legalne?

Zgodnie z przepisami prawa, instytucje mogą przetwarzać dane z dowodu osobistego tylko wtedy, gdy mają ku temu wyraźną podstawę prawną, np.:

Banki i instytucje finansowe

mogą kopiować dowód osobisty w ramach przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu (na mocy ustawy AML).

Operatorzy telekomunikacyjni

mają prawo kopiować dowód w procesie zawierania umowy na usługi telekomunikacyjne.

Firmy ubezpieczeniowe

mogą sporządzać kopie dowodów osobistych przy zawieraniu umów ubezpieczeniowych.

Czy wypożyczalnia rowerów może kserować dowód osobisty?

Nie. Wypożyczalnie rowerów, samochodów czy sprzętu sportowego nie mają podstawy prawnej do kopiowania dowodu osobistego. Mogą jedynie:

- ☑ Zanotować dane identyfikacyjne z dowodu, takie jak imię, nazwisko i numer dokumentu, jeśli jest to konieczne do wykonania umowy.
- ☒ Nigdy jednak nie powinny tworzyć pełnych kopii dowodów osobistych, które zawierają nadmiarowe informacje, takie jak numer PESEL czy zdjęcie.

Jak reagować, gdy firma żąda kopii dowodu bez uzasadnienia?

Zapytaj o podstawę prawną żądania.

Każda instytucja, która przetwarza Twoje dane, musi wyjaśnić, na jakiej podstawie to robi.

Zaproponuj alternatywę

np. spisanie tylko niezbędnych danych.

Zgłoś nieprawidłowości

do Prezesa Urzędu Ochrony Danych Osobowych (UODO), jeśli uważasz, że doszło do naruszenia Twoich praw.

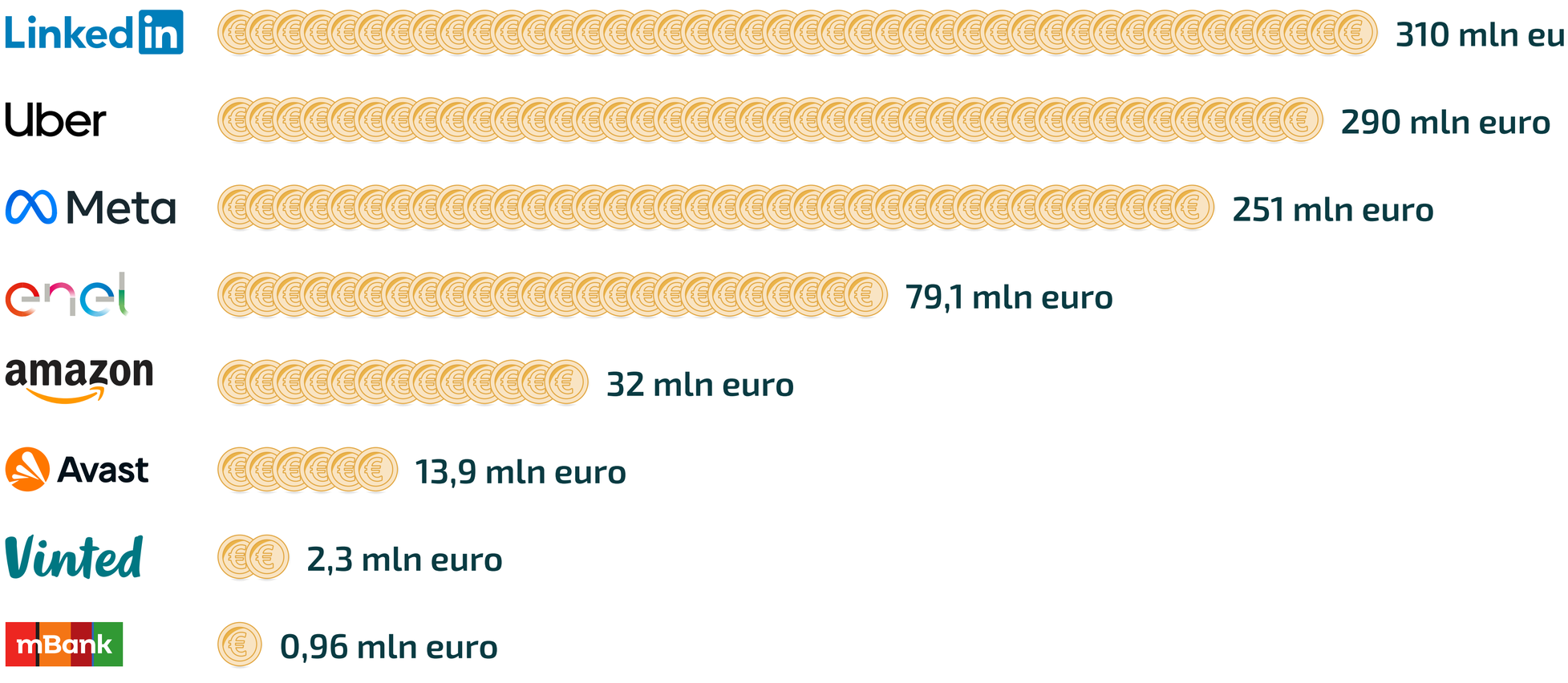
Pamiętaj: Twoje dane są Twoim majątkiem – nie udostępniaj ich bez potrzeby!

XIX Dzień Ochrony Danych Osobowych

28 stycznia 2025r.

Kary RODO w 2024

Znane firmy ukarane za naruszenia RODO w 2024:



Największe kary RODO w 2024 w Polsce:

1 **mBank**
4 053 173 zł

Prezes UODO nałożył na mBank karę 4 053 173 zł **za niezawiadomienie osób poszkodowanych wyciekiem danych**. Pracownik firmy przetwarzającej dane osobowe na zlecenie banku pomylił się i przesłał dokumenty klientów do innej instytucji finansowej. Dokumenty wróciły do banku, ale koperta wcześniej została otwarta. Bank nie zawiadomił o problemie klientów, mimo że po zgłoszeniu naruszenia PUODO poinformował o konieczności podjęcia takich działań.

2 **Morele.net**
3 819 960 zł

Kara została nałożona na Morele.net w 2019 r. **za niewłaściwe zabezpieczenie danych osobowych klientów**, co doprowadziło do wycieku. W styczniu 2024 roku UODO podtrzymał decyzję o nałożeniu kary, zwiększając jej wysokość z pierwotnych 2 830 410 zł do 3 819 960 zł.

3 **American Heart of Poland S.A.**
1 440 549 zł

American Heart of Poland S.A. została ukarana karą w wysokości 1 440 549 zł **za m.in. niewłaściwą ochronę danych osobowych po ataku hakerskim**. Naruszenie objęło dane 21 tys. osób, w tym informacje zdrowotne i finansowe. W toku postępowania Prezes UODO nie tylko zwrócił uwagę na niewystarczające środki bezpieczeństwa zastosowane przez administratora, ale również brak regularnego testowania systemów oraz niewłaściwą analizę ryzyka.

4 **Res-Gastro M. Gaweł Sp. k.**
238 345 zł

Pracownik firmy gastronomicznej Res-Gastro M. Gaweł Sp. k. z Kolbuszowej na Podkarpaciu **zgubił pendrive'a z danymi osobowymi**. Prezes UODO ustalił, że sposób przetwarzania danych osobowych był niezgodny z obowiązującymi przepisami RODO ze względu na niepoprawnie przeprowadzoną analizę ryzyka, która nie przewidziała zagrożenia polegającego na zagubieniu nośnika danych. Nie zastosowano odpowiednich środków organizacyjnych i technicznych, aby zapewnić bezpieczne przetwarzanie danych, co skończyło się karą 238 tys. 345 zł. Wysokość kary wynika m.in z dużych obrotów firmy.

XIX Dzień Ochrony Danych Osobowych

28 stycznia 2025r.

Najwyższe kary RODO w historii:

1 **Meta (Facebook)**
1,2 miliarda euro (2023)

Jest to obecnie najwyższa kara w historii RODO. Została nałożona przez irlandzki organ ochrony danych **za naruszenie przepisów dotyczących transferu danych osobowych** użytkowników z UE do USA

2 **Amazon**
746 milionów euro (2021)

Kara nałożona przez luksemburski organ ochrony danych **za naruszenia związane z przetwarzaniem danych osobowych** w celach reklamowych bez odpowiedniej zgody użytkowników

3 **Instagram**
405 milionów euro (2022)

Kara nałożona przez irlandzki organ ochrony danych **za naruszenia prywatności dzieci**, w tym publikowanie numerów telefonów i adresów e-mail małoletnich użytkowników

4 **WhatsApp**
225 milionów euro (2021)

Kara nałożona przez irlandzki organ ochrony danych **za brak przejrzystości w informowaniu użytkowników** o przetwarzaniu ich danych osobowych

5 **Google LLC**
150 milionów euro (2021)

Kara nałożona przez francuski organ ochrony danych (CNIL) **za stosowanie niezgodnych z prawem mechanizmów uzyskiwania zgody na pliki cookie**

6 **Enel Energia SpA**
79,1 miliona euro (2024)

Najnowsza z wysokich kar, nałożona przez włoski organ ochrony danych **za naruszenia związane z telemarketingiem**

Główne przyczyny nałożenia kar RODO w 2024r.:

1 **Niewystarczające środki techniczne i organizacyjne zabezpieczające dane osobowe**

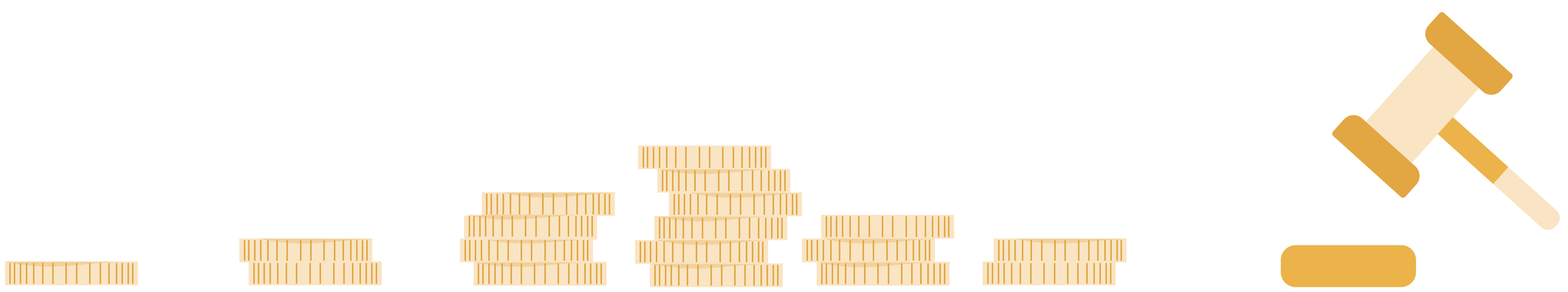
2 **Opóźnienia w zgłaszaniu naruszeń ochrony danych**

3 **Nieuprawnione przetwarzanie danych osobowych**

4 **Naruszenia prywatności pracowników**

5 **Brak odpowiedniej podstawy prawnej do przetwarzania danych**

6 **Niedopełnienie obowiązku informacyjnego**



XIX Dzień Ochrony Danych Osobowych

28 stycznia 2025r.

Źródła

1. **Unveiling the Shadows: How Cyber Criminals Steal Your Passwords;**
   https://www.sans.org/newsletters/ouch/unveiling-shadows-how-cyber-criminals-steal-your-passwords/

2. **Dutch DPA imposes a fine of 290 million euro on Uber because of ...**
   https://www.autoriteitpersoonsgegevens.nl/en/current/dutch-dpa-imposes-a-fine-of-290-million-euro-on-uber-because-of-transfers-of-drivers-data-to-the-us

3. **[PDF] Dutch DPA Fines Uber €290m for GDPR Data Transfer Violation**
   https://www.willkie.com/-/media/files/publications/2024/09/dutch-dpa-fines-uber-290m-for-gdpr-data-transfer-violation.pdf

4. **Data transfers outside the EU: UBER fined €290 million - CNIL**
   https://www.cnil.fr/en/data-transfers-outside-eu-uber-fined-eu290-million

5. **DPA issues Uber €290 million fine for GDPR data transfer breach**
   https://www.pinsentmasons.com/out-law/news/dpa-issues-uber-290-million-fine-gdpr-data-transfer-breach

6. **Uber hit with $324 million EU fine for improper data transfer**
   https://www.theverge.com/2024/8/26/24228589/uber-eu-fine-gdpr-driver-data-transfer

7. **Uber's €290M GDPR fine: Lessons for data transfers**
   https://harperjames.co.uk/news/data-transfers-gdpr-fine/

8. **Amazon we Francji z gigantyczną karą. Za inwigilację pracowników**
   https://businessinsider.com.pl/gospodarka/amazon-we-francji-z-gigantyczna-kara-za-inwigilacje-pracownikow/tz1cl7v

9. **Biggest GDPR Fines of 2024 | Skillcast**
   https://www.skillcast.com/blog/biggest-gdpr-fines-2024

10. **Przegląd kar za naruszenie RODO w UE w 2024**
    https://www.politykabezpieczenstwa.pl/pl/a/przeglad-kar-za-naruszenie-rodo-w-ue-w-2024

11. **GDPR Enforcement Tracker - list of GDPR fines**
    https://www.enforcementtracker.com

12. **Biggest GDPR Fines of 2024 | Skillcast**
    https://www.skillcast.com/blog/biggest-gdpr-fines-2024

13. **Data protection authority fines Avast 13.9 million euros - Heise**
    https://www.heise.de/en/news/Tschechien-Datenschutzbehoerde-verdonnert-Avast-zu-13-9-Millionen-Euro-Strafe-9707928.html

14. **Czech DPA imposed fine of 351 million CZK for GDPR infringement**
    https://uoou.gov.cz/en/news/business-communication/czech-dpa-imposed-fine-of-351-million-czk-for-gdpr-infringement

15. **The five highest fines in May 2024 - Ailance - 2B Advice**
    https://2b-advice.com/en/2024/06/10/the-five-highest-fines-in-may-2024/

16. **Holenderski organ ochrony danych nakłada wysokie kary za naruszenia RODO dla Uber i Clearview AI**
    https://odoserwis.pl/a/2177/holenderski-organ-ochrony-danych-naklada-wysokie-kary-za-naruszenia-rodo-dla-uber-i-clearview-ai

17. **Kary RODO | Analiza przypadków i lista naruszeń 2024 - Orodo**
    https://orodo.pl/kary-rodo/

18. **Kary RODO w Polsce – lista kar pieniężnych (firmy i wysokości)**
    https://resilia.pl/blog/rejestr-kar-rodo-polskie-firmy-od-momentu-wprowadzenia/

19. **Bezpieczeństwo w firmie Przegląd kar za naruszenie RODO w**
    https://www.politykabezpieczenstwa.pl/pl/a/przeglad-kar-za-naruszenie-rodo-w-ue-w-2024

20. **Przegląd kar za naruszenie RODO w Polsce w 2024**
    https://www.politykabezpieczenstwa.pl/pl/a/przeglad-kar-za-naruszenie-rodo-w-polsce-w-2024

21. **Kara Prezesa UODO w wysokości prawie 1,5 mln złotych – wnioski ...**
    https://www.traple.pl/kara-prezesa-uodo-w-wysokosci-prawie-15-mln-zlotych-wnioski-dla-administratorow/

22. **GDPR Enforcement Tracker - list of GDPR fines**
    https://www.enforcementtracker.com

23. **GDPR Fines Structure and the Biggest GDPR Fines to Date - Exabeam**
    https://www.exabeam.com/explainers/gdpr-compliance/gdpr-fines-structure-and-the-biggest-gdpr-fines-to-date/

24. **Siedmiokrotny wzrost kar za naruszenie RODO w Europie - Prawo.pl**
    https://www.prawo.pl/prawo/kary-za-naruszenie-rodo-w-europie-duzy-wzrost,512924.html

25. **52 Biggest GDPR Fines and Penalties (2018 - 2024) - Enzuzo**
    https://www.enzuzo.com/blog/biggest-gdpr-fines