

Zagrożenia dla ochrony danych osobowych w sieci

o czym warto pamiętać
i jak chronić swoją prywatność

Na dobry początek

Dane osobowe to każda informacja o konkretnej osobie (np. uczniu czy nauczycielu).

Nie mamy do czynienia z danymi osobowymi w przypadku, gdy informacja dotyczy instytucji (np. firmy), grupy osób, osoby fikcyjnej (np. postaci literackiej) czy takiej, której nie jesteśmy w stanie w żaden sposób rozpoznać.

Do danych osobowych zaliczamy zazwyczaj:

imię i nazwisko, adres zamieszkania, numer telefonu, datę urodzenia, adres e-mail, numer PESEL.

Danymi osobowymi mogą być jednak także między innymi: zdjęcia, oceny uczennic i uczniów czy wyniki badań.

Na dobry początek

Wiele stron internetowych zachęca do udostępniania informacji o sobie (nie tylko imienia czy nazwiska, ale również zdjęć, filmów, informacji o zainteresowaniach itd.).
Miej świadomość, że publikując takie informacje, dzielisz się nimi **z całym światem**, a to, co trafia do Internetu, pozostaje tam na zawsze. Dlatego warto ostrożnie publikować informacje o sobie i unikać podawania swojego imienia i nazwiska.

Na dobry początek

Niestety, w sieci zostawiamy wiele śladów również nie do końca świadomie.

Na podstawie tego, czego szukamy, z jakich stron WWW korzystamy, co pobieramy lub co udostępniamy, **jest tworzony nasz profil.**

Służy on do tego, by na ekranie Twojego monitora pojawiały się reklamy, które według danej firmy mogą Cię zainteresować.

Pamiętaj, że w sieci można Cię zidentyfikować, nawet jeśli nie podasz swojego imienia i nazwiska.

Na dobry początek

Każdy nasz ruch jaki wykonujemy w sieci jest widoczny i pozostawia po sobie trwały ślad umożliwiający naszą identyfikację. Wszystkie komputery (niezależnie od ich rodzaju), posiadają swój unikalny numer nazywany „numerem IP”. I to właśnie za pomocą numeru IP wszyscy użytkownicy Internetu są identyfikowani w sieci.

Dlatego właśnie, wbrew temu, co czasem nam się wydaje, w Internecie nie jesteśmy zupełnie bezkarni. Za to, co wypisujemy na forach lub portalach społecznościowych, możemy zostać pociągnięci do odpowiedzialności.

Dlaczego należy chronić swoje dane osobowe?

Należy chronić swoje dane osobowe w Internecie z kilku powodów.

Po pierwsze — ktoś może wykorzystać w złych zamiarach (choćby w celu ośmieszenia Cię) to, co znajdzie w sieci na Twój temat. Wyobraź sobie na przykład, że udostępniasz zdjęcie, ono zostaje pobrane, a następnie zamieszczone wraz ze złośliwym komentarzem w serwisie Wiocha.pl lub podobnym.

Po drugie — wiele firm pragnie zdobyć informacje o Tobie, ponieważ dzięki nim zarabia. Przekazują one te dane innym podmiotom, a Ty przestajesz mieć nad nimi kontrolę.

Po trzecie — nie wiesz, kto i w jaki sposób może wykorzystać informacje na Twój temat w przyszłości. Nawet jeśli teraz nie widzisz w przekazywaniu danych problemu — za jakiś czas możesz zmienić zdanie.

Niebezpieczeństwa

jakie niesie zostawianie w sieci informacji na swój temat, np. podawanie nazwiska, adresu czy udostępnianie zdjęć to:

- Kradzież danych osobowych z systemów zabezpieczonych,
- Wykorzystanie powierzonych danych przez osoby nieupoważnione,
- Tzw. phishing, czyli podszywanie się pod system uważany za bezpieczny w celu wyłudzenia danych,
- Podstuchiwanie/podglądanie przez włączoną w urządzeniu kamerę i/lub mikrofon.

Najczęstsze zagrożenia w Internecie – wirusy

Mogą:

- wykraść nasze poufne informacje,
- zniszczyć dane, jakie mamy na dysku,
- za pomocą naszego adresu e-mail wysyłać spam do naszych kontaktów,
- zaszyfrować nasze dane i wymuszać okup za ich odszyfrowanie,
- sprawdzić historię naszego przeglądania i wymuszać okup,
- wysyłać smsy typu premium (bardzo drogie) z naszego telefonu,
- przekazywać informacje o naszym położeniu hakerom

Phishing – wyłudzenie danych

Do Twojej skrzynki pocztowej może trafić e-mail na przykład od banku (a Ty nie masz swojego konta), dostawcy mediów (wszystko zapłacone), kuriera (nie zamawiałaś niczego), obcokrajowca (nie znasz go) czy też od znajomego. Przypomina on o zapłaceniu zaległego rachunku, o przesyłce, może zawierać prośbę o pomoc lub zachęca do obejrzenia zdjęć. Zawiera także zazwyczaj link lub załącznik oraz prośbę o kliknięcie lub otwarcie załącznika.

Po kliknięciu w proponowany link otwiera się strona, która często jest łudząco podobna do prawdziwej strony, za którą się podaje (na przykład jakiś sklep), lub nawet identyczna z nią. W istocie okazuje się jednak, że jest to inna strona, przygotowana przez przestępców.

Wiele osób, kiedy widzi znajomo wyglądającą stronę, wprowadza na niej swoje prawdziwe dane (login, hasło) i w ten sposób przekazuje je przestępcom.

Kliknięcie w załączony link zwykle kończy się zainstalowaniem szkodliwego oprogramowania.

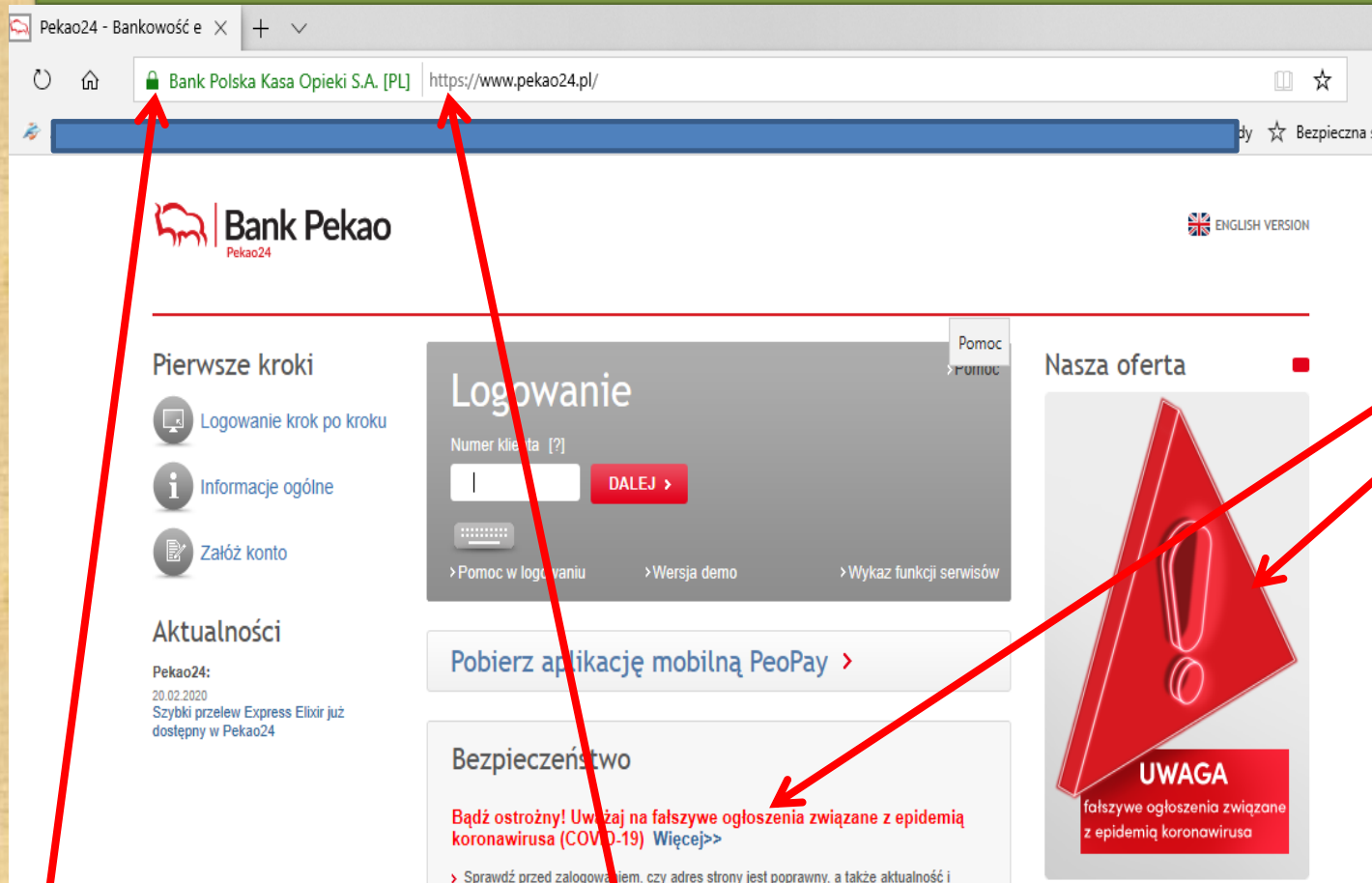
Phishing – jak postępować, aby uniknąć przykrych skutków

- Zachowaj spokój i nie ulegaj manipulacji,
- Uważnie analizuj otrzymywane wiadomości (sprawdź adres nadawcy),
- Nie otwieraj **odruchowo** łączy przesyłanych pocztą lub komunikatorami – najpierw sprawdź, kto i po co ci je wysyła,
- Powstrzymaj się przed otwieraniem załączników, zanim zostaną sprawdzone przez program antywirusowy,
- Nie otwieraj na swoim komputerze przypadkowych nośników pamięci (pendrive'a, płyty, karty pamięci),
- Nie udostępniaj swoich prywatnych danych logowania (np. loginu, hasła, kodu PIN) innym osobom,

Phishing – jak postępować, aby uniknąć przykrych skutków

- Nie instaluj żadnych aplikacji, rozszerzeń ani kodeków proponowanych przez strony lub usługi, do których nie masz pełnego zaufania.
- Nigdy nie wprowadzaj żadnych danych (np. e-maila, loginu, hasła, PINu czy kodu z tokena), jeśli strona nie potwierdza swojej autentyczności ważnym certyfikatem (adres strony zaczyna się od https i widać obok niego zamkniętą, zieloną kłódkę).
- Unikaj logowania się do swoich usług i podawania jakichkolwiek prywatnych danych w publicznych sieciach Wi-Fi, jeśli nie masz włączonej usługi VPN (Virtual Private Network).
- Upewnij się, że smartfon, tablet i komputer są zabezpieczone trudnym do odgadnięcia hasłem lub kombinacją gestów, nie zostawiaj odblokowanego urządzenia bez nadzoru.

Strona prawdziwa, zobacz:



Zielona kłódka, zamknięta

https: przed adresem

Często możesz zobaczyć takie ostrzeżenia

Strony „phishingowe” – zobacz:

Od: **Pekao_S.A** <colinmdu78@pb01.wixshoutout.com>
Date: śr., 22 maj 2019 o 05:51
Subject: Your online access has been blocked
To: **niebezpiecznik.pl**

Vous ne voyez pas ce message ? [Ouvrir dans un navigateur](#)

Dear customer,

Your access is blocked, You are requested to update the Mobile Security application to restore access to your account by clicking below :

<https://www.pekao.com.pl/login/en/r0ei0/index.jsp>

P.S : The link in this message will expire withing 24 hours

Pekao S.A



Bank Pekao

Your account has been blocked kindly click to update

Partager via :



<https://www.pekao.com.pl/login/en/r> →

Si vous pensez avoir reçu cet email par erreur ou si vous souhaitez vous désabonner, [cliquez ici](#)

Adres nadawcy nie ma nic wspólnego z Pekao S.A.

Link, który przekierowuje na stronę przestępcy

Strony „phishingowe” – zobacz:

Od: Allegro <powiadomienia@telus.net> użyj adresu... Czwartek, 29 Marca 2018 19:47

Temat: Musisz potwierdzić swoje Allegro konto

Aby otrzymywać darmowe Powiadomienia SMS o nadejściu wiadomości e-mail od Allegro [kliknij tutaj](#) | [pokaż więcej informacji](#)

[pokaż wersję tekstową wiadomości](#)

 Nadawca listu nie umieść "cięż" informacji o kodowaniu listu. Jedź "li masz problemy z wydź "wietleniem tredź "ci, wyprdź "buj najpopularniejszych kodowadź":
[UTF-8](#) [ISO-8859-2](#) [windows-1250](#)

allegro

Witaj !

Musisz potwierdzić swoje Allegro konto.

Zauwazylismy, ze Twoje konto zostalo dostep z kilku adresow IP.
Zawieszenie konta allegro , Jak mozna je odblokowac, ile to trwa i ze jestes wlascicielem tego konta na :

[Potwierdź swoje konto](#)

Pozdrawiamy,
Zespół Allegro
[Kontakt z Działem Współpracy z Klientem](#)

Grupa Allegro Sp. z o.o. z siedziba w Poznaniu, 60-166 Poznan, przy ul. Grunwaldzkiej 182, wpisana do rejestru przedsiębiorcow prowadzonego przez Sad Rejonowy Poznan - Nowe Miasto i Wilda w Poznaniu, Wydział VIII Gospodarczy Krajowego Rejestru Sadowego pod numerem KRS [0000268796](#), o kapitale zakladowym w wysokosci [33 916 500](#) zł, posiadajaca numer identyfikacji podatkowej NIP: [527-25-25-995](#)

Wiadomości od tego serwisu zawsze zawierają imię i nazwisko kupującego. Nie ma tego. Należy zachować ostrożność.

Zobacz, jakim językiem napisany jest tekst. Już to powinno wzbudzić Twoją czujność. Opuszczasz takie strony.

Strony „phishingowe” – zobacz:

Brak logo Poczty Polskiej, ale wygląda podobnie

Poczta Polska

redakcja@pablik.pl,

Co to za adres? Gdzie Poczta Polska

Kurier nie dostarczył przesyłkę do numeru zgłoszenia **RR4835593349PL** na adres **6.09.2015**, ponieważ nikt w tym czasie. Proszę [zobaczyć informacje](#) na temat wysyłki, drukowania i iść na pocztę, aby otrzymać pakiet.

Zobacz informacje

Uwaga

 <http://support.tealiateam.com/system/faq/faq16jwKBZs.php?id=>

Nie ma kłódki przed adresem. To jest właśnie ten niebezpieczny link. Nie ma https:

Jeżeli przesyłka nie dotrze w ciągu 7 dni roboczych Poczta Polska będzie miała prawo do ubiegania się koszty utrzymania przesyłki 50 zł za jeden dzień. Dziękujemy za korzystanie z naszych usług dostawy. Życząc miłego dnia Twoja Poczta Polska.

To jest generowany automatycznie e-mail, kliknij jeżeli chcesz się [wypisać](#)

Tekst napisany dziwnym językiem. Przeczytaj, widzisz? Opuszczasz takie strony.

Inne zagrożenia

- możliwość kontaktu z nieznanymi osobami, które mogą okazać się niebezpieczne,
- przemoc rówieśnicza i dręczenie za pomocą m.in. mediów społecznościowych, które mogą doprowadzić nawet do samobójstwa,
- Wykradanie lub przejmowanie i upublicznianie zdjęć czy filmów,
- kradzież pieniędzy, kradzież tożsamości.

Hejt i fake news

Zapamiętaj!

- Nie pozwól się straszyć i ośmieszać. Nie jesteś sam.
- Gdy coś cię zaniepokoi, powiedz o tym rodzicom lub wychowawcy.
- W sytuacji zagrożenia w Internecie możesz skorzystać z pomocy oferowanej pod numerem telefonu: 116 111.

Cyberprzemoc

- Przykrym zjawiskiem, z jakim możesz spotkać się podczas użytkowania komunikatora jest cyberprzemoc, czyli zagrożenie polegające na wyrządzaniu krzywdy przez ludzi złośliwych i ordynarnych. Do takich działań zalicza się m.in. wyzywanie, straszenie, czy poniżanie kogoś w Internecie. Może to odbywać się na przykład poprzez robienie komuś zdjęć bez jego zgody, a następnie publikowanie ich i rozsyłanie w sieci. Umieszczone w sieci zdjęcie, przedstawiające wydarzenie niemiłe dla osoby na nim uwiecznionej, opatrzone złośliwymi komentarzami, rodzi w niej poczucie upokorzenia i bezradności.
- Osobę stosującą cyberprzemoc określa się mianem stalkera.

Złośliwe oprogramowanie

- Jeżeli strona WWW wymaga instalacji oprogramowania (ściągnięcia i zapisania programu na komputerze, laptopie, itp.), czy podania jakichkolwiek danych osobowych, zanim się zarejestrujesz, skonsultuj się najpierw z dorosłym.

Ochrona danych osobowych

Warunki wyrażenia zgody przez dziecko w przypadku usług społeczeństwa informacyjnego określa art. 8 RODO.

Mówi on, że zgodne z prawem jest przetwarzanie danych osobowych dziecka, które ukończyło 16 lat.

Oznacza to, że osoba, która ma 16 lat, może samodzielnie wyrazić zgodę bez potrzeby jej potwierdzenia przez rodziców czy opiekunów prawnych.

Natomiast jeżeli dziecko nie ukończyło 16 lat, przetwarzanie jego danych osobowych jest możliwe dopiero, gdy zgodę wyrazi lub zaaprobuje ją osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem oraz wyłącznie w zakresie wyrażonej zgody.

Przykład: Piętnastolatek kupi samodzielnie książkę w Internecie, ale nie będzie mógł się zgodzić na otrzymywanie informacji o nowościach wydawniczych. Do tego konieczna będzie już akceptacja rodzica.

Usługa społeczeństwa informacyjnego co to takiego?

- Zgodnie z Dyrektywą 2015/1535

usługą społeczeństwa informacyjnego jest każda płatna usługa świadczona drogą elektroniczną, która została indywidualnie zamówiona przez odbiorcę.

Są to więc takie działania jak np. słuchanie muzyki za pośrednictwem aplikacji takich jak Spotify czy też założenie konta na Netflix.

Ważne jest, aby zauważyć, iż do kategorii tej nie można przypisać usług mających charakter materialny.

W związku z czym zakup płyty z dostawą do domu nie będzie objęty ową definicją. Możesz ją kupić.

Jeszcze o wyrażeniu zgody

Wyrażenie zgody przez rodzica lub opiekuna
prawnego **nie jest potrzebne**

w przypadku usług profilaktycznych czy też
doradczych oferowanych bezpośrednio dzieciom,
np. jeśli chcesz skorzystać z pomocy online działającej
na zasadach tzw. telefonu zaufania dla dzieci:

<https://116111.pl>

<https://fdds.pl>

Jak się bronić przed zagrożeniami dla naszych danych osobowych

- Regularnie aktualizujemy oprogramowanie i system operacyjny.
- Nigdy nie otwieramy e-maili nieznanego pochodzenia, nawet jeśli nadawca ma zbliżony adres np. do naszego banku.
- Prawdziwe serwisy zwykle nie proszą za pomocą e-maili o ponowne zalogowanie się. Nie klikamy w takie linki.
- Nigdy nie klikamy w linki, co do których nie mamy pewności.
- Do każdego serwisu, społecznościowego, bankowego, ale i takiego z grami (szczególnie jeśli wpłacamy tam jakiegokolwiek pieniądze) mamy inne hasło – nie brzmiące „12345678”!
- Nigdy nikomu nie podajemy swoich haseł i loginów, nie przesyłamy ich przez Internet.
- Zawsze przed wpisaniem hasła i loginu do strony sprawdzamy w oknie, czy adres strony się zgadza.

Jak się bronić przed zagrożeniami

- Nie podajemy w sieci swoich danych – imienia, nazwiska, wieku, adresu zamieszkania itp.
- Chronimy swoje zdjęcia – nie umieszczamy ich w Internecie zbyt dużo. Te, które wrzucamy, zabezpieczamy (większość serwisów społecznościowych posiada możliwość ograniczania dostępu do udostępnianych treści osobom nieznanym).
- Instalujemy program antywirusowy i pilnujemy, aby zawsze był aktualny.
- Nie korzystamy z hot-spotów niewiadomego pochodzenia.

Jak się bronić przed zagrożeniami

Zanim zaufasz osobie poznanej w sieci, zastanów się, skąd masz pewność, że jest ona naprawdę kimś za kogo się podaje!



Nie podawaj w sieci swoich danych – imienia, nazwiska, wieku, adresu zamieszkania itp.

Pamiętaj: Twoje dane – to Twoja sprawa.

Spędzasz teraz zapewne więcej czasu w Internecie, dlatego zachowaj w pamięci te porady, o których dziś mówimy i stosuj je w praktyce.

Wychowawca klasy wraz z inspektorem ochrony danych osobowych