Warto wiedzieć...

10 zasad ochrony prywatności przy instalowaniu aplikacji

Rozmawiajmy o ochronie prywatności w sieci

Liczne aplikacje służą do komunikacji, rozrywki, nauki, a także ułatwiają załatwienie codziennych spraw, poruszanie się czy wspomagają aktywność fizyczną. Za korzystanie z wielu „darmowych" aplikacji „płacimy" naszymi danymi i godzimy się na ich wykorzystanie do różnych celów. Warto więc zwracać uwagę m.in. na to, jakie dane zbierają aplikacje i na co się zgadzamy przy ich instalowaniu oraz przede wszystkim, czy aplikacje i usługi pochodzą z zaufanych i sprawdzonych źródeł.

Poniżej przedstawiamy zbiór 10 najważniejszych wskazówek, o których warto pamiętać podczas instalowania aplikacji oraz po jej zainstalowaniu, w celu zwiększenia bezpieczeństwa i ochrony naszej prywatności:

Podczas instalowania aplikacji:

- Zwracajmy uwagę, czy twórcy i dostawcy aplikacji wywiązują się z **obowiązku informacyjnego.** Powinni nas poinformować w sposób przejrzysty i zrozumiały o tym, jakie dane osobowe i na jakich warunkach będą przetwarzać.
- Jeżeli dane osobowe są **przetwarzane na podstawie naszej zgody,** musi być ona wyrażona dobrowolnie, a my musimy mieć świadomość, na co dokładnie się godzimy. Pamiętajmy, że przysługuje nam **prawo do wycofania zgody** w każdym momencie.
- **Zapoznajmy się z polityką prywatności**, aby mieć pełną świadomość, na co się zgadzamy. Zwracajmy szczególną uwagę na to, czy dana aplikacja udostępnia nasze dane osobowe innym firmom, z którymi współpracuje**.**
- **Zwracajmy uwagę, do jakich danych osobowych i funkcji telefonu aplikacja będzie mieć dostęp**. Niektóre aplikacje domagają się dostępu do: informacji o naszej lokalizacji, zdjęć, kontaktów, czy dokumentów, nawet jeżeli nie jest to konieczne do realizacji usługi.
- Jeśli usługi społeczeństwa informacyjnego, takie jak np. gry czy aplikacje edukacyjne, są oferowane dziecku bezpośrednio, **zgodę na przetwarzanie danych osobowych dziecka poniżej 16. roku życia** musi wyrazić lub zaaprobować jego rodzic/opiekun prawny.
- W celu ochrony prywatności najmłodszych dzieci, warto korzystać z **aplikacji do kontroli rodzicielskiej.** Dzięki temu każda aplikacja, z której dziecko chciałoby skorzystać, będzie wymagać zgody rodzica/opiekuna prawnego na jej instalację. Warto też wspólnie z dzieckiem decydować o wyborze aplikacji oraz omówić ustawienia dotyczące ochrony prywatności.

Po zainstalowaniu aplikacji:

- Decydujmy o ustawieniach, które zapewnią nam możliwie największą ochronę naszych danych. **Weryfikujmy i personalizujmy** ustawienia prywatności w aplikacji, z której już korzystamy, aby ograniczać udostępnianie informacji o nas innym firmom/osobom, czy aplikacjom.
- Zwracajmy uwagę na to, czy aplikacja może mieć dostęp do różnych form płatności. Zweryfikujmy, czy nie zezwoliliśmy aplikacji na dostęp do naszej karty kredytowej lub płatniczej, aby nie obciążać konta niechcianymi wydatkami z powodu nieświadomych zakupów w aplikacji, np. w związku z zakupem gier.
- Zwracajmy uwagę na **udostępnianie szczególnych kategorii danych,** np. danych o zdrowiu, i pamiętajmy, by nie przekazywać takich danych administratorom, jeśli nie jest to konieczne. Dane osobowe wymagają szczególnej ochrony, gdyż kontekst ich przetwarzania może powodować poważne ryzyko dla podstawowych praw i wolności.
- **Regularnie dokonujmy przeglądu zainstalowanych aplikacji** pod kątem ochrony naszej prywatności. Kolejne aktualizacje aplikacji mogą wprowadzać nowe ustawienia, dotyczące przetwarzania naszych danych osobowych, które mogą być dla nas niekorzystne.

Wprawdzie zgodnie z RODO, nasza prywatność powinna być domyślnie chroniona w najwyższym stopniu, jednak w praktyce nierzadko jesteśmy narażeni na ryzyko w tym zakresie. Coraz częściej słyszymy o szpiegowskich aplikacjach, czy naruszeniach, polegających na wyłudzeniu danych. Dlatego pamiętajmy, aby dokonywać regularnego przeglądu zainstalowanych aplikacji i usuwać te, z których nie korzystamy, a także świadomie wybierać te aplikacje, które najmniej ingerują w naszą prywatność.

URZĄD OCHRONY DANYCH OSOBOWYCH

Warto wiedzieć, że...

dzięki kilku kliknięciom możesz ograniczyć swoją widoczność w sieci /część I.

Zadbaj o prywatność w serwisach społecznościowych.

.

Korzystajmy z ustawień prywatności w serwisach społecznościowych, aby ograniczyć swoją widoczność w sieci i zakres informacji dostępnych do publicznej wiadomości. Im więcej i aktywniej korzystamy z danego portalu, tym bardziej powinniśmy zwrócić uwagę na szczegółowe ustawienia, które będą nam potrzebne do ochrony naszej prywatności i danych osobowych. Zwracajmy uwagę na zakres udostępnianych przez nas informacji, rodzaj danych osobowych i na to, kto ma dostęp do publikowanych przez nas treści. Publikowanie informacji, które powinny być szczególnie chronione m.in. poglądów politycznych, informacji o nałogach, przekonań religijnych, może narazić nas na bardzo poważne konsekwencje.

Zawsze pamiętajmy o żelaznej zasadzie – im mniej informacji o sobie udostępniamy w sieci tym lepiej, tym bezpieczniej.

Ustawienia prywatności w sieci

Liczne firmy usprawniają swoje działania w poszukiwaniu rozwiązań, które ograniczają bezpieczeństwo i prywatność użytkowników sieci społecznościowych oraz zmieniają ustawienia domyślne. Nowe funkcje, za pomocą których gromadzą i przechowują informacje o nas i naszej aktywności, pozwalają im efektywniej zarządzać danymi.

Warto zadbać o ustawienia prywatności

Warto się przyjrzeć możliwościom konfiguracji i dostosować ustawienia prywatności na portalu, z którego korzystamy do własnych potrzeb. Nie ma powodu, żeby zgadzać się na domyślnie proponowaną konfigurację, która w przypadku portalu komercyjnego, ma na celu ułatwić mu zbieranie naszych danych i dzielenie się nimi z zewnętrznymi organizacjami/firmami.

O co chodzi w domyślnej ochronie prywatności w sieci?

- ❑ Produkty lub usługi powinny być tak zbudowane, by obowiązywały rygorystyczne ustawienia szanujące prywatność. Jedynie nasze świadome działanie powinno umożliwiać szersze przetwarzanie naszych danych osobowych.
- ❑ Organizacja, która jest administratorem (a więc decyduje o celach i środkach przetwarzania danych osobowych) naszych danych ma obowiązek zapewnić odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były dane niezbędne dla osiągnięcia celu przetwarzania.
- ❑ Jedynymi danymi, które mogą być przetwarzane i przechowywane (przez określony czas) są dane niezbędne do korzystania z platformy, a organizacje mogą je przechowywać tak długo, jak to tylko konieczne.
- ❑ Niestety, dane na nasz temat gromadzone przez platformy społecznościowe, operatorów wyszukiwarek internetowych czy dostawców poczty elektronicznej, często wykraczają poza zakres danych świadomie przez nas udostępnionych.
- ❑ Firmy mogą śledzić każdy nasz ruch w sieci społecznościowej, a także na podłączonych urządzeniach.
- ❑ W dalszym kroku, wykorzystują te informacje do tworzenia naszego profilu użytkownika sieci, czego konsekwencją jest np. wyświetlanie nam zindywidualizowanych reklam.

Jak spersonalizować sposób korzystania z popularnego portalu społecznościowego, w celu ochrony prywatności? W kolejnym materiale krok po kroku podpowiemy, z jakich wybranych opcji dotyczących zbierania danych i ochrony prywatności skorzystać, aby odzyskać częściową kontrolę nad danymi, które sami udostępniamy.

URZĄD OCHRONY DANYCH OSOBOWYCH

Warto wiedzieć...

dzięki kilku kliknięciom możemy ograniczyć swoją widoczność w sieci – część II

Facebook. Sprawdźmy razem ustawienia prywatności

Poprzez konfigurację ustawień prywatności jesteś w stanie ograniczyć swą widoczność w sieci tak, by publikowane przez Ciebie posty oraz informacje o Tobie i Twoich znajomych dostępne były wyłącznie dla wybranych odbiorców. Niezależnie od urządzenia, z którego logujesz się do *Facebooka*, zwróć uwagę na zagadnienie personalizacji ustawień.

Oto zbiór 20 najważniejszych wskazówek dotyczących ustawień prywatności, które warto sprawdzić na *Facebooku*, w celu zwiększenia bezpieczeństwa i poczucia prywatności:

1. Sprawdź, co i komu udostępniasz

Weryfikuj ustawienia prywatności, by mieć pewność, że udostępniasz materiały tylko wskazanym przez siebie odbiorcom. Określ, kto będzie mógł oglądać Twoje posty, kontaktować się z Tobą lub wyszukiwać profil poprzez podany adres e-mail i numer telefonu.

2. Ukryj listy znajomych

Lista Twoich znajomych jest domyślnie dostępna dla wszystkich osób korzystających z *Facebooka*. Można ją jednak ukryć:

> ***Ustawienia –> Prywatność –> Kto może zobaczyć Twoją listę znajomych?***

3. Ogranicz widoczność swojego profilu z zewnątrz

Jeśli nie chcesz, by inne przeglądarki i wyszukiwarki internetowe podawały link do Twojego profilu – wyłącz tę opcję w ustawieniach:

> ***Ustawienia –> Prywatność –> Jak można Cię znaleźć i nawiązać kontakt?***

4. Zwracajmy uwagę, co udostępniamy w *relacji* i kto może ją zobaczyć

Relacje pozwalają udostępniać nam teksty, zdjęcia oraz filmy przez 24 godziny. Wszystkie treści w relacji widoczne są w aplikacji *Facebook*. Przed publikacją treści warto określić, komu chcesz je udostępniać.

5. Zarządzaj swoim profilem

Ogranicz widoczność podstawowych danych na profilu: daty urodzenia, numeru telefonu, adresu e-mail, miejsca zamieszkania. Stosuj sprawdzoną zasadę „im mniej danych osobowych, tym lepiej".

Pamiętaj! Na urządzeniach mobilnych bezpieczniej zalogować się do *Facebooka* za pomocą przeglądarki internetowej z zainstalowanymi wtyczkami. Aplikacje mobilne m.in. *Facebook* i *Messenger*, żądają dostępu do znacznie większej ilości danych z urządzenia, np. kontaktów z książki adresowej czy możliwości dostępu do aparatu.

6. Nie udostępniaj danych wrażliwych

Publikowanie informacji, które powinny być szczególnie chronione – poglądów politycznych, informacji o zdrowiu i nałogach, preferencji seksualnych, przekonań religijnych – może narazić Cię na bardzo poważne konsekwencje. Jeśli to możliwe, rezygnuj z ich podawania.

7. Zarządzaj ustawieniami lokalizacji

Nie warto zezwalać portalowi na śledzenie Twojej lokalizacji w celu tworzenia historii miejsc, które odwiedzamy. Zarządzajmy dostępem *Facebooka* do usług, które pozwalają na precyzyjne określenie lokalizacji urządzenia przy użyciu wybranych opcji, a także zarządzanie historią miejsc Twojego pobytu.

8. Kontroluj ustawienia dotyczące rozpoznawania twarzy

Przy pomocy technologii rozpoznawania twarzy portal analizuje zdjęcia i filmy użytkowników. Na tej podstawie tworzony jest szablon, dzięki któremu nasza twarz jest rozpoznawana w postach innych użytkowników. Jeśli wyłączymy funkcję rozpoznawania twarzy, portal nie będzie wykorzystywać jej do proponowania innym, by oznaczali nas na zdjęciach.

9. Twój *dziennik aktywności* na portalu

Wzmacniaj poczucie kontroli nad treściami, które sam publikujesz. Ograniczaj grono osób, dla których opublikowane informacje będą dostępne. Portal zapamiętuje każdą Twoją aktywność: komentarze, *lajki*, obejrzane filmy i *relacje*, gry, zapytania w wyszukiwarce serwisu. Sprawdź ustawienia dotyczące *dziennika aktywności*.

10. Ograniczaj widoczność Twoich postów, stron i osób, które obserwujesz

Weryfikuj ustawienia prywatności, by mieć pewność, że udostępniasz materiały tylko wskazanym przez siebie odbiorcom. Określ, kto będzie mógł oglądać Twoje posty, kontaktować się z Tobą lub wyszukiwać profil poprzez podany adres e-mail i numer telefonu;

URZĄD OCHRONY DANYCH OSOBOWYCH

Warto wiedzieć...

dzięki kilku kliknięciom możemy ograniczyć swoją widoczność w sieci – część II

Facebook. Sprawdźmy razem ustawienia prywatności

11. Zdecyduj, kto będzie mógł publikować na Twojej tablicy i oznaczać Cię w postach

Korzystaj z możliwości akceptowania wybranych postów, które zostaną opublikowanie na Twojej tablicy lub postów, w których nas oznaczono za pomocą funkcji Zatwierdzanie na osi czasu. Posty te nadal będą widoczne tylko na tablicy osoby, która Cię oznaczyła, i dla osób, którym udostępnia ona swoje wpisy.

12. Usuwaj historię wyszukiwań

Mamy możliwość usuwania z historii konkretnych zapytań lub całości historii. Podobnie jest w przypadku historii wydarzeń, w których oznaczyliśmy swój udział.

13. Przejrzyj strony, które lubisz

Twoje *polubienia* sprzed lat mogą do dziś być wykorzystywane przez reklamodawców. Aby sprawdzić listę *polubień*, należy wejść do Dziennika aktywności na swojej stronie profilowej. Warto przejrzeć też całą aktywność na osi czasu.

14. Ograniczaj dostęp aplikacji zewnętrznych do danych z Twojego profilu

Możesz wyłączyć dzielenie się danymi między aplikacjami – ograniczyć dostęp do listy znajomych, wieku, miejsca zamieszkania, adresu e-mail. Większość programów wymaga dostępu najczęściej do profilu publicznego zawierającego imię i nazwisko oraz zdjęcie profilowe.

15. Ograniczaj liczbę usług, do których logujesz się za pomocą danych do jednego konta

Zablokowanie możliwości logowania przez portal do aplikacji zewnętrznych oznacza również uniemożliwienie zbierania przez nie danych, a także dostarczania profilowanych reklam, sugerowanych na bazie naszych bieżących zachowań w sieci. W ten sposób nie tylko zwiększysz poziom ochrony prywatności, ale również bezpieczeństwa danych. W przypadku ich wycieku lub wykradzenia z jednej usługi, narażone będą również dane przechowywane przez pozostałe.

16. Określ, czy aplikacje, z których korzystają znajomi, mogą wykorzystywać informacje o nas

Nawet jeśli nie korzystasz z aplikacji, ale korzystają z niej Twoi znajomi, to w konsekwencji aplikacja może uzyskać dostęp do Twoich danych. Dzieje się tak w przypadku, gdy widoczność znajomych ustawiona jest jako *publiczna*. Możesz to zmienić i zdecydować, że informacje o Tobie nie mogą być wykorzystywane w aplikacjach przez inne osoby.

17. Bezpieczeństwo Twojego konta

Warto zadbać o bezpieczeństwo konta na wypadek utraty kontroli nad nim bądź urządzeniem, za pomocą którego się logujesz. Jeśli używasz wielu urządzeń jednocześnie, możesz zdalnie wylogować się z innych sesji:

> ***Ustawienia –> Bezpieczeństwo –> Miejsce logowania*** **(widnieje tam lista urządzeń i ostatnich sesji)**

Smartfon może stać się również dodatkową warstwą zabezpieczeń. Za każdym razem, przy próbie logowania z nowego urządzenia i przeglądarki, będzie trzeba potwierdzić tożsamość na urządzeniu zaufanym. To dobry i prosty sposób, by uniknąć przechwycenia konta. Zalecane jest również włączenie powiadomienia o nierozpoznanych logowaniach na Facebooku

> ***Ustawienia –> Bezpieczeństwo –> Konfiguracja dodatkowych zabezpieczeń***

18. Hasła do konta

Dostęp do konta powinien być możliwy za pomocą silnego hasła zawierającego wielkie i małe litery, cyfry oraz znaki specjalne. Warto wykorzystać również podwójny sposób weryfikacji przy logowaniu i włączyć dwuskładnikowe (dwuetapowe) uwierzytelnianie. Warto również zaszyfrować wiadomości e-mail z powiadomieniami z Facebooka, dzięki czemu tylko Ty będziesz miał do nich dostęp.

19. „Portal społecznościowy wie o nas wszystko"

Przejrzenie archiwum portalu może uświadomić nam, że stwierdzenie to jest prawdziwe. Warto jednak pamiętać o możliwości skorzystania z dostępu do danych użytkownika i przejrzeć informacje, które przetwarzane są przez portal lub pobrać kopię swoich danych (funkcja *Pobierz archiwum*). Ilość informacji o użytkowniku, jaką dysponuje *Facebook*, jest ogromna – szczególnie jeśli ten korzysta z Messengera.

20. Usuwanie konta

Usunięcie konta z portalu to długa procedura, ale po jej zakończeniu zniknie większość posiadanych o użytkowniku informacji.

Pamiętaj! Usunięcie postu lub zdjęcia z profilu na *Facebooku* nie gwarantuje, że zniknęło ono z sieci, ponieważ każdy, kto miał dostęp do opublikowanych przez nas materiałów, mógł je wcześniej skopiować lub zrobić zrzut ekranu.

Chcesz wiedzieć więcej…

Jeśli pragniesz zdobyć więcej informacji na temat zasad przetwarzania danych osobowych, sięgnij po przewodnik dotyczący prywatności i zasad dotyczących danych. Znajdziesz tam szczegółowy opis sposobu gromadzenia informacji i ich udostępniania oraz czas ich przechowywania przez aplikacje, w tym *Facebooka*, *Instagrama*, *Messengera*.

URZĄD OCHRONY DANYCH OSOBOWYCH

Warto wiedzieć…

Gra Twoimi danymi

Jak możemy dbać o bezpieczeństwo naszych danych, gdy gramy w gry on-line?

Prawie wszystkie współczesne gry tuż po instalacji, wymagają od swoich graczy zgody na przetwarzanie danych osobowych. Podanie danych do zawarcia transakcji zakupu lub założenia konta wiąże się z obowiązkiem zaakceptowania regulaminu gry oraz potwierdzeniem zapoznania się z „Polityką prywatności", gdzie znajdują się informacje dotyczące procesu przetwarzania danych osobowych gracza. Przedstawiciele branży gamingowej wykorzystują dane osobowe na własny użytek lub sprzedają je firmom zewnętrznym. Dane, które udostępnimy w grze mogą również stać się celem ataku cyberprzestępców. Nasze dane i prywatność mają dużą wartość i powinniśmy o nie zadbać.

Oto 10 praktycznych wskazówek, które pomogą zadbać o nasze bezpieczeństwo podczas grania w sieci.

1. **E-mail do obsługi gier** – załóż specjalną skrzynkę e-mail do grania. Jeśli Twoje dane logowania wyciekną lub zostaną skradzione, reszta Twoich cyfrowych spraw nie będzie zagrożona. Adres mailowy, zawierający pełne imię i nazwisko, to również dane, które należy chronić.
2. **Gry pobieraj tylko ze sprawdzonych, legalnych źródeł** - piratowane gry, podejrzane „darmowe" wersje beta – to najczęstsze narzędzia hakerów, którzy chcą poznać Twoje dane logowania albo uzyskać dostęp do karty płatniczej.
3. **Wybierając nick** nigdy nie używaj swojego imienia, nazwiska, daty urodzenia, ani numeru PESEL. Najrozsądniej będzie wymyślić fikcyjny, z niczym nie kojarzący się nick.
4. **Nigdy nie używaj tej samej nazwy dla konta i postaci w grze.** Używaj takich, które nie pozwolą na połącznie jednego z drugim.

URZĄD OCHRONY DANYCH OSOBOWYCH

7. **Dostosuj ustawienia** tak, by gra nie miała dostępu do danych o lokalizacji**,** z mikrofonu i aparatu, gdy z niej nie korzystasz. Sprawdź również, czy możesz wyłączyć w menu dzielenie się danymi osobowymi i dalej cieszyć się grą.

8. Korzystając z **komunikatora, chatu albo streamując** uważaj, aby nie udostępniać żadnych danych osobowych dotyczących logowania, ani finansowych.

9. **Używanie kodów** może grozić instalacją wirusów lub kradzieżą Twoich danych. Jeśli decydujesz się ich używać, zachowaj szczególną ostrożność.

10. „**Nie ma nic za darmo**” – prezenty on-line przyjmuj tylko od osób albo firm, które znasz i którym ufasz. E-mail z darmowymi skinami czy złotem może być tzw. atakiem phishingowym albo próbą instalacji na Twoim urządzeniu keyloggera czyli programu śledzącego Twoje ruchy na klawiaturze. Nie klikaj w linki w podejrzanych wiadomościach.

11. Jeśli chcesz robić **zakupy w grze**, korzystaj z przedpłaconych kuponów**,** aby nie podawać danych z karty płatniczej.

Oprócz tych zasad pamiętaj o podstawowych zasadach cyberbezpieczeństwa, takich jak używanie silnych i unikatowych haseł, logowanie dwustopniowe, korzystanie z aktualnego oprogramowania antywirusowego czy VPN, w gdy łączysz się publiczną siecią Wi-Fi.

Warto być ostrożnym nawet w trakcie zabawy!

URZĄD OCHRONY DANYCH OSOBOWYCH

Warto wiedzieć...

Instagram

jesteś jednym z ponad miliarda użytkowników

Korzystając z popularnej na całym świecie aplikacji Instagram, służącej do edytowania oraz publikowania zdjęć i czasowych relacji (*stories*), pamiętaj o podstawowych zasadach ochrony danych osobowych. Kieruj się poniższymi wskazówkami:

- Gdy publikujesz swój wizerunek, rób to mądrze – nie zamieszczaj zdjęć swojego najbliższego otoczenia, a także osób, które nie wyraziły na to zgody. Twój wygląd zewnętrzny lub nawet głos to również dane, które mogą zostać skradzione. Dbaj o prywatność!

- Nie podawaj zbyt wielu informacji na swój temat. Imię i nazwisko, data urodzin czy miejsce zamieszkania nie muszą być widoczne na Twoim profilu. Przyjmij zasadę „im mniej o mnie w sieci – tym lepiej".

- Jeśli chcesz zwiększyć poziom prywatności, ustaw status swojego konta na ***prywatne***. Funkcję tę znajdziesz w zakładce oznaczonej zębatką.

  > Aplikacja mobilna: ***ustawienia*** → ***prywatność*** → ***prywatność konta*** → ***konto prywatne***
  > Przeglądarka internetowa: ***ustawienia*** → ***prywatność i bezpieczeństwo*** → ***konto prywatne***

  Teraz możesz mieć pewność, że nikt nie zaobserwuje Cię bez Twojej zgody. Profil prywatny gwarantuje też, że Twoje zdjęcia będą widoczne wyłącznie dla osób zaufanych. Status przełączyć można w każdej chwili.

- Jeśli ktoś bez Twojej zgody udostępnia zdjęcia i filmy albo publikuje treści, których nie chcesz oglądać, możesz przestać obserwować takiego użytkownika lub zablokować go. Możesz także zgłosić aplikacji konto osoby, która według Ciebie narusza zasady społeczności.

- Sam możesz zdecydować, z kim chcesz podzielić się swoją relacją, dzięki czemu odbiorcami Twojego ***stories*** może być tylko grupa zaufanych przyjaciół i znajomych. Listę bliskich znajomych w łatwy sposób możesz ustawić na swoim profilu. W dowolnym momencie możesz ją zaktualizować lub usunąć.

  > Aplikacja mobilna: ***ustawienia*** → ***konto*** → ***bliscy znajomi***

- Twoje hasło do Instagrama powinno być silne, trudne do złamania, ale i takie, które będziesz w stanie zapamiętać. Sama aplikacja rekomenduje użycie liter drukowanych, cyfr oraz innych znaków, np. łącznika lub myślnika. By zmienić hasło na nowe, zajrzyj do opcji aplikacji.

  > Aplikacja mobilna: ***ustawienia*** → ***zabezpieczenia*** → ***hasło***
  > Przeglądarka internetowa: ***ustawienia*** → ***zmień hasło***

  Korzystaj również z dwuetapowego uwierzytelniania za pośrednictwem SMS, dzięki czemu zwiększysz bezpieczeństwo swojego konta.

  > Aplikacja mobilna: ***ustawienia*** → ***zabezpieczenia*** → ***uwierzytelnianie dwuskładnikowe***
  > Przeglądarka internetowa: ***ustawienia*** → ***prywatność i bezpieczeństwo*** → ***uwierzytelnianie dwuskładnikowe***

- Dzięki narzędziom Instagrama bezproblemowo sprawdzisz, jakich zmian w profilu dokonywałeś przez cały okres użytkowania aplikacji – czy i kiedy zmieniałeś hasło, adres mailowy, numer telefonu. Jak brzmiał stary nick, co zamieściłeś w biogramie, oraz czy podawałeś tam linki do stron zewnętrznych. Możesz uzyskać do nich dostęp, kierując się poniższą instrukcją.

  > Aplikacja mobilna: ***ustawienia*** → ***zabezpieczenia*** → ***dostęp do danych***
  > Przeglądarka internetowa: ***ustawienia*** → ***prywatność i bezpieczeństwo*** → ***dane konta***

- Za każdym razem wyloguj się po zakończonej sesji. Zapewni to maksymalną ochronę konta oraz utrudni osobom trzecim dostęp do niego. Pamiętaj, by dane do logowania nie były zapisane w przeglądarce, z której korzystasz. Po zalogowaniu pojawi się komunikat: ***Zapisać Twoje dane logowania?*** Tu należy wybrać opcję ***nie teraz***. Rozwiązanie to umożliwi ochronę Twojego loginu i hasła przed innymi osobami korzystającymi z komputera.

- Miej na uwadze, że Instagram stale ewoluuje. W momencie gdy pojawia się oficjalna aktualizacja, zapoznaj się z nią, czytając podane w wyciągu informacje. Każdorazowo monitoruj zachodzące zmiany, by w razie potrzeby reagować.

- Wszelką dodatkową pomoc znajdziesz pod adresem **facebook.com/help/instagram**.

URZĄD OCHRONY DANYCH OSOBOWYCH

Warto wiedzieć...

(Nie) bezpieczeństwo urządzeń połączonych w sieci

Internet rzeczy.

Inteligentne urządzenia i zabawki łącząc się z Internetem (m.in. zegarki, lalki, roboty, tablety, drony) zbierają informacje i dane osobowe, które przesyłają za pomocą technologii Bluetooth lub Wi-Fi. Warto zwrócić uwagę na to, jakie informacje o nas są gromadzone za pośrednictwem takiego urządzenia i co możemy zrobić w celu ochrony naszej prywatności.

1. Sprawdź, jakie dane osobowe są niezbędne do korzystania z urządzenia.

Wiele urządzeń wymaga zarejestrowania w Internecie przy pomocy aplikacji. Zwracaj uwagę na zakres danych osobowych, które są wymagane do zarejestrowania się i korzystania z zabawki. Podawaj tylko te dane osobowe, które są konieczne.

2. Łącz zabawkę tylko z zaufanymi sieciami Wi-Fi.

Jeśli połączysz się z niezabezpieczoną siecią Wi-Fi, z powodu braku odpowiednich zabezpieczeń osoba nieuprawniona może uzyskać dostęp do przekazywanych przez Ciebie danych, za pomocą połączenia z Bluetooth lub Wi – Fi.

3. Minimalizuj liczbę udostępnianych danych.

Zwracaj uwagę na to kogo i co nagrywasz podczas używania urządzenia. Sprawdź, czy można usunąć zachowane informacje w dowolnym momencie.

4. Zapoznaj się z informacjami od producenta.

Sprawdź, gdzie będą przechowywane Twoje dane i kto będzie miał do nich dostęp. Spersonalizuj ustawienia domyślne łączenia i zarządzaj ustawieniami zabezpieczeń. Zwracaj uwagę na to czy producent często aktualizuje oprogramowanie dotyczące zabezpieczeń. Zastosuj silne hasło dostępu lub PIN do urządzenia.

5. Pilnuj zabawki.

W przypadku zgubienia lub kradzieży zabawki, udostępnione dane staną się łatwo dostępne dla osób postronnych np. wizerunek, nagrania audio/wideo, dane o zdrowiu i inne dane.

7. Wyłączaj zabawkę, gdy nie jest używana.

Wyłączenie zabawki spowoduje ograniczenie dostępu do danych z zewnątrz i zbierania danych przez urządzenie, gdy z niego nie korzystamy. Zadbaj też, aby kamera i mikrofon były wyłączone, kiedy ich nie używasz.

8. Usuń dane, gdy zabawka nie będzie potrzebna.

Przywróć urządzenie do stanu fabrycznego i usuń konto w serwisie producenta, gdy nie będziesz już korzystać z zabawki.

URZĄD OCHRONY DANYCH OSOBOWYCH

Warto wiedzieć…

Jakie sztuczki sprawiają, że nasze działania w sieci zagrażają naszej prywatności?

Deceptive design patterns (ang. zwodnicze wzorce projektowe) to interfejsy wdrażane na platformach mediów społecznościowych, stronach internetowych i aplikacjach, które powodują, że użytkownicy podejmują niezamierzone, niechciane i potencjalnie szkodliwe decyzje dotyczące przetwarzania ich danych osobowych.

Przyczyny naszych błędnych decyzji w sieci:

1. Przeciążenie treścią (ang. overloading): przytłoczenie dużą liczbą próśb np. o wyrażenie zgody na przetwarzanie naszych danych osobowych.
2. Pomijanie (ang. skipping): Celowe ukrywanie w interfejsie strony komunikatu dotyczącego wyrażenia zgód na przetwarzanie danych, po to abyśmy zapomnieli lub nie myśleli o aspektach związanych z ochroną danych.
3. Wpływanie (ang. stirring): wywieranie na nas wpływ poprzez emocjonalną presję, lub zachęty w celu udzielenia zgody na przetwarzanie naszych danych osobowych. Na przykład podczas korzystania z aplikacji, czy strony internetowej klikamy w okienko „odmowy" i pojawiają się hasła typu: „Nie chcesz być zdrowy!", „Nie chcesz oszczędzić!"
4. Utrudnianie (ang. obstructing): utrudnianie lub blokowanie możliwości uzyskiwania informacji o naszych danych lub sposobie zarządzania danymi np. poprzez ukrywanie informacji o sposobie przetwarzania danych osobowych w trudno dostępnych zakładkach strony.
5. Niespójność (ang. fickle): utrudnianie poruszania się po różnych narzędziach służących kontroli ochrony danych oraz zrozumienia celu ich przetwarzania np. niejasno sformułowane komunikaty, po przeczytaniu których użytkownik tak naprawdę nie wie, w co powinien kliknąć.
6. Pozostawienie w niewiedzy (ang. left in the dark): projektowanie interfejsu w sposób ukrywający informacje lub narzędzia służące kontroli ochrony danych lub pozostawianie użytkownika w niepewności np. czy dane są udostępniane innym podmiotom, w jaki sposób dane są przetwarzane czy, i jaki rodzaj kontroli możemy mieć nad naszymi danymi.

Warto poświęcić odrobinę uwagi i chwilę swojego czasu, żeby zadbać o swoją prywatność. Mamy prawo wiedzieć jakie dane osobowe są gromadzone i w jaki sposób są przetwarzane. Nasza zgoda powinna być świadoma i dobrowolna. Świadomość stosowania zwodniczych wzorców projektowych może pomóc nam lepiej zarządzać naszymi danymi w sieci.

URZĄD OCHRONY DANYCH OSOBOWYCH

Fiszki

Deceptive design patterns (ang. zwodnicze wzorce projektowe) to interfejsy i doświadczenia użytkowników wdrażane na platformach mediów społecznościowych, stronach internetowych i aplikacjach, które powodują, że użytkownicy podejmują niezamierzone, niechciane i potencjalnie szkodliwe decyzje dotyczące przetwarzania ich danych osobowych.

Interfejs (interface) zasady łączenia ze sobą i współpracy dwóch różnych urządzeń lub programów; też: urządzenie lub program realizujące te zasady.
interfejs użytkownika program umożliwiający współpracę użytkownika z oprogramowaniem komputera.

Warto wiedzieć

NIEZABEZPIECZONA KAMERA I MIKROFON CO POWINNIŚMY WIEDZIEĆ!

Zarówno nauczyciele, jak i uczniowie spędzają obecnie wiele godzin przed ekranami komputerów, laptopów, tabletów, smartfonów, już nie tylko w ramach czasu przeznaczonego na rozrywkę, ale w dużej mierze na naukę i obowiązki szkolne czy zawodowe.

Pamiętajmy jednak, żeby świadomie i rozsądnie korzystać z usług społeczeństwa informacyjnego, biorąc szczególnie pod uwagę ochronę swojej prywatności i osób bliskich. Informacje w sieci bardzo szybko mogą zostać zapisane, utrwalone oraz przekazane, a więc przetwarzane przez innych użytkowników, np. w postaci nagrania audio-wideo.

Nieuprawnione zdobycie dostępu do kamery internetowej bądź mikrofonu nie jest wyjątkowo trudne, głównie z powodu podstawowych, standardowych zabezpieczeń (jak w przypadku większości urządzeń połączonych z siecią w domyślnych konfiguracjach producentów). Oznacza to, że przy niewielkim nakładzie pracy osoba niepożądana może w trybie ciągłym podglądać obraz z takiej kamery czy podsłuchiwać użytkownika danego sprzętu. W dalszej kolejności użytkownik ten może m.in. stać się ofiarą szantażu, ośmieszenia czy innych niezgodnych z prawem działań wykorzystujących jego tożsamość i informacje o nim.

Chrońmy swoje dane i prywatność poprzez świadome decyzje oraz działania w cyberprzestrzeni.

Dlatego warto wiedzieć, że:

- ważna jest ochrona komputera poprzez instalowanie programów zabezpieczających, systematyczną aktualizację wszystkich aplikacji oraz używanie silnych haseł;

- kamera powinna być ustawiona w taki sposób, aby nie obejmowała swoim zasięgiem niepożądanych osób trzecich i przestrzeni, której nie chcesz pokazywać rozmówcom;

- wystarczy chwila nieuwagi, by zainfekować komputer bądź telefon, a przy tym, dając cyberprzestępcy dostęp do Twojego urządzenia i wszystkich zgromadzonych danych, dlatego bądźmy ostrożni, otwierając linki bądź załączniki otrzymane od nieznanego nadawcy;

- nie zapominajmy też o coraz popularniejszych domowych urządzeniach, które są stale podłączone do Internetu i umożliwiają nam np. zdalne wykonywanie jakiś codziennych czynności, one także często mają wbudowane kamery i mikrofony.

Zatem co zrobić z kamerką i mikrofonem…
Jednym z rozwiązań chroniącym nasz wizerunek oraz prywatność jest dezaktywacja kamerki wraz z mikrofonem w menedżerze urządzeń. Należy wtedy pamiętać, aby je uruchamiać tylko wtedy, gdy będziemy chcieli z nich ponownie skorzystać.
Inną możliwością jest zasłonięcie kamerki internetowej w czasie, gdy nie potrzebujemy z niej korzystać. Możemy to zrobić za pomocą nieprzezroczystej taśmy klejącej, karteczki samoprzylepnej czy specjalnej do tego osłonki.

Warto wiedzieć...

Bezpieczeństwo w sieci czyli jak zadbać o siebie?

Po(d)ręcznik internauty

Nowe technologie mają wpływ na nasze życie. Należy jednak poznać współczesne zagrożenia, aby świadomie i bezpiecznie korzystać z sieci. Podpowiadamy, jak zadbać o siebie i zwiększyć swoje bezpieczeństwo oraz zyskać większą kontrolę nad danymi osobowymi w Internecie, aby nie stały się łatwym łupem przestępców.

1. ZADBAJ O ZRÓŻNICOWANE I SILNE HASŁA LOGOWANIA

Nie zaleca się zapamiętywania haseł w pamięci przeglądarki lub w aplikacji na urządzeniu.
Jeśli dowiesz się o wycieku danych z portalu, natychmiast zmień hasło dostępu;

2. DWUSKŁADNIKOWE ZABEZPIECZENIE KONTA

Samo hasło to często zbyt mało, aby ochronić dostęp do naszego konta np. w serwisie społecznościowym, banku, w sklepie internetowym czy w państwowej usłudze zdrowotnej. Warto do logowania dodać drugi składnik (np. kod przekazany przez email, sms), który dodatkowo chroni nasze konto przed dostępem osób niepowołanych. W ten sposób znacznie podniesiemy poziom bezpieczeństwa tego konta;

3. DOPASUJ USTAWIENIA PRYWATNOŚCI KONTA

Sprawdź domyślne ustawienia prywatności konta w mediach społecznościowych. Ustaw je tak, aby dostęp do prywatnych informacji, danych osobowych, zdjęć, miały wyłącznie zaufane osoby. Rozważ także, czy Twój profil powinien być widoczny dla zewnętrznych wyszukiwarek;

4. UWAŻAJ, JAKIMI INFORMACJAMI, ALE TEŻ ZDJĘCIAMI LUB FILMAMI, DZIELISZ SIĘ Z INNYMI

Pamiętaj, że osoba której zdjęcia zamieszczasz, powinna wyrazić na to zgodę. Nie publikuj zdjęć intymnych, ośmieszających czy zdradzających zbyt wielu informacji o Tobie i osobach bliskich. Chroń dane, które podlegają szczególnej ochronie m.in. dane o zdrowiu, nałogach, poglądach politycznych czy orientacji seksualnej;

5. NIE UJAWNIAJ ZBYT WIELU INFORMACJI O SOBIE

Minimalizuj liczbę informacji o sobie i swoich danych osobowych udostępnianych w Internecie. Uważaj na zamieszczenie zdjęć/nagrań wraz danymi o lokalizacji. Nie zamieszczaj zdjęć dokumentów np. legitymacji szkolnej, dowodu tożsamości, karty płatniczej, świadectwa szkolnego czy prawa jazdy;

6. UWAŻAJ NA ZAPROSZENIA OD NIEZNANYCH UŻYTKOWNIKÓW

Zachowaj ostrożność przy zawieraniu nowych znajomości w sieci. Pamiętaj też, że ktoś obcy może się podszyć za osobę Ci znaną, po przejęciu jego konta np. w mediach społecznościowych;

7. UWAŻAJ NA TZW. PHISHING i SZKODLIWE OPROGRAMOWANIE

Oszuści wyłudzają dane osobowe z pomocą socjotechniki. Próbują nakłonić nas do podania naszego loginu i hasła na fałszywej stronie internetowej, która do złudzenia przypomina np. stronę logowania do portalu społecznościowego, maila czy konta w banku. Oszuści wykorzystują również ankiety w mediach społecznościowych, oferty pieniędzy za reklamę czy wykonane szczepienia. Mogą w ten sposób przejąć kontrolę nad kontem użytkownika;

8. WERYFIKUJ, KTO JEST PRAWDZIWYM NADAWCĄ WIADOMOŚCI E-MAIL

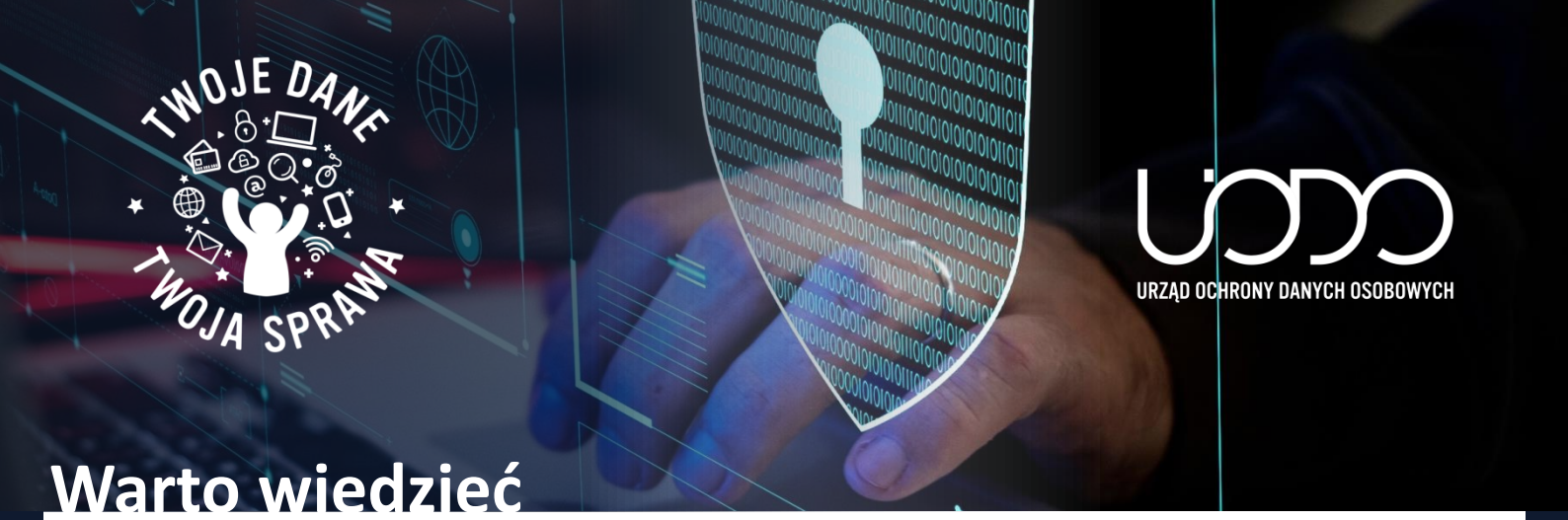
Zwracaj uwagę na adres mailowy, z którego została wysłana wiadomość, czy na pewno pochodzi od zaufanego nadawcy. Często w fałszywych mailach występują błędy np. w nazwie domeny. Oryginalna strona instytucji może mieć domenę z końcówką „.pl", a nadawca fałszywego maila korzysta z domeny np. „.com";

9. UWAŻAJ NA PUBLICZNE LUB NIEZABEZPIECZONE POŁĄCZENIA INTERNETOWE

Nie loguj się do serwisów społecznościowych oraz kont podczas korzystania z otwartych sieci tj. takich do których dostęp nie jest zabezpieczony hasłem, albo do których dostęp posiada większa lub niedająca się określić liczba użytkowników.

Dbajmy o siebie i swoje bezpieczeństwo. Dobre praktyki, powinny stać się nawykiem każdego internauty. O tym warto pamiętać nie tylko od święta.

URZĄD OCHRONY DANYCH OSOBOWYCH



Warto wiedzieć

Portale społecznościowe – 8 wskazówek pozwalających chronić prywatność

Portale społecznościowe (w tym wbudowane w nie komunikatory) stanowią stały element codzienności wielu z nas, a już ponad wszelką wątpliwość – uczniów. Granica wieku, od którego można korzystać z usług społeczeństwa informacyjnego wynosi 16 lat, natomiast przed ukończeniem tego wieku, dzieci mogą posługiwać się nimi za zgodą rodziców. Korzystanie z serwisów społecznościowych może sprawić wiele radości, ale też wiązać się z zagrożeniami dla naszej prywatności i ochrony danych osobowych.

Pamiętajmy, że dane osobowe udostępniane w social mediach to nie tylko imię, nazwisko, ale również szeroki zakres danych, takich jak: nazwa szkoły, nick, czy geolokalizacja naszych urządzeń mobilnych zapisywana na przykład w metadanych zdjęć (obok innych ważnych danych, jak data i czas ich wykonania). Danymi osobowymi może być także nasza aktywność w mediach: polubienia i komentarze pod konkretnymi postami, ale do szczególnej kategorii danych osobowych należą informacje o naszym zdrowiu, wyznaniu czy poglądach politycznych.

Świadomość ryzyka daje możliwość ochrony przed ewentualnymi zagrożeniami. Dlatego, korzystając z tego typu portali, warto pamiętać o kilku istotnych wskazówkach:

1. **Zadbaj o zróżnicowane i silne hasła logowania**. Hasło powinno być trudne do odgadnięcia i zawierać duże/małe litery, cyfry oraz znaki specjalne. Nie zaleca się zapamiętywania haseł w pamięci przeglądarki lub w aplikacji na urządzeniu. Nie należy także używać tej samej nazwy użytkownika w połączeniu z identycznym hasłem we wszystkich aplikacjach, z których korzystasz;
2. **Dopasuj ustawienia prywatności konta.** Ustaw je tak, aby dostęp do prywatnych informacji, danych osobowych, zdjęć, komentarzy miały jedynie zaufane osoby, będące w gronie Twoich znajomych. Rozważ także, czy Twój profil powinien być widoczny dla zewnętrznych wyszukiwarek;
3. **Uważaj, jakimi informacjami, ale też zdjęciami lub filmami, dzielisz się z innymi.** Przykładowo, publikowanie zdjęć, swoich i najbliższych, wystawione jest na ocenę innych osób, a ewentualna ich reakcja i komentarze mogą okazać się raniące, dokuczliwe, a nawet wulgarne. Pamiętaj, że osoba której zdjęcia zamieszczasz – powinna być, co najmniej poinformowana o tym fakcie. Raz opublikowana informacja, treść bądź fotografia może pozostać w cyberprzestrzeni już na zawsze, a konsekwencje złych wyborów ciągnąć się latami;
4. **Nie ujawniaj zbyt wielu informacji o sobie.** Social media nie są odpowiednimi miejscami do dzielenia się danymi/informacjami takimi, jak adres zamieszkania, numer telefonu czy miejsce pracy rodziców. Uważaj na zamieszczenie zdjęć/nagrań pozwalających osobie nieznajomej zlokalizować miejsce Twojego pobytu. Nie zamieszczaj zdjęć np. legitymacji szkolnej, dowodu tożsamości, karty płatniczej, druków zawierających dane osobowe, kart pokładowych czy prawa jazdy. Należy mieć świadomość, że dane osobowe/kontaktowe mogą pozyskać przestępcy, którzy zechcą wykorzystać je przeciwko Tobie lub Twoim najbliższym;
5. **Uważaj na zaproszenia od nieznanych użytkowników.** Bądź ostrożny i nie akceptuj automatycznie zaproszeń do grona znajomych lub obserwowania od obcych osób. Osoba podająca się za Twojego rówieśnika, może okazać się w rzeczywistości zupełnie kimś innym, dlatego należy być ostrożnym przy zawieraniu nowych znajomości w sieci. Pamiętaj też, że ktoś obcy może się podszyć także za Twojego bliskiego, przejmując wcześniej jego tożsamość w sieci.
6. **Uważaj na tzw. phishing**. Jest to jedno z najbardziej niebezpiecznych działań zmierzających do kradzieży loginów i haseł, które dotyczy również portali społecznościowych. Hakerzy rozsyłają odsyłacze do fałszywych serwisów społecznościowych, do złudzenia przypominających te, z których korzystasz na co dzień. Po kliknięciu w taki link i wprowadzeniu danych do logowania cyberprzestępcy mogą uzyskać dostęp do Twoich danych;
7. **Uważaj na szkodliwe oprogramowanie, które może być przesyłane za pomocą komunikatorów**. Zachowaj czujność zanim otworzysz otrzymany link, upewniając się, że pochodzi z zaufanego źródła. Hakerzy, wykorzystując nieuwagę użytkownika, rozsyłają linki do zainfekowanych stron lub dodają złośliwe rozszerzenia do przeglądarek, dzięki czemu mogą przejąć kontrolę nad kontem użytkownika;
8. **Uważaj na publiczne lub niezabezpieczone połączenia internetowe.** Nie loguj się do serwisów społecznościowych podczas korzystania z otwartych sieci, gdyż może to grozić udostępnieniem wrażliwych informacji cyberprzestępcom.

Warto wiedzieć

Użytkowanie Smarfona a ochrona naszej prywatności

Smartfon to przenośne urządzenie multimedialne łączące w sobie funkcje telefonu komórkowego i komputera przenośnego. Jest to często najbardziej osobiste urządzenie elektroniczne, którego używamy. Zabieramy go do szkoły, do pracy, na spotkania, a nawet jest tuż obok, gdy idziemy spać. Wykorzystując jego możliwości, używamy wielu aplikacji (akceptując przy tym regulaminy), przeglądamy Internet, wymieniamy wiadomości, korzystamy z serwisów społecznościowych, robimy zdjęcia, kręcimy filmiki, oraz pozwalamy na gromadzenie danych o naszym położeniu. Jednymi słowy, nasze urządzenie jest skarbnicą informacji o nas, naszych upodobaniach i stylu życia – „wie o nas" praktycznie wszystko.

Cyberprzestępcy dostrzegli ogrom możliwości, jakie dają smartfony, na nielegalne zdobycie naszych danych osobowych, poufnych informacji i innych ważnych treści, które przechowujemy w urządzeniach. Dlatego musimy być szczególnie czujni podczas używania swoich przenośnych urządzeń i jeszcze bardziej chronić własne dane osobowe, oraz szeroko pojętą prywatność.

Dlatego warto wiedzieć, jak chronić dane…

- **Blokuj ekran**. Ustawienie automatycznej blokady urządzenia i konieczność jego odblokowania za pomocą kodu PIN lub wzoru, ograniczy ryzyko dostępu do naszej prywatnej przestrzeni i możliwość kradzieży danych;
- **Systematycznie aktualizuj oprogramowanie urządzenia oraz korzystaj ze sprawdzonego programu antywirusowego.** Regularne skanowanie smartfona może wykryć zainfekowane pliki czy też niebezpieczne aplikacje;
- **Sprawdzaj uprawnienia aplikacji**. Przemyśl czy określona aplikacja powinna mieć dostęp, do zasobów takich jak galeria, kontakty, geolokalizacja, wiadomości, ale też czy godzisz się na dostęp do kamery i mikrofonu. Rozważ, czy ewentualny dostęp do zasobów smartfona ma być stały czy jedynie na czas działania aplikacji;
- **Zastosuj tryb prywatny**. Umożliwia on przeglądanie stron WWW bez zapisywania historii, plików cookie i wyszukiwanych fraz. Pamiętaj, że nie gwarantuje on pełnej anonimowości w sieci, ale pozwala na zwiększenie poziomu prywatności;
- **Uważaj na ładowanie przez kabel USB.** Bądź ostrożny, podłączając smartfon do obcego komputera lub gniazdka USB – może być to niebezpieczne i narazić Cię na kradzież danych lub zainfekowanie urządzenia. Warto posiadać kabel, który pozwala wyłącznie na ładowanie urządzenia, ale nie na przesył danych;
- **Rozważnie korzystaj z publicznych sieci bezprzewodowych Wi-Fi.** Pamiętaj, że nazwa sieci Wi-Fi może być ustalona dowolnie i celowo wprowadzać w błąd, sugerując, że należy np. do Twojej szkoły, a tak naprawdę być siecią uruchomioną w celach przestępczych. Dlatego staraj się korzystać wyłącznie z serwisów oraz usług z zaszyfrowanym ruchem, np. w przeglądarce będą to połączenia zabezpieczone za pomocą protokołu HTTPS. Możesz też rozważyć wykorzystanie sprawdzonej aplikacji VPN;
- **Pomyśl nad kupnem folii prywatyzującej.** Naklejenie tego typu filtru na ekran, uniemożliwia osobom będącym w pobliżu podglądanie wyświetlanych w smartfonie treści. Oznacza to tyle, że osoba siedząca obok nas, np. w pociągu, w poczekalni, nie zobaczy co czytamy i jakie wykonujemy operacje na naszym urządzeniu;
- **Systematyczne czyść urządzenie**. Kasuj „śmieci systemowe" - aplikacje i dane, z których już nie korzystasz. Pamiętaj również o kasowaniu historii przeglądania i zamykaniu zbyt wielu otwartych wcześniej kart (w niektórych nadal możemy być zalogowani do stron WWW). Zwiększy to bezpieczeństwo, jak również szybkość działania urządzenia;
- **Pamiętaj o wylogowaniu się z serwisów WWW.** Spowoduje to przerwanie uwierzytelnionego połączenia ze stroną, a nawet usunięcie danych logowania, np. w postaci plików cookie, zmniejszając przy tym możliwość kradzieży Twojej tożsamości;
- **Bądź przezorny.** Zabezpiecz się na wypadek zagubienia/kradzieży smartfona. Warto włączyć usługi lokalizujące urządzenie oraz umożliwiające zdalne usunięcie danych czy też zresetowanie do fabrycznych ustawień;
- **Zadbaj o kopię zapasową.** Twórz regularnie lokalną kopię danych lub korzystaj z backupu w chmurze. Dzięki temu szybko odzyskasz dostęp do ważnych danych w przypadku awarii, zgubienia lub kradzieży telefonu;
- **Gdy chcesz sprzedać/oddać telefon zwróć szczególną uwagę, aby Twoje poufne dane nie dostały się w ręce obcej osoby, a zwłaszcza cyberprzestępców.** Oprócz procesu przywrócenia ustawień fabrycznych urządzenia, warto włączyć opcję szyfrowania danych, znajdującą się w ustawieniach prywatności.

Warto wiedzieć...

Snapchat

korespondencja obrazem

Aplikacja Snapchat umożliwia komunikowanie się jej użytkownikom głównie za pomocą wyświetlanych jednorazowo zdjęć (*snapów*). Użytkownik sam decyduje, ile sekund trwa przesłana przez niego projekcja. Zdjęcia można też zamieszczać w czasowych, domyślnie publicznych relacjach (*stories*).

Jeśli zdecydujesz się na używanie aplikacji Snapchat, pamiętaj o dbaniu o swoją prywatność – zgodnie z poniższymi zasadami:

- Nie zamieszczaj zdjęć swojego najbliższego otoczenia – domu, pokoju, klasy w szkole. Pamiętaj o niepublikowaniu wizerunku osób, które nie wyraziły na to zgody. Należy wziąć także pod uwagę, że zakrywanie twarzy lub innych obszarów zdjęcia za pomocą wbudowanych grafik Snapchata, nie zapewnia prywatności występującym na zdjęciu osobom. Oprogramowanie firm trzecich potrafi takie elementy graficzne usunąć, odkrywając oryginalną zawartość fotografii.

- Nakładając filtry/nakładki na zdjęcie, staraj się ograniczać te dedykowane lokalizacji. Jeśli używasz *Snap Mapy*, ogranicz swoją widoczność do minimum. W zakładce „ustawienia" skonfigurujesz grupę odbiorców mogących wyświetlać Twoją lokalizację. Pamiętaj, by nigdy nie zdradzać nieznajomym, gdzie aktualnie przebywasz!

  > Aplikacja mobilna: ***ustawienia → usługi dodatkowe/prywatność***

- Zwracaj uwagę na powiadomienia wewnątrz aplikacji. Jeśli odbiorca zrobi zrzut ekranu (*screenshot*), Snapchat poinformuje o tym nadawcę, wysyłając stosowne powiadomienie. Otrzymasz wówczas komunikat „*nazwa użytkownika* zrobił(a) zrzut ekranu". Jeśli wzbudza to Twoje podejrzenia – reaguj!

- Nigdy nie podawaj nieznajomym swoich danych; nie wysyłaj zdjęć, filmów, numerów telefonu, adresów. Jeśli nie znasz kogoś osobiście, nie dodawaj go do grona znajomych.

- Pamiętaj o tym, by nie udostępniać więcej danych, niż jest to konieczne do korzystania z aplikacji.

- Stwórz trudne do złamania hasło. Powinno składać się z dużych i małych liter, być długie, zawierać liczby lub inne znaki. Ponadto wskazane jest używanie uwierzytelnienia dwuetapowego.

  > Aplikacja mobilna: ***ustawienia → moje konto → hasło/uwierzytelnienie dwuetapowe***

- W ustawieniach dokonasz istotnych zmian w zakresie ochrony danych osobowych – wyczyścisz zapis rozmów i historię wyszukiwania.

  > Aplikacja mobilna: ***ustawienia → usługi dodatkowe/prywatność/czynności na koncie***

- Wyloguj się po każdej zakończonej sesji. Zapewni to maksymalną ochronę konta.

- Monitoruj zachodzące w aplikacji zmiany. Zapoznawaj się na bieżąco z informacjami o aktualizacji Snapchata. Ich treść powinna być dla Ciebie zrozumiała. Jeśli nie jest, skonsultuj się z rodzicem albo opiekunem.

- Systematycznie aktualizuj system i oprogramowanie urządzenia oraz korzystaj ze sprawdzonego programu antywirusowego. Regularne skanowanie smartfona może wykryć zainfekowane pliki, niebezpieczne aplikacje czy też źle zabezpieczone sieci Wi-Fi.

URZĄD OCHRONY DANYCH OSOBOWYCH

Warto wiedzieć...

Świadomi rodzice to bezpieczne dzieci.

Rozmawiajmy o ochronie prywatności w sieci.

Nasze działania w sieci budują naszą cyfrową tożsamość. Decydujący wpływ na ochronę prywatności mają podjęte decyzje i dokonywane wybory, nie tylko młodych użytkowników Internetu, ale również ich rodziców i opiekunów. Ważnym wsparciem w procesie nabywania odpowiednich nawyków dotyczących ochrony danych osobowych przez dzieci i młodzież jest rozmowa na temat bezpiecznego korzystania z Internetu.

Podczas rozmów z dziećmi, pamiętajmy o podjęciu kilku ważnych kwestii, o których mowa poniżej.

- ❑ Budujmy świadomie swoją tożsamość cyfrową, **ograniczając liczbę informacji udostępnianych o sobie.** Należy zwracać uwagę na ochronę swojej prywatności w sieci, ale także prywatności osób bliskich.

- ❑ **Ograniczajmy się do udostępniania danych, które są niezbędne do skorzystania z usługi czy aplikacji**. Kontrola naszych danych wymaga pewnej refleksji przed udostępnieniem informacji w mediach społecznościowych, na forach internetowych czy zwykłych stronach WWW, np. przy wypełnianiu formularzy, rejestracji do różnych usług czy platform.

- ❑ **Wszystko, co robimy w sieci pozostawia cyfrowe ślady.** Kiedy korzystamy z Internetu, nie jest możliwe zachowanie pełnej anonimowości. Strony internetowe zbierają dane i gromadzą informacje o nas, również w sposób automatyczny m.in.: w celach statystycznych.

- ❑ **Nie publikujmy opinii i komentarzy pod wpływem emocji** – to również informacje, które mają wpływ na nasz wizerunek w sieci. Nie zawsze możemy sprostować informacje powiązane z naszym nickiem lub/czy adresem IP, gdy są nieprawdziwe lub nieaktualne, albo po prostu je usunąć, mimo że co do zasady przysługuje nam takie prawo.

- ❑ **Sprawdzajmy domyślne ustawienia prywatności w serwisach, z których korzystamy**, aby ograniczyć ilość informacji o nas, które będą powszechnie dostępne.

- ❑ **Sprawdzajmy, kto i jakie informacje o nas gromadzi w przypadku różnych czynności,** np. korzystania z aplikacji, robienia zakupów. Mamy prawo wiedzieć, kto i dlaczego, a także w jakim celu zbiera i wykorzystuje informacje o nas.

- ❑ **Stosujmy techniczne zabezpieczania, aby utrudnić dostęp innych osób do urządzeń oraz serwisów społecznościowych**, z których korzystamy, np. kody pin, silne hasła czy dwuetapowe uwierzytelnienie. Ważna jest również ochrona urządzenia poprzez instalowanie programów zabezpieczających oraz systematyczna aktualizacja aplikacji.

- ❑ **Sprawdzajmy domyślne ustawienia kamery internetowej bądź mikrofonu** w urządzeniach podłączonych do sieci, aby ograniczyć do nich dostęp osobom postronnym bez naszej wiedzy. Jednym z rozwiązań jest dezaktywacja kamery czy mikrofonu w menadżerze urządzenia i uruchamianie ich tylko wtedy, gdy będziemy z nich korzystali.

- ❑ Ustalajmy wspólnie z dziećmi zasady bezpiecznego korzystania z Internetu i zwracajmy szczególną uwagę dzieci na **zasadę ograniczonego zaufania**, zarówno do treści zamieszczanych w sieci, jak również osób, poznanych w Internecie.

Ważne jest podejmowanie świadomych decyzji w sieci oraz rozmowa i wsparcie rodziców, którzy mają prawo i obowiązek dbać o bezpieczeństwo swoich dzieci.

URZĄD OCHRONY DANYCH OSOBOWYCH

Warto wiedzieć

TikTok - pozornie nieszkodliwa aplikacja społecznościowa

skierowana głównie do nastolatków, która umożliwia użytkownikom tworzenie i udostępnianie krótkich filmów ze śpiewem i tańcem. Udostępnione w aplikacji wideo można wzbogacić o wiele filtrów i nakładek. Klip wyświetla się zapętlony, a fani (obserwujący) mogą go lajkować i komentować.

Aplikacja publikuje wszystkie treści (nagrania) bez żadnej kontroli nad jej zawartością, umożliwiając publiczny dostęp wszystkim użytkownikom aplikacji. Niesie to za sobą ryzyko rozpowszechniania nagrania, a więc i dostępu do nieodpowiednich dla uczniów treści, takich jak pornografia, przemoc czy materiały szerzące nienawiść i wulgarne treści.

Coraz częściej słyszy się także o zarzutach stawianych aplikacji TikTok związanych z dyskryminacją. Jak się okazuje, nie każdy użytkownik może czerpać równą radość z obecności na tej platformie: aplikacja filtruje treści według własnych kryteriów „atrakcyjności".

Dlatego tak ważna jest rozwaga i czujność także wśród uczniów, aby wiedzieli, jakie treści i komu mogą udostępniać. Aby zwiększyć bezpieczeństwo uczniów i ochronę ich prywatności podczas korzystania z aplikacji, warto przekazać im następujące wskazówki:

- włącz ustawienia *Konto prywatne* – od tej pory konto będzie niedostępne dla osób spoza listy kontaktów (pamiętaj, by w opisie nie podawać swoich danych osobowych – jest on zawsze widoczny dla pozostałych użytkowników, nawet, gdy konto jest ustawione jako prywatne);

- wyłącz funkcje *Umożliw innym znalezienie mnie*, zwiększy to dodatkowo poziom bezpieczeństwa. Po wyłączeniu tej opcji nikt nie będzie mógł wyszukać konkretnego profilu;

- loguj się za pomocą systemu logowana w aplikacji TikTok. Staraj się nie korzystać z logowania za pomocą innych mediów społecznościowych;

- nie ujawniaj (w ustawieniach aplikacji) lokalizacji użytkownika oraz staraj się nie prowadzić transmisji na żywo np. z domu;

- zachowaj ostrożność, przyjmując nieznajomych do grona obserwatorów i nie odpowiadaj na prośby o numery telefonów, adresy, zdjęcia lub filmy;

- w ustawieniach prywatności zablokuj funkcję pobierania filmów – mogą one być wykorzystane przez innych użytkowników w nieuprawniony sposób;

- rodzice i opiekunowie mogą skorzystać z trybu bezpieczeństwa, dzięki któremu mają możliwość monitorowania profilu dziecka, a także nadawania kontom statusu prywatności, blokowania nieuprawnionym osobom dostępu do lokalizacji, decydowania o czasie korzystania z aplikacji oraz ograniczenia dostępu do nieodpowiednich treści.

Przede wszystkim rekomendujemy rozmowę z uczniem na temat funkcjonowania mediów społecznościowych i wyjaśnienie, jakie mogą być konsekwencje niewłaściwego ich używania.

Warto wiedzieć...

Uważni w cyberprzestrzeni

Jak bezpiecznie przeglądać strony w Internecie?

Zachowaj ostrożność w przypadku udostępniania swoich danych osobowych w cyberprzestrzeni. Aby uniknąć różnych metod oszustwa lub nieuczciwego wykorzystania informacji o Tobie, istotne jest wyrobienie w sobie nawyku sprawdzania przekazywanych informacji lub konsultowania się z zaufanymi osobami przed podjęciem działań w sieci, które mogłyby potencjalnie Tobie zaszkodzić. Uważaj, aby nie udostępniać danych osobowych na fałszywych stronach. Jak więc bezpiecznie przeglądać strony w Internecie i rozpoznać oznaki cyberataków, aby uniknąć zainfekowania złośliwym oprogramowaniem urządzeń oraz utraty danych osobowych? Oto kilka podpowiedzi, na co zwracać uwagę.

WSKAZÓWKI DOTYCZĄCE BEZPIECZNEGO PRZEGLĄDANIA W INTERNECIE

⊗ Nie wprowadzaj żadnych danych na stronach, które nie stosują szyfrowania danych, tj. nie posiadają na początku adresu skrótu https oraz ikony zamkniętej kłódki w pasku adresu przeglądarki;

⊗ Zawsze upewnij się, że na przeglądanej stronie internetowej znajduje się polityka prywatności, która zawiera informacje o administratorze (dane kontaktowe) i zasady ochrony danych osobowych;

⊗ Zainstaluj oprogramowanie zabezpieczające do blokowania nietypowej aktywności w przeglądarce, tj. wyskakujących okienek z ofertami/plikami/programami do pobrania;

⊗ W przypadku znalezienia się na stronie internetowej, która wzbudza Twoje podejrzenia, nie podawaj danych osobowych np. danych logowania w serwisie społecznościowym czy danych do poczty e-mail itp.;

⊗ Nie ufaj informacjom o możliwych wygranych czy nagrodach. Nie podawaj danych osobowych w celu odebrania wygranej, a także nie pobieraj dodatkowych aplikacji w celu odebrania wygranej.

CECHY CHARAKTERYSTYCZNE DLA NIEBEZPIECZNYCH STRON INTERNETOWYCH

1. ZNIEKSZTAŁCENIE TREŚCI

Atak ten jest łatwy do zidentyfikowania. Oszuści zmieniają zawartość witryny za pomocą własnej nazwy, logo czy obrazów zawierających treści przyciągające uwagę np. prowokacyjnych reklam.

2. OKIENKA ZAWIERAJĄCE ODNOŚNIKI

Występowanie „wyskakujących" okienek, które zawierają informacje niezwiązane z zawartością przeglądanej strony. Kliknięcie okienka może spowodować pobranie złośliwego oprogramowania.

3. MALVERTISING

Złośliwe reklamy, które łatwo dostrzec promują „cudowne" uzdrowienia lub skandale z celebrytami. Zwykle wyglądają nieprofesjonalnie i zawierają błędy ortograficzne czy gramatyczne. Takie reklamy, ale także te które pasują do Twojej historii przeglądania, mogą również zawierać złośliwe oprogramowanie.

4. ZESTAWY DO PHISHINGU

To są strony naśladujące najczęściej odwiedzane strony w sieci np. strony banków, portali społecznościowych, aby nakłonić użytkowników do podania danych osobowych nieuprawnionym osobom. Zwracaj uwagę, czy nazwa strony widoczna w przeglądarce (adres URL) nie zawiera błędów gramatycznych, czy też np. innego rozszerzenia.

5. ZŁOŚLIWE PRZEKIEROWANIE

Jeśli podczas wpisywania adresu URL następuje przekierowanie na inną stronę, która wygląda podejrzanie, nie przeglądaj takiej strony i uruchom ponownie przeglądarkę.

6. SPAM W WYSZUKIWARKACH

Pojawienie się nietypowych linków na stronie, często w sekcji komentarzy, jest prawdziwą oznaką spamu wyszukiwawczego.

7. ALERTY WYSZUKIWAREK I PROGRAMÓW ANTYWIRUSOWYCH

Popularne wyszukiwarki skanują witryny w poszukiwaniu złośliwego oprogramowania i ostrzegają o tym. Wbudowany moduł do sprawdzania witryn posiadają również niektóre programy antywirusowe. Ostrzeżenia te jednoznacznie wskazują, że strona jest zainfekowana złośliwym oprogramowaniem.

Źródło: https://vdai.lrv.lt/lt/naujienos/patarimai-kaip-apsaugoti-savo-asmens-duomenis-ir-finansus-karo-ukrainoje-metu-padaugejus-sukciavimo-atveju-internete

URZĄD OCHRONY DANYCH OSOBOWYCH

Warto wiedzieć, że...

Wyciek danych a ochrona prywatności w sieci.

Jak zadbać o swoje bezpieczeństwo?

Ogromna ilość informacji łatwo dostępnych w Internecie, to wystarczająca motywacja dla hakerów, aby dokonać ich kradzieży. Hasła są jak klucze do sejfu. Jeśli ktoś zdobędzie nasze hasło do danego portalu, może uzyskać dostęp do naszych prywatnych danych, dokonać przejęcia naszego konta w mediach społecznościowych, kradzieży naszej tożsamości czy transferu pieniędzy. Hasła są więc najbardziej pożądane, bo dzięki nim haker zdobywa dostęp do wielu naszych zasobów, w tym do innych danych osobowych, które może wykorzystać. Wyciek danych w Internecie, to poważne zagrożenie dla naszego bezpieczeństwa. Na co więc powinniśmy zwrócić szczególną uwagę, aby zminimalizować ryzyko? Co zrobić w sytuacji, kiedy dane zostały już zhakowane – podpowiadamy w kolejnej poradzie.

Jak zminimalizować ryzyko wycieku danych?

- **stosujmy silne hasło** – można w tym celu posłużyć się generatorem haseł;
- **stosujmy dwuetapowe logowanie** – jest to podwójne sprawdzenie tożsamości (uwierzytelnianie), które polega na podaniu loginu i hasła, a następnie potwierdzeniu logowania zazwyczaj zewnętrznym tokenem (np. kodem SMS). Zastosowanie takiego dodatkowego zabezpieczenia skutecznie ochroni przed atakami hakerskimi (phishingiem, przechwytywaniem sesji czy wyłudzeniem danych). Ponadto token nie zadziała podczas logowania na fałszywej stronie;
- **logujmy się na własnych urządzeniach**;
- **stosujmy zróżnicowane hasła** do różnych portali i systemów, w czym może pomóc nam manager haseł;
- **korzystajmy z zaufanego połączenia internetowego**, nigdy z publicznych hot spotów;
- **ograniczajmy uprawnienia aplikacji do logowania** za pomocą konta w portalu społecznościowym.

Co zrobić, gdy podejrzewamy, że nasze dane dostały się w niepowołane ręce?

- **zmieńmy hasło** najszybciej jak to możliwe, przy zachowaniu zasad tworzenia silnego hasła;
- zachowajmy szczególną **ostrożność przed atakami phishingowymi,** w tym celu nie otwierajmy załączników i linków od nieznanych osób, instytucji i firm, np. firm kurierskich, gdy nie zamawialiśmy przesyłki. Ataki te mogą się nasilić po wycieku danych kontaktowych;
- **nie udostępniajmy haseł i danych do logowania podczas rozmów telefonicznych z nieznanymi osobami**. Tak jak w przypadku metody na tzw. „wnuczka" czy „policjanta", oszuści mogą za pomocą różnych socjotechnik podszywać się pod inne osoby, dysponując informacjami z portalu. W ten sposób próbują wyłudzić kolejne dane, które umożliwią im dostęp do naszych kont lub urządzeń;
- **weryfikujmy autentyczność certyfikatu SSL** strony, na którą się logujemy. Można to sprawdzić, klikając w ikonę kłódki przy pasku adresu, rozwinąć szczegóły i zobaczyć, czy połączenie jest bezpieczne;
- **nie zapisujmy danych logowania w przeglądarce ani danych kart płatniczej lub kredytowej dla automatycznego wypełniania formularza danymi**. W żadnym wypadku nie podajemy nigdzie kodu dostępu, np. numeru PIN –- o ten element nikt nie ma prawa nas pytać, nawet konsultant instytucji bankowej;
- **nie wchodźmy na strony za pośrednictwem linków przesłanych pocztą elektroniczną czy komunikatorów od nieznanych nadawców czy takie które wydają nam się podejrzane.** To popularna metoda przestępców, aby przekierować użytkowników na fałszywe strony;
- zainstalujmy i utrzymujmy aktualność **zabezpieczenia antywirusowego i zapory w systemie.**

Zwracajmy szczególną uwagę na minimalizowanie liczby danych osobowych i informacji o nas, które udostępniamy w Internecie. Udostępniajmy tylko dane osobowe, w sytuacji kiedy to jest konieczne do realizacji usługi. A w sytuacji wycieku danych z portalu, koniecznie, niezwłocznie zmieniajmy hasło.

URZĄD OCHRONY DANYCH OSOBOWYCH

Warto wiedzieć…
Cookies czyli ciasteczka

Czym je się internetowe ciasteczka?

Cookies (z ang. ciasteczka) to małe pliki, wysyłane przez strony internetowe i zapisywane w pamięci przeglądarki internetowej na naszym urządzeniu (telefonie, komputerze czy tablecie). Ciasteczka to w istocie krótkie pliki tekstowe, zawierające ciągi liter i cyfr, które pozwalają stronie na rozpoznanie naszej przeglądarki. Pliki cookies w połączeniu z innymi informacjami mogą jednoznacznie identyfikować użytkownika sieci, a przez to możemy je uznać za **dane osobowe**.

Po zapisaniu ciasteczek, nasza przeglądarka staje się rozpoznawalna dla strony internetowej i dzięki temu możemy się do niej bezproblemowo logować, kontynuować wcześniej rozpoczęte wyszukiwania lub zakupy czy oglądać spersonalizowane treści i reklamy. Bez plików cookies niemożliwe byłoby też aktywowanie wielu internetowych usług, udział w konkursach czy głosowaniach w sieci.

Pamiętajmy, że mamy możliwość decydowania o tym, czy i jakie nasze ciasteczka będą zbierane. W momencie gdy odwiedzamy jakąś witrynę po raz pierwszy musimy **wyrazić zgodę na zbieranie wybranych typów ciasteczek**. Ustawienia ciasteczek możemy zmienić też w menu przeglądarki tak by ograniczyć ich ilość.

Trzy podstawowe typy ciasteczek to (opis typów znajduje się na fiszkach dołączonych do porady):

1. Ciasteczka sesyjne
2. Ciasteczka stałe
3. **Ciasteczka stron trzecich**

Korzystając z ciasteczek stron trzecich, firmy i strony internetowe mogą zbierać i analizować informacje o naszej lokalizacji, finansach, nawykach zakupowych i nie tylko. Dobrym nawykiem jest zatem ograniczenie plików cookies do niezbędnego minimum.

Usuwanie ciasteczek nie jest na co dzień konieczne, **ale należy to zrobić gdy użyczamy lub pozbywamy się naszego urządzenia**.

Gdy korzystamy z nieprzebranych zasobów sieci musimy być świadomi, że zostawiamy za sobą ślady, które mogą być wykorzystywane do tworzenia naszych profili marketingowych. Uważne obchodzenie się z internetowymi ciasteczkami może pomóc nam zabezpieczyć chociaż część naszej prywatności i zwiększyć naszą wolność wyboru.

URZĄD OCHRONY DANYCH OSOBOWYCH