**Bezpieczne korzystanie z Internetu**Internet stał się nieodłączną częścią naszej codzienności. To, co
jeszcze niedawno robiliśmy w sposób tradycyjny, dziś szybko i
sprawnie wykonujemy wirtualnie. Obecnie w sieci zrobimy zakupy,
posłuchamy muzyki, obejrzymy film, zapłacimy rachunki, napiszemy
list czy odbędziemy rozmowę z rodziną lub przyjaciółmi. Jest nieocenionym źródłem wiedzy, wymiany doświadczeń, miejscem
wirtualnych spotkań z innymi ludźmi. Pełni funkcję poznawczą, społeczną, rozrywkową. Wielość zalet wirtualnej rzeczywistości nie może jednak zakryć zagrożeń, które się w niej kryją. Warto więc poznać podstawowe zasady bezpiecznego korzystania z Internetu.

1.Strzeż się wirusów
Podstawą bezpiecznego korzystania z Internetu jest zainwestowanie w porządne [oprogramowanie antywirusowe](https://bezpiecznyinternet.edu.pl/co-to-jest-program-antywirusowy-i-jak-dziala/). Ustrzeże nas ono przed dużą ilością przykrych konsekwencji, które niesie za sobą ludzka nieostrożność i pomoże uchronić nasz komputer. Program antywirusowy zawczasu wykryje [złośliwe oprogramowanie](https://bezpiecznyinternet.edu.pl/co-to-jest-wirus-komputerowy-i-jak-dziala/) czy obecność wirusa i nie pozwoli im się zagościć w naszym komputerze, Niemniej jednak nawet posiadając najlepszy program do ochrony przed wirusami, warto z rozwagą pobierać pliki z sieci oraz nie otwierać nieznanych załączników w mailach oraz linków. Niestosowanie tego typu oprogramowania może spowodować, że przez wirusa stracimy ważne dane, zdjęcia i inne informacje, często dla nas bardzo ważne.

2. Chroń swoje dane
Nie należy podawać w sieci swoich danych osobowych. Nieuważne zgody na przetwarzanie danych osobowych lub na otrzymywanie informacji marketingowych mogą w konsekwencji prowadzić do tragicznych w skutkach wydarzeń jak kradzież tożsamości. Najczęściej takie dane jak imię, nazwisko i adres podajemy podczas zakupów w sieci. Co powinno wzbudzić nasz niepokój? Zbyt duża ilość wymaganych danych, niestandardowych przy zakupach – na przykład takich jak PESEL, adres zameldowania itp. Zaznaczenie zgody na przetwarzanie danych osobowych powoduje przede wszystkim utratę kontroli nad tym co stanie się z nimi w przyszłości. Dane gromadzone przez firmy są często odsprzedawane innym podmiotom gospodarczym, które nękają później ich właścicieli wielością ofert lub ankiet.
3. Uważaj na internetowe znajomości
Coraz częściej poznajemy ludzi przez Internet. W wirtualnej rzeczywistości można zawrzeć wartościowe i ciekawe znajomości. Pamiętajmy jednak, że nigdy nie wiadomo kto siedzi po drugiej stronie. Dlatego nie należy przesadzać z nadmierną wylewnością w takich relacjach, a na ewentualne spotkania umawiać się w miejscach publicznych. Anonimowość, którą daje wirtualna rzeczywistość staje się niekiedy płaszczem dla przestępców, złodziei oraz innych ludzi o nieczystych intencjach. Warto o tym pamiętać. Do wszelkich znajomości zawieranych w internecie należy podchodzić w ostrożnością, stosując zasadę ograniczonego zaufania.

4. Hasła i szyfrowanie to podstawa naszego bezpieczeństwa w sieci Nikomu pod żadnym pozorem nie należy podawać swoich [haseł](https://bezpiecznyinternet.edu.pl/jak-stworzyc-bezpieczne-haslo/). Powinny być one trudne do odszyfrowania i składać się ze skomplikowanej kombinacji dużych i małych liter, cyfr oraz znaków specjalnych. Powinniśmy wystrzegać się zabezpieczania różnych kont tym samym hasłem lub hasłem prostym i łatwym do odgadnięcia. Niezwykłą wagę należy przykładać przede wszystkim do ochrony kont bankowych, skrzynki mailowej, kont w serwisach społecznościowych, kont w pracy czy na uczelni. Czyli wszędzie tam, gdzie można odnaleźć swobodny dostęp do naszych danych wrażliwych, bazy zdjęć i innych informacji, które ktoś mógłby wykorzystać przeciwko nam. Jeśli na jakiejkolwiek stronie wyświetla nam się jej regulamin – warto go przeczytać. Warto zawsze sprawdzić wiarygodność strony, z której korzystamy oraz jej właściciela. Tutaj z pomocą przychodzi tak zwany certyfikat SSL – należy sprawdzać czy strona posiada to zabezpieczenie, szczególnie gdy się na niej logujemy.
5. Chroń dzieci przed niebezpieczeństwem w Internecie
Jeśli jesteś rodzicem pamiętaj o tym, że nie wolno dawać dzieciom całkowitej wolności w sieci. Mądrze ustawiona blokada rodzicielska uchroni je przed znakomitą większością wirtualnych niebezpieczeństw. Na bieżąco należy śledzić aktywność dziecka w sieci i niezwłocznie reagować jeśli cokolwiek nas zaniepokoi. Najważniejsze jest żeby dziecko wraz z nami poznawało wirtualny świat i nauczyło się z niego mądrze korzystać. Nic nie zastąpi rozmów z młodym człowiekiem na temat zagrożeń, które czają się w internecie, oraz uczulenie go na aspekty, o których powinien informować w razie potrzeby. Dziecięca naiwność jest często wykorzystywana przez cyberprzestępców, dlatego rolą rodziców jest przewidywać potencjalne zagrożenia i im zapobiegać. Zasady mądrego i ostrożnego korzystania z internetu, które sami stosujemy powinniśmy wpoić naszym pociechom.

Opracowała: Beata Brzezińska