# KONSUMENT 60+ W SIECI

## PORADNIK DLA SENIORÓW

**Autorzy:**

r. pr. Paulina Cichowska
r. pr. Magdalena Dębska-Szymczak

**Skład i opracowanie graficzne:**

Katarzyna Winkler

**Wydawca:**

Fundacja LexCultura
ul. Fiołkowa 18/2
53-239 Wrocław
tel. 730336909

fundacja@lexcultura.pl
www.lexcultura.pl
@LexCultura
fundacja_lexcultura

**ISBN 978-83-965751-3-5**



*Poradnik powstał w ramach zadania publicznego pt. „Seniorze, skręć w pr@wo! Kierunek: bezpieczny Internet.” współfinansowanego ze środków Ministerstwa Rodziny i Polityki Społecznej w ramach rządowego programu wieloletniego na rzecz Osób Starszych „Aktywni+” na lata 2021–2025, Edycja 2023.*

*Wrocław*
*sierpień 2023*

# PORADNIK DLA SENIORA – ZAGROŻENIA W SIECI

Internet jest doskonałym źródłem informacji. Zapewnia nam wygodne przeglądanie nieskończonej liczby ofert i dokonywanie zakupów za pośrednictwem stron internetowych. Zapewnia rozrywkę i ciekawe opcje wykorzystania czasu wolnego, a tym samym może pomóc zachować sprawność umysłu.. Ponadto daje możliwość kontaktu z rodziną, przyjaciółmi, jak również możliwość zawierania nowych znajomości. Dzięki temu możemy aktywnie uczestniczyć w życiu rodzinnym pomimo odległości i niejednokrotnie braku czasu na spotkania na żywo. Niestety dostęp do Internetu niesie za sobą zagrożenia. Dzięki wprowadzeniu w życie kilku podstawowych zasad bezpieczeństwa oraz racjonalnego korzystania z Internetu możemy ich uniknąć.

Zapraszamy do zapoznania się z naszym poradnikiem dotyczącym bezpieczeństwa w sieci!

# 10 PODSTAWOWYCH ZASAD BEZPIECZEŃSTWA W INTERNECIE:

1. **Stosuj oprogramowania antywirusowe**

- w sieci obok wersji płatnych dostępne są wersje bezpłatne, które są równie skuteczne,
- programy antywirusowe chronią także Twoje dane osobowe,
- programy te chronią dostępu do Twojej bankowości elektronicznej, Twoich kont w sklepach internetowych oraz mediach społecznościowych,
- mogą zostać zainstalowane również na urządzeniach takich jak laptop, tablet, telefon.

2. **Nie zapisuj haseł dostępu w przeglądarkach internetowych**

- hasła te mogą zostać wykradzione przez hakerów,
- skuteczniej będzie jeśli zapiszesz hasło na kartce i położysz ją przy komputerze.

3. **Upewnij się, że Twoje hasło jest bezpieczne**

- nie stosuj prostych i podstawowych konfiguracji hasła,
- postaraj się,aby hasło zawsze składało się z dużej i małej litery, cyfry oraz znaku specjalnego,
- nie podawaj nikomu swoich haseł,
- postaraj się nie stosować tego samego hasła do różnych celów, każde Twoje konto powinno być chronione innym hasłem.

## 4. Uważaj na wiadomości oraz e-maile od nieznanych nadawców

- nie klikaj w linki znajdujące się w wiadomościach,
- nie otwieraj załączników od nieznanych odbiorców,
- nie daj się nabrać na komunikaty żądające zapłaty brakującej kwoty,
- nie daj się zastraszyć egzekucją komorniczą lub działaniami windykatorów,
- nie płać rachunków oraz faktur za usługi oraz produkty, których nie zamawiałeś,
- sprawdzaj nadawców wiadomości email.

W przypadku otrzymania e-maila od nieznanego nadawcy, nie klikaj w żadne linki ani nie pobieraj jego zawartości. Nadawców niebezpiecznych maili poznasz po zagadkowych i niemających sensu adresach e-mail, składających się z kombinacji cyfr i liczb lub po niedopasowanej treści maila zawierającej wiele błędów!

## 5. Zachowaj bezpieczeństwo bankowości elektronicznej

- nie podawaj danych do logowania do bankowości elektronicznej w żadnej innej sytuacji poza przypadkiem, kiedy rzeczywiście logujesz się do swojej bankowości,
- nigdy nie podawaj danych karty płatniczej tj. numeru, danych właściciela karty, daty ważności i numeru CVC/CVV,
- nigdy nie podawaj powyższych danych przez telefon, prawdziwy pracownik banku nie zapyta Cię o nie.

## 6. Zachowaj bezpieczeństwo podczas zakupów online

- zawsze sprawdzaj, czy nie masz do czynienia z oszukańczą stroną internetową,

- przed zakupem czytaj opinie innych konsumentów o sklepie internetowym, w którym chcesz dokonać zakupu,
- przeczytaj w regulaminie sklepu, jak długo będziesz czekał na produkt i skąd jest on dostarczany,
- sprawdź siedzibę sklepu, a jeżeli masz do czynienia ze sklepem zagranicznym, musisz zdawać sobie sprawę, że dochodzenie Twoich praw może być utrudnione,
- zawsze sprawdzaj zasady zwrotu, wymiany oraz kosztów przesyłki.

## 7. Staraj się nie korzystać z ogólnodostępnych, otwartych sieci wi-fi

- zazwyczaj dostęp do otwartych sieci wi-fi znajduje się w miejscach publicznych (np. restauracje, dworzec),
- nigdy nie wykonuj za pośrednictwem takich sieci płatności przez Internet,
- nie loguj się wtedy do swoich kont w sklepach internetowych ani mediach społecznościowych,
- sieci te są najbardziej narażone na ataki hakerów!

## 8. Dokonuj aktualizacji urządzeń, z których korzystasz

- aktualizuj oprogramowanie w laptopie, tablecie i telefonie,
- aktualizacja zabezpiecza nasze urządzenia przed atakami hakerów,
- usprawniają urządzenia i ulepszają ich działanie,

## 9. Zwracaj uwagę na nazwy sklepów internetowych oraz przeglądarek internetowych

- zawsze zwracaj uwagę na to, czy nazwa sklepu, mediów społecznościowych bądź innych przedsiębiorców jest poprawna,

- zerknij, czy logo jest oryginalne,
- często cyberprzestępcy zmieniają literę w nazwie sklepu bądź bankowości elektronicznej w celu wyłudzenia danych osobowych,
- nie klikaj w pojawiające się na ekranie reklamy.

Nie pobieraj zawartości z nieznanych źródeł. Często w zapisywanych plikach czyhać mogą niebezpieczne wirusy. Pobieraj pliki tylko z zaufanych źródeł!

## 10. Bądź ostrożny podczas zawierania znajomości i prowadzenia rozmów z innymi użytkownikami – nigdy nie wiesz, kto znajduje się po drugiej stronie

- nie podawaj swoich danych osobowych: adresu, numeru telefonu, nr PESEL, nr dowodu osobistego,
- nigdy nie przelewaj pieniędzy na rzecz obcych osób, pomimo próśb rozmówcy,
- nie przesyłaj swoich zdjęć, ani zdjęć swojego domu,
- akceptuj prośby o znajomość tylko od osób Tobie znanych,
- najlepiej zmień ustawienia na swoim koncie w taki sposób, by tylko znajomi i osoby nas obserwujące mogli widzieć udostępniane przez Ciebie treści.

# 6 PODSTAWOWYCH ZAGROŻEŃ W SIECI

1. **Nieodpowiednie lub szkodliwe treści**

   treści przemocowe, gorszące, nieobyczajne, seniorzy powinni korzystać z programów antywirusowych i oprogramowania filtrującego treści, aby chronić się przed takimi zagrożeniami,

2. **Cyberprzemoc**

   niektórzy seniorzy mogą stać się ofiarami cyberprzemocy, w tym nękania, obrażania lub wyśmiewania w Internecie. Ważne jest, aby seniorzy czuli się swobodnie i zgłaszali takie incydenty i szukali wsparcia,

3. **Nadużycie danych osobowych**

   starsi ludzie mogą stać się ofiarami kradzieży tożsamości lub nieuprawnionego wykorzystania swoich danych osobowych. Ważne jest, aby być ostrożnym podczas udostępniania danych osobowych online i korzystać z silnych haseł oraz zabezpieczonych sieci Wi-Fi,

4. **Ataki phishingowe, oszustwa finansowe**

   starsze osoby często są celami dla oszustów, którzy próbują wyłudzić pieniądze poprzez fałszywe inwestycje, loterie lub inne schematy. Ważne jest, aby być ostrożnym i nigdy nie udostępniać poufnych informacji finansowych osobom lub witrynom, którym nie można ufać,

5. **Malware i wirusy**

złośliwe oprogramowania, mogą spowodować utratę danych, kradzież tożsamości i szkody finansowe,

6. **Brak prywatności danych**

dane osobowe mogą być obserwowane, zbierane, monitorowane i wykorzystywane w sposób nieodpowiedni, naruszają interesy odbiorców.

# NIEODPOWIEDNIE LUB SZKODLIWE TREŚCI W SIECI


Oto kilka przykładów:

- **Nękanie i hejt**

  Internet daje anonimowość, co może prowadzić do przypadków nękania, hejtu i zastraszania innych ludzi. Może to obejmować obraźliwe komentarze, groźby lub szerzenie plotek.

- **Pornografia dziecięca**

  jest to jedna z najbardziej niebezpiecznych i nielegalnych form treści w Internecie. Szerzenie, przeglądanie lub udostępnianie takiej treści jest przestępstwem i stanowi poważne zagrożenie dla dzieci.

- **Ekstremizm i terroryzm**

  w Internecie można znaleźć treści propagujące ekstremistyczne ideologie, nienawiść, przemoc i terroryzm. Są to nieodpowiednie i niebezpieczne treści, które mogą wpływać na osoby podatne na manipulację.

- **Fałszywe informacje**

  Internet jest pełen dezinformacji i fake newsów. Fałszywe informacje mogą wprowadzać w błąd, dezorientować i prowadzić do szkodliwych decyzji lub działań.

Ważne jest, aby być ostrożnym podczas korzystania z sieci, sprawdzać wiarygodność informacji i zwracać uwagę na to, co udostępniamy lub konsumujemy online.

Oto kilka sposobów, które mogą pomóc Ci unikać szkodliwych treści w Internecie:

- Zawsze wybieraj wiarygodne źródła informacji! Sprawdzaj wiarygodność stron internetowych, artykułów i informacji, zanim uwierzysz w nie lub podzielisz. Szukaj informacji z zaufanych źródeł, takich jak renomowane strony internetowe, instytucje, media lub badania naukowe.
- Używaj filtrów i blokuj treści nieodpowiednie! Włącz odpowiednie filtry w wyszukiwarkach i aplikacjach, które będą blokować treści nieodpowiednie lub niebezpieczne. Możesz również zainstalować oprogramowanie blokujące reklamy i szkodliwe treści.
- Kontroluj ustawienia prywatności i bezpieczeństwa! Zadbaj o swoje prywatne dane i ustawienia bezpieczeństwa w swoich kontach na platformach społecznościowych i innych witrynach. Ustal, kto może widzieć Twoje informacje i treści oraz ogranicz dostęp do nich.
- Bądź świadomy phishingu i oszustw internetowych! Uważaj na podejrzane wiadomości e-mail, linki, komunikaty czy prośby o podanie poufnych informacji. Nie klikaj w podejrzane linki ani nie pobieraj plików z nieznanych źródeł!

Pamiętaj, że samoświadomość, ostrożność i zdrowy rozsądek są kluczowe w unikaniu szkodliwych treści w Internecie. W razie wątpliwości zawsze możesz skonsultować się z zaufanymi osobami lub organami odpowiedzialnymi za bezpieczeństwo online.


## CYBERPRZEMOC

### Co to jest?

Cyberprzemoc to forma agresji i znęcania się nad innymi ludźmi za pomocą nowych technologii, takich jak internet, media społecznościowe, telefony komórkowe itp. Obejmuje ona działania takie jak groźby, zastraszanie, wyśmiewanie, poniżanie czy rozpowszechnianie obraźliwych treści online. Cyberprzemoc może mieć poważne konsekwencje dla ofiar, zarówno emocjonalne, jak i psychologiczne. Jest ważne, aby walczyć z cyberprzemocą i promować bezpieczne, szanujące i odpowiedzialne korzystanie z technologii.

Przykłady cyberprzemocy:

- Wyśmiewanie i obrażanie innych osób w komentarzach internetowych, na portalach społecznościowych lub w wiadomościach prywatnych,
- Rozpowszechnianie obraźliwych treści, zdjęć lub filmów na temat danej osoby bez jej zgody, co może prowadzić do upokorzenia i szkody dla ofiary,
- Tworzenie fałszywych kont lub podszywanie się pod inną osobę w celu zniesławienia lub szkalowania jej reputacji.
- Groźby lub nękanie za pomocą wiadomości e-mail, SMS-ów lub wiadomości prywatnych, które mogą powodować duży stres i lęk u ofiary,
- Wykluczanie i izolowanie danej osoby w środowisku internetowym, na przykład poprzez blokowanie dostępu do grup czy wykluczanie z rozmów,
- Szturmowanie danej osoby negatywnymi komentarzami, hejtami i trollingiem w celu zniszczenia jej wizerunku i samopoczucia,
- Ujawnianie prywatnych informacji lub tajemnic danej osoby w celu szkody moralnej lub emocjonalnej.

Wszystkie te przykłady stanowią różne formy cyberprzemocy, które mogą powodować poważne konsekwencje dla ofiar. Ważne jest, abyśmy byli świadomi i przeciwdziałali takim działaniom, promując kulturę szacunku, empatii i bezpieczeństwa w świecie online.

# JAK PRZECIWDZIAŁAĆ CYBERPRZEMOCY?

1. **Podnoszenie świadomości**

edukujmy siebie i innych na temat cyberprzemocy, jej konsekwencji i wpływu na ofiary. Rozmawiajmy z rodziną, przyjaciółmi i społecznością o tym problemie.

2. **Zachowanie bezpieczeństwa online**

używajmy silnych haseł, nie udostępniajmy swoich danych osobowych publicznie i ostrożnie dobierajmy kontakty online.

3. **Blokowanie i zgłaszanie**

eśli staniemy się świadkami lub ofiarami cyberprzemocy, blokujmy osoby, które ją stosują, i zgłaszajmy incydenty odpowiednim platformom lub władzom.

4. **Mocne relacje społeczne**

wspierajmy i otaczajmy się osobami, które promują szacunek i bezpieczeństwo online. Budowanie silnych relacji społecznych może pomóc w zapobieganiu i łagodzeniu skutków cyberprzemocy.

5. **Szczególna uwaga w przypadku dzieci i młodzieży**

uczmy młodsze osoby, jak rozpoznawać cyberprzemoc i jak na nią reagować. Zachęcajmy do komunikacji z dorosłymi w przypadku napotkania problemów.

6. **Odpowiedzialne korzystanie z mediów społecznościowych**

bądźmy odpowiedzialni w sposobie korzystania z mediów społecznościowych. Unikajmy udziału w hejcie, obrażaniu innych lub rozpowszechnianiu negatywnych treści.

**7. Raportowanie i wsparcie ofiar**

jeśli zauważymy, że ktoś jest ofiarą cyberprzemocy, oferujmy wsparcie i informujmy odpowiednie osoby lub instytucje, które mogą pomóc.

## Czy cyberprzemoc stanowi przestępstwo?

Tak, w Polsce cyberprzemoc może być traktowana jako przestępstwo zgodnie z obowiązującym prawem. Istnieją przepisy, które obejmują różne formy cyberprzemocy i określają je jako przestępstwa.

Przykładowe przestępstwa związane z cyberprzemocą w Polsce to:

- groźby karalne, które wzbudzają w zagrożonym obawę, że będą spełnione - art. 190 Kodeksu Karnego,
- uporczywe nękanie, stalking, czyli uporczywe i niepożądane kontaktowanie się z osobą w sposób zagrażający jej bezpieczeństwu lub powodujący jej strach, wykorzystywanie technologii komunikacyjnych do nieustannego kontaktowania się z inną osobą w celu zasypywania jej wiadomościami lub groźbami - art. 190a Kodeksu Karnego,
- znęcanie się fizyczne lub psychiczne, w szczególności nad osobą starszą, wywołując u niej strach, stres oraz uchybiając jej godności - art. 207 Kodeksu Karnego
- znieważenie poprzez używanie słów powszechnie uznanych za obraźliwe, ujawnianie tajemnic życia prywatnego danej osoby, takich jak prywatne fotografie czy informacje, w celu poniżenia lub obrażenia jej godności - art. 216 Kodeksu Karnego
- oszustwa komputerowe, takie jak kradzież tożsamości, oszustwa finansowe, zwykła kradzież, hakerstwo - art. 286 oraz art. 287 Kodeksu Karnego

Przykładowe sytuacje, na które musicie zwrócić szczególną uwagę:

- **Metoda na wnuczka**

  w sieci działa w podobny sposób jak w realnym życiu. Wystarczy, że ktoś włamie się na konto społecznościowe bliskiej osoby lub skorzysta z jej komunikatora, aby wyłudzić pieniądze. Wiadomości wysyłane przez oszustów mogą zawierać linki, które po kliknięciu przeniosą seniora na fałszywą stronę z płatnościami. Oszust może też podać numer konta, na który prosi, aby pieniądze został przelane „niezwłocznie".

- **Metoda „na kod" czy też „na znajomego"**

  działa na podobnej zasadzie jak metoda na wnuczka. Osoba „znajoma" odzywa się do seniora i prosi o podanie np. danych karty kredytowej lub debetowej, tłumacząc jednocześnie, że pilnie musi zapłacić za zakupy, a właśnie nie ma przy sobie portfela.

- **Wykorzystywanie zaufania do instytucji**

  zdarza się, że oszuści podają się za ZUS, Urząd Skarbowy czy bank, aby wyłudzić wrażliwe informacje. Często wysyłają też wiadomości e-mailowe ze specjalnym linkiem, który po kliknięciu instaluje złośliwe oprogramowanie i pozwala przestępcom przejąć dane dostępowe do różnych serwisów.

- **Fałszywe zbiórki pieniędzy**

  na szczęście coraz większa liczba zbiórek jest weryfikowana, a osoby, które zbierają datki, muszą przejść dokładną kontrolę. Niestety jednak wciąż jeszcze zdarzają się sytuacje, w których organizatorzy nielegalnej kwesty próbują w ten sposób oszukać wrażliwych seniorów.

Powyżej wymienione przestępstwa są jedynie przykładami i nie obejmują wszystkich możliwych form cyberprzemocy. W przypadku popełnienia lub stania się ofiarą cyberprzemocy, skonsultuj się z prawnikiem i zgłoś naruszenia odpowiednim organom ścigania!


## NADUŻYCIE DANYCH OSOBOWYCH

### Co to jest kradzież tożsamości?

Kradzież tożsamości w sieci, znana również jako cyberprzestępstwo tożsamościowe, to proces nieuprawnionego pozyskiwania czyjegoś identyfikatora osobistego lub danych w celu popełnienia oszustw lub nadużyć. Może obejmować kradzież numeru dowodu osobistego, danych kont bankowych, informacji o kartach kredytowych lub loginów i haseł do kont online. Kiedy przestępca zdobywa te informacje, może je wykorzystać do popełniania oszustw finansowych lub innych działań, które mogą negatywnie wpływać na ofiarę.

## JAK PRZECIWDZIAŁAĆ NADUŻYCIU DANYCH OSOBOWYCH?

1. Zachowuj ostrożność w sieci! Unikaj udostępniania swoich osobistych danych, takich jak numer dowodu osobistego czy dane kont bankowych, na podejrzanych stronach internetowych lub w niezabezpieczonych wiadomościach.

2. Ustawiaj silne i unikalne hasła! Używaj silnych, złożonych haseł do swoich kont online i unikaj używania tego samego hasła do różnych usług. Dodatkowo, warto korzystać z dwuetapowej weryfikacji, gdy jest to dostępne.

3. Uważaj na phishing! Bądź czujny wobec podejrzanych wiadomości e-mail, linków i załączników. Upewnij się, że wiadomości pochodzą od wiarygodnych źródeł, a strony internetowe, na których wprowadzasz dane osobowe, są bezpieczne.

4. Aktualizuj urządzenia i instaluj oprogramowania antywirusowe! Regularnie aktualizuj swoje urządzenia i oprogramowanie, w tym zainstaluj skuteczne oprogramowanie antywirusowe i anty-malware.

5. Monitoruj swoje dane! Regularnie sprawdzaj swoje konta bankowe i karty kredytowe, aby wykryć ewentualne nieprawidłowości lub podejrzane transakcje.

Pamiętaj, że dbanie o swoją tożsamość online to ciągły proces. Warto być czujnym i stosować się do tych praktyk, aby zminimalizować ryzyko kradzieży tożsamości w sieci.

## ATAKI PHISINGOWE I OSZUSTWA FINANSOWE

### Na czym polegają ataki phishingowe?

Ataki phishingowe są techniką stosowaną przez przestępców internetowych, która polega na próbie oszustwa i spowodowaniu, aby osoba podjęła działanie zgodnie z ich zamierzeniami. Cyberprzestępcy podszywają się m.in. pod firmy kurierskie, firmy telekomunikacyjne czy urzędy, a nawet pod osoby nam najbliższe i starają się wyłudzić informacje dotyczące danych do logowania

się np. do naszych kont bankowych czy używanych przez nas kont społecznościowych.

Atak phishingowi polega na wysłaniu do określonej osoby np. wiadomości SMS czy wiadomości e-mail, coraz częściej obserwuje się również powiadomienia przesyłane za pośrednictwem portali społecznościowych czy komunikatorów. Należy zachować szczególną czujność, gdyż oszuści potrafią tworzyć wiadomości do złudzenia przypominające „oryginalne" powiadomienia od określonych podmiotów, a w tym celu wykorzystują skopiowane logotypy i szaty graficzne wykorzystywane przez określone organizacje i podmioty. Takie wiadomości mogą próbować skłonić osobę do ujawnienia informacji poufnych, często zawierają link do strony internetowej, która po wejściu rozprzestrzenia szkodliwe oprogramowanie czy zainfekowany załącznik.

**Jak rozpoznać, czy mamy do czynienia z atakiem phishingowym?**

- wiadomości phishingowe często zawierają błędy ortograficzne, interpunkcyjne, składniowe, często nie posiadaną także polskich znaków diakrytycznych, czyli np. „ą", „ę",
- bądź ostrożna/y na treści typu „wyślij dane w ciągu 24 godzin", „padłeś ofiarą przestępstwa" inne podobne,
- weryfikuj nazwę nadawcy,
- pamiętaj, że Twój bank lub jakakolwiek inna instytucja oraz urzędy publiczne nie poproszą Cię przekazanie danych za pomocą wiadomości SMS,
- zweryfikuj podejrzaną wiadomość poprzez telefon do banku czy innej instytucji/urzędu,
- cyberprzestępcy często posługują się skróconymi linkami, dlatego dokładnie zweryfikuj wskazany w wiadomości adres domeny internetowej, i jeśli wzbudza Twoje wątpliwości nie wchodź w niego!

### Co zrobić w sytuacji ataku phishingowego?

- przede wszystkim bądź ostrożna/y i szczególnie wyczulona/y na wszelkie wiadomości zawierające podejrzane linki czy skłaniające do podania wrażliwych danych,
- pod żadnym pozorem nie wchodź w link przesłany w podejrzanej wiadomości ani nie podawaj żądanych przez nadawcę danych,
- jeżeli masz uzasadnione podejrzenie, że jesteś ofiarą phishingu niezwłocznie zgłoś ten fakt Policji lub/i prokuraturze,
- możesz również zgłosić phishing przez wypełnienie krótkiego formularza na stronie

**https://incydent.cert.pl/**

## MALWARE I WIRUSY

Malware to skrót od „malicious software", czyli szkodliwe oprogramowanie. Jest to rodzaj programu komputerowego, który ma złośliwe intencje i może powodować szkody w systemie komputerowym lub naruszać prywatność użytkownika. Przykłady malware to wirusy, trojany, robaki komputerowe, ransomware i keyloggery.

Celem malware może być kradzież danych, uszkodzenie systemu, podsłuchiwanie aktywności użytkownika lub przejęcie kontroli nad komputerem. Ważne jest, aby chronić swój system przed malware, korzystając z programów antywirusowych i zachowując ostrożność podczas pobierania plików lub otwierania podejrzanych wiadomości.

Wirusy komputerowe to rodzaj szkodliwego oprogramowania, które replikuje się i rozprzestrzenia na inne pliki lub systemy komputerowe. Podobnie jak wirusy w organizmach, wirusy komputerowe wymagają hosta (pliku, programu lub systemu), aby się rozmnażać i działać. Gdy wirus zostanie uruchomiony lub plik zainfekowany zostanie otwarty, wirus może się skopiować i przenieść do innych plików lub komputerów, infekując je. Efekty działania wirusów mogą być różne, od uszkodzenia danych i programów, po kradzież informacji, kontroli nad systemem lub spowolnienie działania komputera.

Wirusy komputerowe mogą się rozprzestrzeniać za pomocą zainfekowanych plików, poczty elektronicznej, stron internetowych lub innych środków komunikacji. Stosowanie zaktualizowanego oprogramowania antywirusowego i unikanie podejrzanych plików czy linków pomaga w ochronie przed wirusami komputerowymi.

Aby uniknąć wirusów komputerowych i malware, warto podjąć kilka środków ostrożności. Oto kilka zaleceń:

- Zainstaluj i regularnie aktualizuj oprogramowanie antywirusowe - wybierz renomowany program antywirusowy i regularnie aktualizuj go, aby chronić swój system przed najnowszymi zagrożeniami,
- Aktualizuj system operacyjny i oprogramowanie - regularnie pobieraj i instaluj dostępne aktualizacje systemu operacyjnego i innych programów. Aktualizacje często zawierają łatki bezpieczeństwa, które chronią przed znanymi luki w zabezpieczeniach,

- Ostrożnie otwieraj załączniki i linki - nie otwieraj załączników ani nie klikaj na linki pochodzące z podejrzanych źródeł, nieznanych nadawców czy podejrzanych wiadomości e-mail. Mogą one zawierać wirusy lub oprogramowanie malware,

- Pobieraj oprogramowanie z zaufanych źródeł - przed pobraniem jakiegokolwiek oprogramowania upewnij się, że pochodzi ono ze sprawdzonego i zaufanego źródła. Unikaj pobierania z podejrzanych stron internetowych,

- Nie klikaj na podejrzane reklamy - unikaj klikania na podejrzane reklamy lub banery na stronach internetowych. Mogą one przekierować Cię na zainfekowane strony lub pobierać malware,

- Uważaj na wiadomości phishingowe - bądź czujny wobec wiadomości e-mail, które próbują uzyskać Twoje poufne informacje. Sprawdzaj dokładnie nadawcę i usuwaj wiadomości, które wydają się podejrzane lub nietypowe,

- Backupuj swoje dane - regularnie twórz kopie zapasowe swoich danych i przechowuj je w bezpiecznym miejscu. W przypadku infekcji malware lub ataku wirusa, będziesz mieć możliwość przywrócenia swoich danych.

Pamiętaj, że ważne jest utrzymanie świadomości i bycie ostrożnym w swoich działaniach online!

## BRAK PRYWATNOŚCI DANYCH

Kwestią oczywistą jest, że prywatności w Internecie jest coraz mniej. Winę za to ponoszą zarówno firmy zarabiające na obrocie danymi o użytkownikach, jak i sami internauci. W wielu przypadkach to my sami pozwalamy, by informacje o nas, nawet te najbardziej osobiste, przedostały się do sieci. Bardzo łatwo zapominamy, że to, co raz trafiło do Internetu, już tak łatwo z niego nie zniknie.

- Sami udostępniamy dane poprzez publikowanie treści, w tym zdjęć, na portalach społecznościowych oraz randkowych. Jesteśmy bardzo często nieostrożni. Zakładamy, że przecież mamy prywatny profil , jednak dostęp do naszych zdjęć, filmów, tego, co piszemy i informacji o nas mają wszyscy inni użytkownicy.

- Zakładamy mnóstwo kont w sklepach internetowych i wyrażamy zgodę na przetwarzanie danych osobowych i akceptujemy długie regulaminy. Większości, jeżeli nie wszystkich, w ogóle nie czytamy. W ten sposób po raz kolejny zgadzamy się na obrót informacjami o nas samych. Nie należy jednak zapominać o przypadkach firm, które w nielegalny sposób obracają danymi o użytkownikach.

Czy przydarzyła Wam się sytuacja, w której chcieliście kupić buty czy sprzęt AGD bądź RTV za pośrednictwem przeglądarki internetowej, zakończyliście poszukiwania, a na następny dzień podczas przeglądania porannych wiadomości w Internecie zaczęły Wam się wyświetlać reklamy tych samych produktów bądź produktów podobnych?

To nic innego, jak wszechobecne zjawisko profilowania w sieci. Dzięki zebranym w Internecie informacjom na temat tego, jakie strony najczęściej odwiedzacie, jakie zakupy robicie lub co na dany moment jest Wam potrzebne, w różnych miejscach, wyświetlają Wam się reklamy produktów, którymi faktycznie możesz być zainteresowany.

Za każdym razem, gdy klikniesz „akceptuję” po wejściu na stronę internetową, Twoje dane (informacje o Twojej aktywności, co oglądasz, kiedy itd.) są nie tylko przechowywane, ale także (odpłatnie) przekazywane dalej, do innych firm.

Wiele osób twierdzi, że śledzenie i profilowanie użytkowników w sieci staje się coraz bardziej inwazyjne i niemal narusza prywatność każdego z nas. Pobierane dane, dotyczą przecież zdrowia, często naruszają życie prywatne, sytuacji finansowej, pochodzenia etnicznego, relacji osobistych, nałogów, słabości i marzeń, a wyświetlane reklamy pojawiają się bez jasnej zgody internauty. Proponowane reklamy mogą nam jednak ułatwić życie, przyspieszyć poszukiwanie wymarzonej torebki, znaleźć specjalistyczne narzędzia czy umożliwić zakup nowego żelazka w okazyjnej cenie.

Podczas internetowych poszukiwań zabawek dla wnuków może się zdarzyć że, pojawią się reklamy i otrzymacie z sieci propozycje innych sklepów, które w ofercie posiadają takie same bądź podobne produkty.

Dzieje się tak, gdyż śledzenie w Internecie umożliwia odpowiednie targetowanie behawioralne reklam.

Pamiętaj! Aby zachować anonimowość, po pokazaniu się komunikatów dotyczących prywatności, nie wyrażaj zgody na:

- śledzenie Twojej działaności przez aplikacje i strony internetowe,
- nie udzielaj zgody na dostęp do kalendarza, kontaktów, historii przeglądarki, wrażliwych logów aplikacji systemowych, aplikacji aktywnych na urządzeniu,
- śledzenie Twojej lokalizacji.

## A co to w ogóle jest przetwarzanie danych?

Odnosząc się bezpośrednio do Ogólnego rozporządzenia o ochronie danych (RODO), a konkretnie do art. 4 pkt 2:

„przetwarzanie oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie, a zwłaszcza te, które wykonuje się w systemach informatycznych".

Aby przetwarzanie naszych danych było legalne, każdy administrator tych danych musi, w sposób odpowiedni, je chronić.

Pamiętaj, że masz swoje prawa! Każda osoba, której dane są przetwarzane, posiada szereg praw, których spełnienie powinien zagwarantować każdy administrator, który przetwarza dane.

- prawo dostępu do danych (art. 15 RODO),
- prawo do sprostowania danych (art. 16 RODO),
- prawo do bycia zapomnianym, tj. do usunięcia danych (art. 17 RODO),
- prawo do ograniczenia przetwarzania (art. 18 RODO),
- prawo do przenoszenia danych (art. 20 RODO),
- prawo do sprzeciwu (art. 21 RODO),
- prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa (art. 22 RODO).

# PODSUMOWUJĄC!

Internet zapewnia nieograniczone możliwości!

Dzięki jego zasobom możemy zrobić udane zakupy bez wychodzenia z domu, odbyć rozmowy z naszymi znajomymi oraz rodziną i oddawać się różnym rodzajom rozrywki. Internet jest również doskonałym źródłem informacji o świecie.

Jednak mimo swoich ogromnych zalet, środowisko Internetu może być niebezpieczne, a użytkowanie zasobów Internetu niesie ze sobą konkretne ryzyka dla seniorów.

Celem naszego poradnika jest wskazanie Wam, jak pozostać bezpiecznym podczas korzystania z sieci.

Mamy nadzieję, że dzięki naszym poradom będziecie zwracać szczególną uwagę na możliwe zagrożenia!



Ministerstwo Rodziny
i Polityki Społecznej

@LexCultura
fundacja_lexcultura
fundacja@lexcultura.pl
www.lexcultura.pl

ISBN 978-83-965751-3-5