

Witam Państwa !
na webinarium organizowanym
w ramach Akademii Przedsiębiorczości
organizowanej przez **Fundację Przedsiębiorczości Revas**

Pokaż uczniom ile warte są ich dane
w sieci i dlaczego warto je chronić?

Magdalena Podgórska

AGENDA:

1. Statystyki i raporty – co o nas mówią?
2. Czym są dane osobowe?
3. O co chodzi z RODO ?
4. Jakie mamy prawa ?
5. Kto chce naszych danych?
6. Jak się chronić i dlaczego?
7. Gdzie szukać informacji i pomocy?

Dane w sieci ?!
O co tyle SZUMU ?



„Internet dzieci” — pierwszy raport z monitoringu aktywności dzieci i młodzieży w internecie

Pobierz raport



Raport dostępny: <https://cyfroweobywatelstwo.pl/internetdzieci/>

CO MÓWIĄ DANE ?

- ◆ Dzieci w wieku **7-12 lat** stanowią 11% wszystkich polskich internautów, co oznacza 1,4 mln aktywnych użytkowników w tej grupie wiekowej
- ◆ aż 94% dzieci w tym wieku korzysta z Internetu codziennie lub prawie codziennie
- ◆ 66% dzieci ma własny smartfon z dostępem do Internetu, a co 4. korzysta z własnego laptopa/komputera

Z jakich serwisów korzystają dzieci?

- ◆ YouTube (97%), Google (95%) i Messenger (60%).
- ◆ 32% regularnie korzysta z TikToka, mimo że formalnie jest on przeznaczony dla osób powyżej 13. roku życia.
- ◆ 24% dzieci odwiedza Facebooka, a 12% Instagrama.
- ◆ 31% dzieci korzysta z platform streamingowych, takich jak Netflix.

CO MÓWIĄ DANE ?

! Czas spędzany online:

- ◆ Średnio dzieci w wieku 7-12 lat spędzają w Internecie ponad 2 godziny dziennie.
- ◆ Dzieci korzystające z TikToka - na platformie 2 godziny i 11 minut dziennie, uruchamiając aplikację wielokrotnie.

⚠ Zagrożenia i wyzwania:

- ◆ W TOP 10 najczęściej odwiedzanych stron przez dzieci znalazły się także domeny z treściami nieodpowiednimi – w tym serwisy pornograficzne.
- ◆ Aż 50% dzieci w wieku 7-14 lat miało kontakt z treściami erotycznymi w IV kwartale 2024 roku.

Skąd się to bierze?



🏠 > Magazyn > [Nastolatki 3.0. Raport z ogólnopolskiego...](#)

📄 Raport 12 Kwietnia 2023 | 1 min. czytania

[Badania społeczne](#) [Edukacja](#) [Nauka](#)

Nastolatki 3.0. Raport z ogólnopolskiego badania uczniów i rodziców

Co dzieci robią, gdy spędzają czas przed komputerem lub z telefonem w rękę? Jakie zagrożenia mogą spotkać młodych ludzi w sieci? Badania „Nastolatki 3.0” realizowane w 2022 roku przez Thinkstat, zespół badania opinii działający w NASK, pokazują jak młodzi ludzie funkcjonują w świecie online oraz jaką wiedzę na temat tego wirtualnego życia mają ich rodzice.

Raport dostępny: <https://nask.pl/magazyn/nastolatki-3-0-raport-z-ogolnopolskiego-badania-uczniow-i-rodzicow>

Pliki do pobrania

CO MÓWIĄ DANE ?

- ◆ badano dzieci w wieku 7-19
- ◆ 25,8% nastolatków posiada od 5 do 8 kont na platformach i portalach społecznościowych
- ◆ ponad 40% młodzieży w tym wieku twierdzi, że w Internecie nie można odróżnić informacji prawdziwych od fałszywych
- ◆ 50,2% wyraża obawę związaną ze śledzeniem ich aktywności nie tylko w świecie cyfrowym, ale też realnym



Ile czasu spędzają w sieci ?

- ◆ YouTube (97%), Google (95%) i Messenger (60%).
- ◆ 32% regularnie korzysta z TikToka, mimo że formalnie jest on przeznaczony dla osób powyżej

CZYM JEST SHARENTING?

- **23% dzieci ma swój cyfrowy ślad już przed narodzinami** w postaci zdjęć z USG ciąży, które krążą w sieci. w Europie ten odsetek wynosi ok. 15%, a w Polsce 10% rodziców decyduje się na taką publikację
- **W Polsce 40% rodziców dokumentuje w mediach społecznościowych dorastanie swoich dzieci.** Rocznie publikują w sieci średnio 72 zdjęcia i 24 filmy. 25% rodziców deklaruje, że zanim wrzuci zdjęcie lub filmik, jeśli jest to możliwe (z uwagi np. na jego wiek), pyta swoje dziecko (dzieci) o zgodę
- 45,5% nastolatków w Polsce deklaruje, że ich rodzice lub opiekunowie upubliczniają ich wizerunek, przy czym 23,8% z nich odczuwa z tego powodu **zawstydzenie**, a 18,8% deklaruje **niezadowolenie**

A może
nie umiemy w Internety ?

Nie **ZAKAZY !**
Tak! **BEZPIECZNA PRZESTRZEŃ**

Zaczniemy od początku !

Po pierwsze !

- bądź na bieżąco
- zrozum mechanizmy
- poznaj zagrożenia

... od ataków socjotechnicznych, nieświadomego udostępniania danych, po niekontrolowane rozpowszechnianie i nielegalne gromadzenie danych ...

Po drugie !

- zobacz świat oczami Ucznia
- przyjrzyj się relacjom
- wspieraj dobrą radą

... znajomość sieci, mediów społecznościowych, aplikacji, komunikatorów, gier, trendów ...

Po trzecie !

- poznaj możliwości
- weryfikuj treści
- sprawdzaj ustawienia

... zmieniająca się technologia, nadążanie za zmianami, kontrola uprawnień, analiza ustawień systemowych ...

Odczarujmy RODO

RODO – Rozporządzenie Parlamentu Europejskiego i Rady (UE) z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie)

- 174 motywy
- 99 artykułów

Po co nam RODO ?

- **jednolitość i kontrola**
- przestrzeganie przepisów prawa
- **neutralność technologiczna**
- odpowiedzialność za dobra osobiste
- jakość obsługi, budowanie zaufania
- **świadomość prawna**
- porównanie na tle innych rozwiązań i ich następstw



KOGO NIE DOTYCZY?

- zwierząt 😊
- danych osób zmarłych
- osób prawnych (np. dane spółki)
- danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości
- danych wykorzystywanych do osobistego/ domowego użytku



CZYM SĄ DANE OSOBOWE?



DEFINICJA nr 1:

"**dane osobowe**" oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej ("osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak:

imię i nazwisko, numer PESEL, adres IP, dane o lokalizacji, rozpoznawalny login, czynniki określające fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej

(art. 4 pkt 1) RODO)

DEFINICJA nr 2:

„**szczególne kategorie danych osobowych**” – (dane wrażliwe) to dane ujawniające:

- pochodzenie rasowe lub etniczne
- poglądy polityczne
- przekonania religijne lub światopoglądowe
- przynależność do związków zawodowych
- dane dotyczące zdrowia (choroby, leczenie)
- dane genetyczne
- dane biometryczne (odcisk palca)
- dane dotyczące orientacji seksualnej

informacja o szczepieniu = dane wrażliwe

(art. 9 RODO)

PESEL ≠ dane wrażliwe

CO MÓWI O TYM PRAWO?



PODSTAWY PRAWNE

RODO – Rozporządzenie Parlamentu Europejskiego i Rady (UE) z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie)

ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych

ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną

ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych

ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne

ustawa z dnia 30 maja 2014 r. o prawach konsumenta

bo najważniejsza jest.....
podstawa przetwarzania
danych osobowych !

ZGODA

może stanowić podstawę prawną, tylko jeśli jest:
konkretna, świadoma, dobrowolna, jednoznaczna

WYKONANIE UMOWY

konieczne w celu realizacji umowy np. sprzedaży,
o pracę, zlecenia, wycieczki, ubezpieczenia

OBOWIĄZEK PRAWNY

podstawa przetwarzania danych jest w przepisach
prawnych np. ustawach, rozporządzeniach

OCHRONA ŻYWOTNYCH INTERESÓW

przetwarzanie danych w celach humanitarnych np. badania
epidemii, katastrofy czy klęski żywiołowe

INTERES PUBLICZNY

wykonywanie zadań publicznych

PRAWNIE UZASADNIONY INTERES

np. marketing bezpośredni, monitoring wizyjny,
zapobieganie oszustwom

PRAWA OSÓB, KTÓRYCH DANE PRZETWARZAMY:

1. dostępu do danych
2. sprostowania danych
3. usunięcia „**bycia zapomnianym**”
4. ograniczenia przetwarzania
5. przenoszenia danych
6. sprzeciwu (dot. „zgody”)
7. wniesienia skargi do UODO

- *art. 15-22 RODO*

DLACZEGO SZKOŁA NIE MOŻE „ZAPOMNIEĆ” UCZNIĄ?

1. zapomnieć można dane, na które ktoś wyraził zgodę
2. szkoła ma **obowiązek** zbierania danych
3. podstawa prawna – m.in. Prawo oświatowe
4. szkoła ma obowiązek archiwizacji danych uczniów
5. rozliczanie się z obowiązków

MAMY PRAWO WIEDZIEĆ !

czyli.... OBOWIĄZEK INFORMACYJNY



Kontakt ze sklepem stacjonarnym

Kontakt ze sklepem internetowym

Masz pytania odnośnie zakupów internetowych? Chcesz sprawdzić status swojego zamówienia?

Kontakt ze sklepem internetowym

Formularz

Temat *

Treść *

* Pola wymagane

Jeśli oczekujesz odpowiedzi

Imię

Nazwisko

Email *

Państwa dane osobowe przetwarzane będą w celu i w okresie niezbędnym dla wyrażania opinii, zapoznania się z nią oraz udzielania odpowiedzi. Administratorem danych jest Leroy - Merlin Polska sp. z o.o. z siedzibą w Warszawie przy ul. Burakowskiej 14, kontakt ochronadanych@leroymerlin.pl. Dane osobowe mogą być przekazywane podmiotom współpracującym na podstawie umów powierzenia w zakresie niezbędnym do realizacji powyższych celów. Państwa dane nie podlegają zautomatyzowanemu przetwarzaniu, w tym profilowaniu. Osobie, której dane dotyczą przysługuje prawo wniesienia sprzeciwu wobec przetwarzania, prawo dostępu do treści i przenoszenia swoich danych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, a także prawo wniesienia skargi do organu nadzorczego. Podanie danych jest dobrowolne, jednak niezbędne dla realizacji wyżej wymienionych celów. Więcej informacji znajduje się w [polityce prywatności](#).



Kod obrazka

Wyślij

Telefon

tel. (22) 250 84 44

Godziny pracy działu

pon - pt w godz. 7:00 - 21:00

sob w godz. 8:00 - 16:00

Adres

ul. Łowicka 33
99-120 Piątek

Rozpocznij czat



Zapraszamy do rozmowy z naszym konsultantem online



malowanie farb



Szycie firan i zasłon



Montaż wyposażenia łazienki



Zamówienia przez telefon



Bezterminowe zwroty



Montaż ogrodzenia

Obsługa klienta

Kontakt
Sklepy stacjonarne
Formy płatności
Czas i koszt dostawy
Zwroty i reklamacje
Pomoc/FAQ
Regulaminy
Zgłoś błąd

Dumnie wspieramy
Polską Reprezentację



Newsletter

Wpisz swój adres e-mail

Zapisz się

Wyrażam zgodę na przesłanie informacji handlowej przez Leroy Merlin Polska Sp. z o.o. z siedzibą w Warszawie przy ul. Burakowska 14 środkami komunikacji elektronicznej, z których przesyłania w każdej chwili mogę zrezygnować, lub dokonać zmiany swoich danych wprowadzonych w procesie rejestracji.

[mniej](#)

Państwa dane osobowe przetwarzane będą w celu świadczenia usługi newsletter tj. wysyłania informacji handlowej oraz dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratora danych, w szczególności marketingu bezpośrednio jego produktów lub usług. Dane będą przetwarzane w tym celu do czasu wycofania zgody. Administratorem danych jest Leroy Merlin Polska sp. z o.o. z siedzibą w Warszawie przy ul. Burakowska 14, kontakt ochronadanych@leroymerlin.pl. Dane osobowe mogą być przekazywane podmiotom współpracującym na podstawie umów powierzenia w zakresie niezbędnym do realizacji powyższych celów. Państwa dane podlegają zautomatyzowanemu przetwarzaniu, w tym profilowaniu w celu określenia osobistych preferencji na potrzeby przesłania oferty handlowej, jednakże nie będzie to wywoływać skutków prawnych lub podobny sposób znacząco wpływać na Państwa sytuację. Osobie, której dane dotyczą przysługuje prawo wniesienia sprzeciwu wobec przetwarzania, prawo dostępu do treści i przenoszenia swoich danych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, a także prawo wniesienia skargi do organu nadzorczego. Podanie danych jest dobrowolne, jednak niezbędne dla realizacji wyżej wymienionych celów. Więcej informacji znajduje się na stronie www.leroymerlin.pl w [polityce prywatności](#).

Zamówienie od Empik 145,99 zł

FORMA DOSTAWY odbiór w punkcie - Empik [zmień](#) 0,00 zł



Złóż zamówienie i odbierz 20% zniżki na zakupy w salonie

PUNKT ODBIORU Rzeszów Graffica (SP) [zmień](#)
ul. Płk. Leopolda Lisa-Kuli 19
35-025 Rzeszów

DANE ODBIORCY

Imię

MAGDALENA

Nazwisko

PODGÓRSKA

Nazwa firmy (opcjonalnie)

Numer telefonu

+48

Ulica

Numer

Lokal (opcjonalnie)

Kod pocztowy

Miejscowość

Użyj tych danych do faktury

ZAPISZ ADRES

ANULUJ

Płatność 145,99 zł

w tym koszt dostawy: 0,00 zł

Płatność BLIK



Wygeneruj kod BLIK w aplikacji Twojego banku i wprowadź go poniżej, aby dokończyć płatność.

123 456

PŁACĘ BLIKIEM

KTO CHCE MIEĆ NASZE DANE?



ILE KOSZTUJĄ DANE?

Firma PrivacyAffairs przygotowała analizę kosztów poszczególnych informacji, za które płacą cyberprzestępcy:

- **1000 \$** za komplet dokumentów oraz dane, które umożliwiają kradzież tożsamości,
- **75 \$** kosztuje zhakowane konto na Facebooku,
- **49 \$** kosztuje zhakowane konto na Twitterze,
- **15 \$** kosztuje sklonowana karta Mastercard oczywiście **wraz z kodem PIN !**

Uwaga: cena skradzionych danych pozwalających logować się do banku internetowego zależy od stanu konta.

Jeśli znajduje się na nim minimum 2 000 \$, można je kupić już za 65 \$!

ILE KOSZTUJĄ DANE?

Cena za jaką można kupić dane osobowe zależy od ich rodzaju:

- **nazwisko + numer telefonu**, adres czy wiek danej osoby = od **0,50 zł do 0,80 zł** za rekord
- w przypadku sprzedaży całej bazy danych cena ta spada nawet do 0,10 zł.
- bazy danych zawierające wyselekcjonowane kontakty, **tzw. leady**, czyli kontakty do osób, które już wykazały zainteresowanie danym produktem czy usługą = **od 100,00 zł do 200,00 zł** za sztukę
- **Najdroższą daną osobową jest PESEL oraz numer dowodu osobistego.**

KTO HANDLUJE DANymi ?

Danymi osobowymi najczęściej handlują:

- **firmy marketingowe,**
- **byli pracownicy banków, firm ubezpieczeniowych, operatorów telekomunikacyjnych,**
- **hakerzy,** którzy wykradają dane z komputerów firm oraz osób fizycznych.

Na “czarnym rynku” można znaleźć oferty sprzedaży dokumentów lub dostępu do konta:

- informacje z dowodu osobistego, karty płatniczej, paszportu,
- e-maile,
- profile w social mediach wraz z dostępem i obserwującymi

1. ograniczać dane !
2. chronić treści !
3. stosować narzędzia !



HASŁA !!

Najczęstszym źródłem wycieku haseł jest ich właściciel.

Dlatego zapamiętaj kilka prostych zasad:

- **nie zapisuj haseł** i nie umieszczaj ich w miejscach widocznych,
- nie stosuj **haseł łatwych** do odgadnięcia np. imion, dat urodzenia itp.,
- nie używaj **tych samych haseł w różnych systemach** i aplikacjach,
- nie zapisuj haseł „na stałe” oraz nie wykorzystuj opcji autozapamiętywania haseł,
- nie twórz haseł przewidywalnych, np. kolejno: HasłoLipiec1!, HasłoSierpień1!, HasłoWrzesień1!
- stosuj „szyfry” np. złożenie hasła z pierwszych liter wyrazów składających się na jakieś zdanie

(np. **OMGzzh*** od Oh My God znowu zapomniałem hasła*)



> Hasła _

W dzisiejszym świecie haseł używa każdy człowiek. Ich rola jest jednak często niedoceniana, a używane przez nas sekrety często pozostawiają wiele do życzenia. Ma to bezpośredni wpływ na nasze bezpieczeństwo w świecie wirtualnym, ale nie tylko. Utrata hasła bądź jego wykradnięcie może nieść za sobą poważne konsekwencje dla każdego. Wiele się mówi o tym, że hasła używane w różnych serwisach powinny być unikalne. Jednak na przestrzeni lat specjaliści rekomendowali metody tworzenia haseł i zarządzania nimi, które przestały być aktualne. Poniżej prezentujemy zbiór materiałów, kierowany do wielu grup odbiorców. Ich celem jest poprawa ogólnej świadomości i usystematyzowane przedstawienie współczesnych zaleceń dotyczących zarządzania hasłami.

Baza Wiedzy



Materiały



Listing 1. 50 najpopularniejszych haseł w analizowanym zbiorze

1. 123456	18. 1qaz2wsx	35. zxcvbnm
2. qwerty	19. 1234567	36. kasia
3. 12345	20. qwerty123	37. 1q2w3e4r
4. 123456789	21. qwerty1	38. kochanie
5. zaq12wsx	22. 123123	39. lol123
6. 1234	23. 0	40. kasia1
7. 12345678	24. bartek	41. natalia
8. polska	25. damian	42. myszka
9. 111111	26. michal	43. 11111
10. misiek	27. qwe123	44. 1qazxsw2
11. monika	28. polska1	45. lukasz
12. 123	29. password	46. mateusz1
13. marcin	30. karolina	47. komputer
14. mateusz	31. kacper	48. 666666
15. agnieszka	32. maciek	49. qazwsx
16. 123qwe	33. samsung	50. piotrek
17. 1234567890	34. qwertyuiop	

UWAGA!

Według naszej najlepszej wiedzy nie istnieje aktualnie publicznie dostępne narzędzie oraz metoda pozwalająca na skuteczny atak na hasła zbudowane zgodnie z przedstawionymi wcześniej rekomendacjami. Teoretyczny, optymalnie przeprowadzony atak na przykładowe hasło *WlazlKostekNaMostekIStuka*, zabezpieczone przestarzałym algorytmem `SHA1` **zająłby co najmniej setki lat**. Oczywiście od momentu publikacji go w tym artykule, jego wartość jako sekretu jest znikoma.



Galwaniczny123\$
zaq1@WSXcde3\$RFV
admin.1admin.1admin.1admin.1



WlazlKostekNaMostekIStuka
zielonyParkingDla3malychSamolotow
DwaBialeLatajaceSophisticatedKroliki

DOWODY OSOBISTE !

Nie każdy może prosić Cię o dowód osobisty !

Zapamiętaj kilka prostych zasad:

- **sprawdzenie tożsamości ≠ legitymowanie**
- **nie pozwalaj skanować dowodu osobistego byle komu**
- dowód jest potrzebny w urzędach, instytucjach, bankach, płatnościach elektronicznych, zawieraniu umów
- nie wysyłaj skanu DO mailem
- jeżeli masz wątpliwości zeskanuj dowód z jakąś odręczną adnotacją „na potrzeby umowy najmu”



KARTY PŁATNICZE !

Jak stracić 300 zł w 5 minut?

- eksperyment społeczny
- system banku wykrył 60 prób wyłudzenia pieniędzy
- po 13 minutach #mbank wydał ostrzeżenie
- po kolejnych 6 minutach telefon z #mbank - zablokował kartę
- 24 h ban na Facebook za post niezgodny z zasadami !
- 300 zł straty

źródło: <https://www.mediafun.pl/moja-karta-trafila-do-sieci-okradzono-mnie-w-5-minut/>



FAŁSZYWE SKLEPY ONLINE!

Jak kupować bezpiecznie ?

- **WERYFIKACJA:** czy na stronie jest telefon do sklepu, NIP, adres, KRS?
- **PŁATNOŚCI:** Czy oferują popularne metody płatności? Czy oferuje możliwość płatności przy odbiorze?
- **OPINIE:** Czy w ogóle są opinie w Internecie? Czy nie ma skrajnych opinii?
- **SOCIAL MEDIA:** czy sklep ma fanpage? Opinie na FB?
- **PODEJRZANE OKAZJE:** uważaj na „wyjątkowe okazje”
- **SPRAWDŹ:** www.legalniewsieci.pl

UWAGA NA PHISHING !!

Maile łudzaco podobne do tych wysyłanych przez pocztę, firmy kurierskie i telekomunikacyjne.

Zwracaj uwagę na wiadomości:

- **czytaj uważnie** treść e-maila, przyjrzyj się formie, porównaj ją z innymi e-mailami od tego samego nadawcy
- **zachowaj czujność** w przypadku wiadomości związanych z kwestiami finansowymi
- **sprawdź, dokąd prowadzi link (nie klikaj)** – jeśli odsyła do formularza, w którym trzeba podać ważne dane - uważaj
- uważaj na e-maile, w których nadawca **straszy Cię konsekwencjami** lub zbyt wiele obiecuje
- **nie otwieraj załączników**, które budzą Twoją wątpliwość



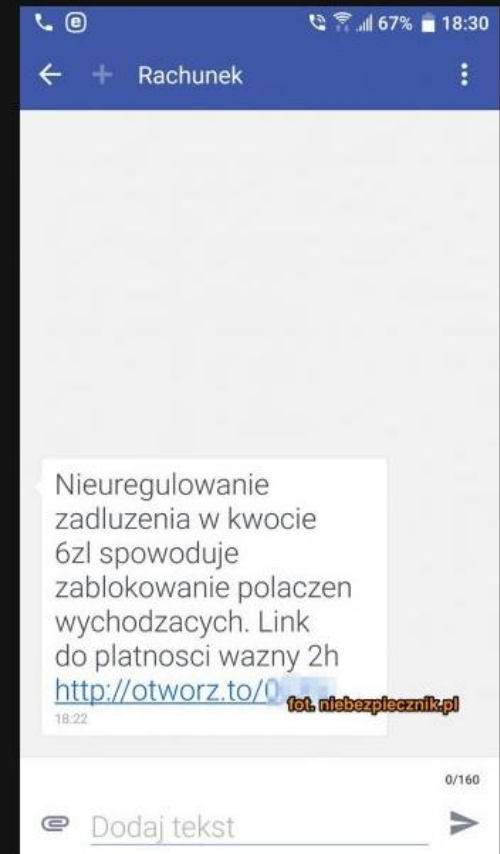
UWAGA NA PHISHING !!

- adresat: RACHUNEK
- link przekierowuje do DotPay / PayU
- fałszywe strony banków
- proszą o podanie wszystkich cyfr/ liter hasła



Na czym polega atak?

Ofiara (a jest ich sporo) na telefon dostaje taką wiadomość:



Netflix

Ostatnio wykryliśmy problem z informacjami rozliczeniowymi powiązanimi z Twoim Kontem.

Witaj!

Nie mogliśmy autoryzować Twojej płatności za kolejny cykl rozliczeniowy Twojej subskrypcji, dlatego zawiesiliśmy Twoje członkostwo. Jednak Twoja obecna subskrypcja jest aktywna do momentu jej wygaśnięcia.

Część informacji na Twoim koncie może być brakująca lub nieprawidłowa.

Oczywiście bardzo byśmy chcieli, abyś wrócił, po prostu kliknij przycisk poniżej, aby zaktualizować swoje dane i nadal cieszyć się wszystkimi najlepszymi programami telewizyjnymi i filmami bez przerwy.

Zaloguj się, aby zacząć

* Link wygasa po 15 minutach.

Zabezpiecz konto: Jeśli nie wiesz, kto przesłał prośbę, najlepiej bezzwłocznie wyloguj się ze wszystkich urządzeń, których nie rozpoznajesz. Możesz także zmienić hasło.

Chętnie odpowiemy na Twoje pytania. Odwiedź [Centrum pomocy](#), aby uzyskać więcej informacji.

Zesłał Netflix

Plus i Play – oszustwo mailowe

Hakerzy w wiadomościach mailowych informują o rzekomym złożeniu wniosku o **kartę eSIM**. Wiadomości przychodzą z bardzo podejrzanych adresów mailowych ctjunkmehnatises@amadeusqatar.com oraz greffinn@isell.com.au. W nich czytamy:

“Drogi Kliencie,

Dziękujemy za przeniesienie Sima do eSIM, jeśli nie pytałeś o to przeniesienie, kliknij poniższy link, aby anulować zamówienie.

Bank Pekao wydał ostrzeżenie. Dotyczy wszystkich klientów

Bank Pekao wydał ostrzeżenie. Dotyczy wszystkich klientów



Źródło zdjęć: © Getty Images | SOPA Images

Oskar Ziomek
06.03.2024 13:27

Zapisz Udostępnij

Oszustwo z Allegro w tle

Akcja phishingowa na szeroką skalę – od tego zaczniemy. Phishing to wyludzanie poufnych danych, podszywając się pod jakąś firmę lub instytucję.

Allegro – autoryzacja danych

W ostatnim czasie oszuści zaczęli masowo wysyłać e-maile, jako Allegro lub Allegro Lokalnie. W wiadomościach pojawia się ostrzeżenie, że nasze konto może zostać zablokowane. Rzekomy powód? Zbyt duża ilość logowań do aplikacji mobilnej wymaga autoryzacji danych użytkownika. Oczywiście wszystkie te informacje trafiają do złodziei.

Allegro – fałszywe reklamy w mediach społecznościowych

Jeśli widziałeś ostatnio reklamę zamieszczoną przez profil Allegro_Group, namawiającą do rejestracji i inwestowania w spółkę – nie klikaj w nią. Linkuje ona do niebezpiecznych stron. Ich zadaniem jest kradzież danych, które wpiszesz w formularzu.

Porada: Zwracaj uwagę na adres e-mail, z którego przychodzi do Ciebie wiadomość. Jeśli ma w sobie literówki lub wygląda nietypowo, oznacz go jako spam.

CyberDefence 24 ARMIA I SŁUŻBY POLITYKA I PRAWO CYBERBEZPIECZEŃSTWO STREFA SAMSUNG

Kolejna akcja phishingowa. Celem użytkownicy poczty Onet

24 CYBERDEFENCE24
09.02.2023 08:19

DRUKUJ PDF f t in @



Fot. mohamed_hassan / Pixabay

Internauci w Polsce muszą uważać na kolejne kampanie uderzające w nasze bezpieczeństwo w sieci. Tym razem szczególną ostrożność muszą zachować użytkownicy Allegro, poczty Onet oraz klienci mBanku.

AKADEMIA
PRZEDSIĘBIORCZOŚCI
www.fundacja.revas.pl

Zwracaj uwagę gdzie udostępniasz informacje !



Discord



LinkedIn

Google



facebook

TO NIE EWIDENCJA LUDNOŚCI !

ZAPYTAJ UCZNIÓW ...

„CO WIE O TOBIE TWÓJ



“???”

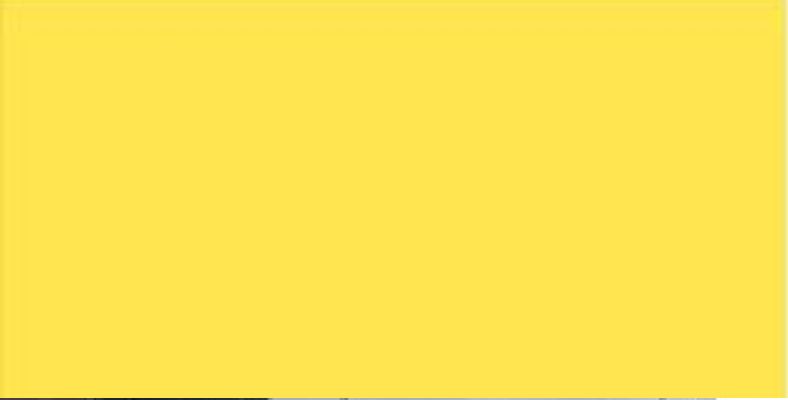
- jak się nazywasz?
- gdzie mieszkasz? gdzie jesteś?
- gdzie pracujesz? gdzie się uczysz?
- gdzie robisz zakupy? co kupujesz?
- co lubisz? czego szukasz w Internecie?
- z kim spędzasz czas?
- co robisz w wolnym czasie?
- na co chorujesz?
- jakie masz problemy?
- w jakim banku masz konto ?
- Twój wizerunek / odcisk palca ?



Pamiętaj, że WIZERUNEK – to też dane osobowe !

- ustawa prawo autorskie i prawa pokrewne
- Kodeks Cywilny
- RODO





- Kodeks Cywilny

Art. 23. [Dobra osobiste człowieka]

Dobra osobiste człowieka, jak w szczególności **zdrowie**, **wolność**, **cześć**, **swoboda sumienia**, **nazwisko lub pseudonim**, **wizerunek**, **tajemnica korespondencji**, nietykalność mieszkania, twórczość naukowa, artystyczna, wynalazcza i racjonalizatorska, **pozostają pod ochroną prawa cywilnego niezależnie od ochrony przewidzianej w innych przepisach.**

dobro chronione: prawo do decydowania o sobie



Uwaga oszust. Podaj dalej

22:37

725 436 658

! Podejrzenie spamu X
Pomóż w zwalczaniu spamu przez zgłoszenie tej wiadomości

To nie jest spam Zgłoś spam

1 udostępnienie

Lubię to! Komentarz Udostępnij

Szukaj

Radek Gac
18 min. ·

**!! UWAGA OSZUST !! GOŚĆ
SPRZEDAJE NARZĘDZIA NIE WYSYŁA,
KUPIŁEM SZLIFIERKĘ MAKITA
ZAPŁACIŁEM NIE WYSŁAŁ**

Foroya Tele 44% 21:40 Foroya Tele 44% 21:41

Profil handlowy Profil handlowy

Roman Zawadzki
Obserwuj

Ogłoszenia Roman Udostępnij

 mocna pilarka stihl 270 nowa ... 300 zł	 Szlifierka kątowa Makita ... 300 zł		
 mocna pilarka stihl 270 nowa	 Szlifierka kątowa Makita	 Nowe baterie	 NOWA PIŁA

3 2 udostępnienia

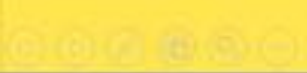
Lubię to! Komentarz Udostępnij

Kiedy potrzebna jest zgoda na zrobienie zdjęcia?

- chcesz **uszanować prywatność** innych
- robisz zdjęcia **w celach zawodowych/ zarobkowych**
- chcesz **udostępniać** zdjęcia
- udostępniasz **zdjęcia dzieci** – zgoda opiekuna

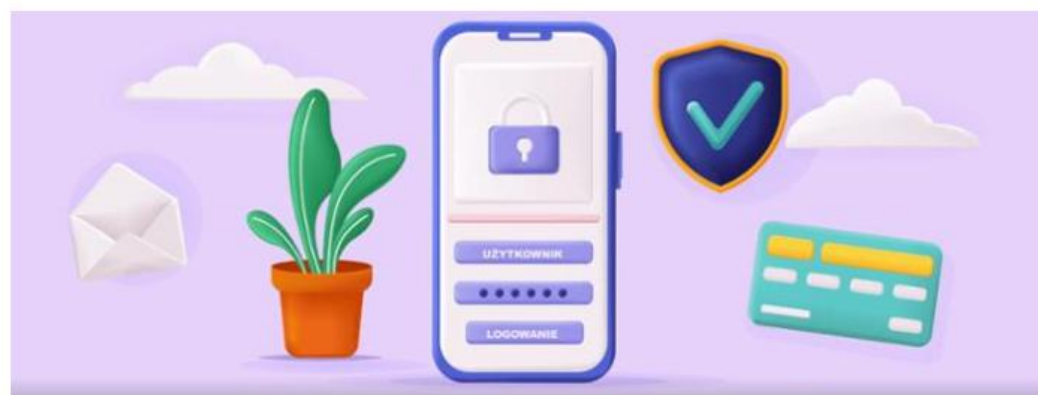


Gdzie szukać informacji?



Nie zagub dziecka w sieci

[Konkurs](#) [Porady dla rodziców](#) [Reaguj! - ważne adresy](#) [Do poczytania](#) [Do obejrzenia](#) [Aktualności](#)



Fundacja Europejskie Rodzicielstwo KPRM NASK Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Aktualności

[zobacz wszystkie](#)

30.06.2022

[Jak tworzyć bezpieczne hasła?](#)



Fundacja Europejskie Rodzicielstwo KPRM NASK Unia Europejska Europejski Fundusz Rozwoju Regionalnego

15.12.2021

[Cyfrowe prezenty - pomysły o bezpieczeństwie](#)



Fundacja Europejskie Rodzicielstwo KPRM NASK Unia Europejska Europejski Fundusz Rozwoju Regionalnego

09.12.2021

[Co każdy rodzic powinien mieć w smartfonie?](#)



Fundacja Europejskie Rodzicielstwo KPRM NASK Unia Europejska Europejski Fundusz Rozwoju Regionalnego

01.12.2021

[Aplikacja mOchrona – stworzona dla rodziców z myślą o dzieciach](#)

<https://cyberprofilaktyka.pl/>



wyszukaj w serwisie...



a a a



O NAS AKTUALNOŚCI BLOG NASZE SZKOLENIA PROJEKTY BIBLIOTEKA KONTAKT

Nowe
**SCENARIUSZE
ZAJĘĆ**
dla klas 1 – 3
oraz 4 – 6

NASK cyberprofilaktyka NASK Ministerstwo Cyfryzacji

PORADNIKI
DLA RODZICÓW I NAUCZYCIELI

NARZĘDZIOWNIK
DLA RODZICÓW

DLA NAUCZYCIELI

SAFER INTERNET
.pl

DYŻURNET
ZGŁOŚ NIELEGALNE TREŚCI



AKTUALNOŚCI

> Nowe scenariusze Cyberlekcji dla klas 1 – 3 oraz 4 – 6

Cyberlekcje 3.0: "Dezinformacja - zagrożenie XXI wieku". Zapraszamy na webinar uczniów klas IV–VI!

> Cyberlekcje 3.0 – zapraszamy na kolejne webinary dla uczniów

Bezpłatne szkolenie dla Wychowawców z placówek wsparcia dziennego, wychowawczych i opiekuńczych oraz z instytucji pieczy zastępczej - Poznań, 10 kwietnia

**AKADEMIA
PRZEDSIĘBIORCZOŚCI**

www.fundacja.revas.pl

<https://uodo.gov.pl/pl>



Wpisz frazę której szukasz



Infolinia Urzędu 606-950-000

Aktualności

O nas

Co robimy

Prawo



29.05.2025

Ochrona danych to nasza
wspólna sprawa – finał XV
edycji programu „Twoje dane –
Twoja sprawa ”

[Czytaj dalej →](#)



AKTUALNOŚCI

[Wszystkie aktualności →](#)



UODO na konferencji
„Cyberhigiena
i cyberochrona
w administracji, biznesie
i oświacie”



Bezpieczeństwo danych
w erze kwantowej –
konferencja
26.05.2025



Człowiek jako filar
bezpieczeństwa –
podsumowanie konferencji
ZUS i UODO
28.05.2025

AKADEMIA
PRZEDSIĘBIORCZOŚCI

www.fundacja.revas.pl

Niebezpiecznik

o bezpieczeństwie i nie...

szukaj...

SZKOLENIA | 5 PORAD | AUDYTY & PENTESTY | SKLEP | KONTAKT

Zobacz niebezpiecznikowy wykład z TEDx

Autor: Piotr Konieczny | Tagi: banki, chargeback, hasła, karty, konferencje i wykłady, Niebezpiecznik, Piotr Konieczny, TEDx, wycieki

Mój wykład z TEDx jest już na YouTube i możecie go zobaczyć [klikając tutaj](#), lub poniżej:



Większość z nas, niestety, zazwyczaj boi się nie tego, czego powinna się obawiać

Zamów nasz wykład dla twojej firmy!



Posłuchaj jednego z naszych 8 cyberwykładów. Wiedzę podajemy z humorem i w przystępny dla każdego pracownika sposób. Zdalnie lub u Ciebie w firmie. Kliknij tu i zobacz opisy wykładów!

Artykuły na e-mail

Aby otrzymać info o nowych postach emailen, wpisz go poniżej:

Rozwiąż Captcha:



Kontakt Logowanie [Załącz konto](#)

Klienci indywidualni Firmy Korporacje i finanse Banki i SKOK-i Administracja publiczna Analizy rynkowe

Alerty BIK się sprawdzają!

- Dostaniesz SMS, gdy ktoś złoży wniosek o kredyt o Twoje dane
- Masz szansę zapobiec wyłudzeniu
- Możesz liczyć na wsparcie doradcy BIK

[Więcej o Alertach BIK](#)



RAPORT BIK

Sprawdzisz swoją historię kredytową

PAKIET BIK

Kontrolujesz swoje kredyty

OFERTA RODZINNA

Chronisz przed wyłudzeniami siebie i swoich bliskich



Bezpieczny Sklep

Sprawdź sklep internetowy, czy jest bezpieczny

podaj link lub nazwę sklepu

[SPRAWDŹ](#)



Sklepy z certyfikatem

Sprawdzone sklepy ze znakiem Bezpieczny Sklep

[Przeglądaj sklepy](#)

[Dołącz do programu](#)

Zgłoszenia do CSIRT NASK

Informujemy, że od dnia 28 sierpnia 2018 r. zespołowi CERT Polska zostały powierzone obowiązki **CSIRT NASK** wynikające z ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560).

Jeżeli chcą Państwo zgłosić osobę kontaktową do CSIRT NASK proszę użyć poniższego odnośnika:

[Zgłaszanie osoby kontaktowej do CSIRT NASK.](#)

Jeżeli chcą Państwo zgłosić złośliwą domenę, proszę użyć poniższego odnośnika:

[Zgłaszanie domeny internetowej służącej do wyludzeń danych i środków finansowych.](#)

www.incident.cert.pl


www.cert.pl


Zgłaszanie podejrzanych wiadomości SMS


Wszystkie podejrzane wiadomości SMS z linkami można zgłosić używając funkcji "Przełącz", bezpośrednio na numer:


8080

Zgłoszenie incydentu – Jaki podmiot Państwo reprezentują?

 Osoba fizyczna / inne podmioty

 Operator usług kluczowych

 Dostawca usługi cyfrowej

 Podmiot publiczny

Wcześniejsze webinaria można zobaczyć
na stronie Fundacji Przedsiębiorczości Revas:
<https://www.fundacja.revas.pl/>



Dziękuję za uwagę!

REVAS

BRANŻOWE SYMULACJE BIZNESOWE



**NARODOWY
BANK POLSKI**

Projekt realizowany
z Narodowym Bankiem Polskim
w ramach programu edukacji ekonomicznej

FUNDACJA
przedsiębiorczości
REVAS
AKADEMIA
PRZEDSIĘBIORCZOŚCI
www.fundacja.revas.pl