SENIORZE
spotkajmy się w sieci

Antywirus i zaślepka?
Wszystko, co musisz wiedzieć o programach i narzędziach zwiększających Twoje bezpieczeństwo w sieci.
Poradnik dla seniora

04.

Partner kampanii:

WARSZAWSKI INSTYTUT BANKOWOŚCI

Fundusze Europejskie Polska Cyfrowa

KPRM

NASK

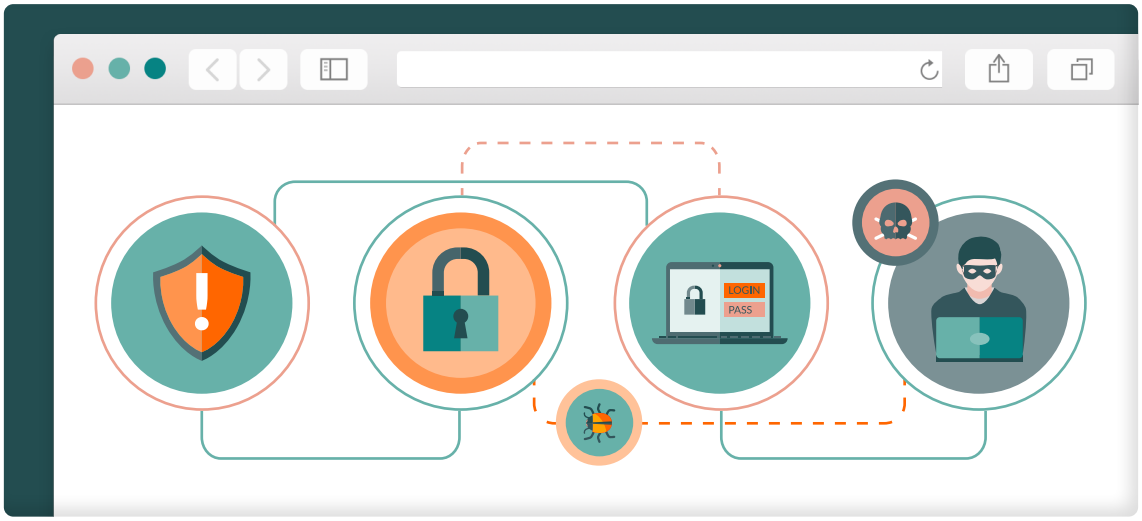
Unia Europejska
Europejski Fundusz Rozwoju Regionalnego

WITAJ!

Za pomocą tej broszury chcemy Ci przedstawić programy i narzędzia, które pomogą zwiększyć Twoje bezpieczeństwo w sieci. Znając je – możesz lepiej chronić swoją prywatność i dane przed cyberatakami.

Pamiętasz sposób Barbary na zapamiętanie programów i narzędzi zwiększających bezpieczeństwo w sieci? W filmie pt. *„Antywirus i zaślepka, czyli z czego korzystać, żeby być bezpiecznym w sieci”* stworzyła sobie analogie do świata rzeczywistego dla każdego z nich. **Ochrona urządzenia przed wirusami** jest zupełnie jak **ochrona domu przed intruzami**. **Zasłanianie kamery** w laptopie to internetowy odpowiednik **zasłaniania okien** przed podglądaczami, a **wieloetapowe potwierdzanie** tożsamości podczas logowania do swojego konta w aplikacjach online to nic innego jak **dodatkowe zamki w drzwiach**. Gdyby się nad tym głębiej zastanowić, to prawdopodobnie każde rozwiązanie podnoszące poziom bezpieczeństwa w internecie będzie miało swoje nawiązanie do codziennego życia.

Warto korzystać z dostępnych zabezpieczeń, nawet jeżeli nie ma całkowitej pewności, że uda się uniknąć każdej trudnej sytuacji. To też tak, jak z bezpieczeństwem w świecie rzeczywistym – jeżeli zabezpieczenia są dostępne, to lepiej je stosować i **minimalizować ryzyko cyberataku**.



Zabezpieczenia w internecie takie jak zabezpieczenia w domu

PROGRAMY ANTYWIRUSOWE SĄ JAK ALARM

Zabezpieczenia podczas korzystania z internetu chronią nasze urządzenia przed intruzami. Czym właściwie są te zabezpieczenia? To różne programy, które instalujemy na naszych sprzętach (komputer, laptop, tablet, smartfon), mające za zadanie nie tylko stanowić **bramę do naszych systemów** i **zabezpieczać nas przed wtargnięciem intruzów** czy **blokować niewłaściwe treści**, ale także **na bieżąco informować nas** o sytuacjach, które powinny wzbudzić naszą podejrzliwość.
Są trochę jak prywatny ochroniarz naszych urządzeń.

> ***PROGRAM ANTYWIRUSOWY*** *– program, który chroni komputer przed złośliwym oprogramowaniem. Skanuje urządzenie i w przypadku znalezienia zagrożenia, takiego jak wirus komputerowy, niweluje je. Cały czas monitoruje także system w razie pojawienia się zagrożeń, o których informuje.*
> *(Po informacje o wirusach i złośliwym oprogramowaniu sięgnij także do broszury pt. „Spektakl i film? Wszystko, co musisz wiedzieć o bezpiecznej rozrywce w sieci. Poradnik dla seniora”).*

Program antywirusowy jest więc jednocześnie jak **monitoring**, **alarm** i **ochroniarz**, strzegący dostępu do naszych danych. Pamiętajmy jednak, że jeśli sami wpuścimy intruza, np. pobierając i uruchamiając program z niezaufanego źródła, nasza ochrona traci swoje znaczenie.

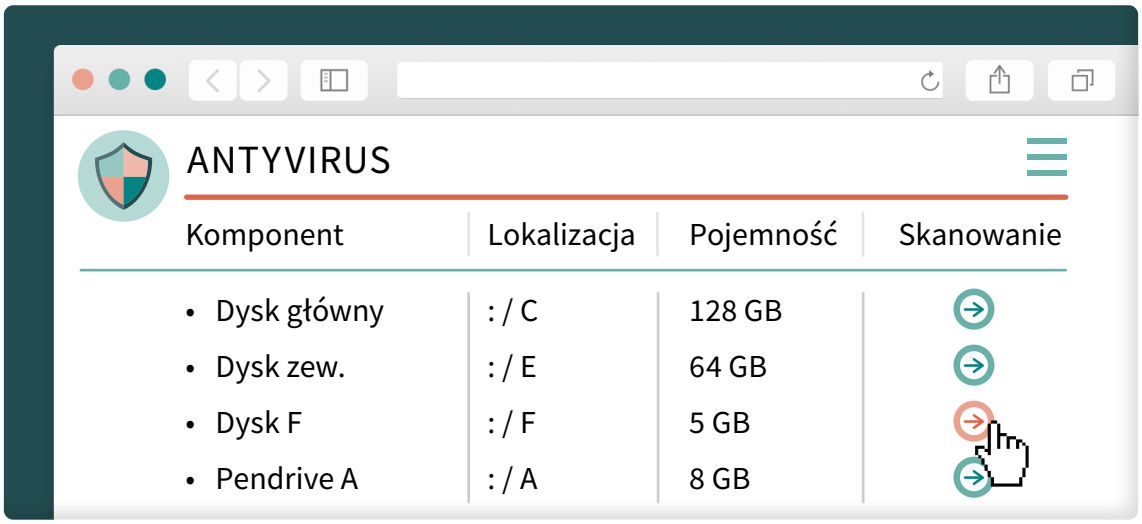
Skąd wziąć narzędzia zabezpieczające nas przed cyberatakiem? Nie musisz od razu kupować płatnego oprogramowania, możesz skorzystać z darmowych wersji programów antywirusowych. Jeśli natomiast dopiero kupujesz urządzenie, takie jak komputer, laptop, tablet czy telefon komórkowy, zwróć uwagę, czy oprogramowanie antywirusowe nie jest już częścią systemu operacyjnego. Najważniejsze, aby program pochodził z **oficjalnych źródeł**, np. strony internetowej producenta czy z oficjalnego sklepu z aplikacjami. Przed dokonaniem wyboru warto też sprawdzić opinie innych użytkowników, bo w ofercie producentów dostępne są również takie programy, które bardzo spowalniają pracę systemu lub działają mniej efektywnie. Jeżeli chcesz dowiedzieć się więcej na temat programów antywirusowych, zobacz krótki film pt. *„Bezpieczne zakupy w sieci. Odc. 1 – Bezpieczny komputer”*.

Wiemy już, że program antywirusowy nie tylko stale neutralizuje ewentualne zagrożenia, ale też informuje nas, na co powinniśmy uważać. Jeśli więc wchodząc na stronę internetową lub pobierając jakiś załącznik na ekranie swojego urządzenia zobaczysz komunikat, że dane treści mogą nie być bezpieczne – zastanów się, czy chcesz podjąć ryzyko.

Niestety, nawet najlepszy „antywirus" może nie uchronić naszego komputera przed niektórymi złośliwymi programami czy wirusami, które są stale doskonalone przez hakerów. W związku z tym pamiętaj, aby wyrażać zgodę na **automatyczną aktualizację** oprogramowania antywirusowego. W ten sposób masz większą szansę na bycie bezpiecznym.

Sieć zwiększa zasięg rozprzestrzeniania się wirusa pomiędzy użytkownikami – czasami wystarczy jedno kliknięcie i wirus, którego otrzymałeś w wiadomości, zostanie automatycznie rozesłany do wszystkich Twoich kontaktów.
Co ważne, wirtualna infekcja może pochodzić nie tylko z **załączników** i **linków** w wiadomościach z e-maila, komunikatorów czy ze stron internetowych, ale także z **urządzeń, jakie podłączamy do komputera**, np. pendrive'ów.

PENDRIVE *(za: „Słownik języka polskiego PWN")* *to „niewielkie urządzenie współpracujące z komputerem poprzez port USB". Służy do przechowywania danych.*



Wiemy już, jak działają programy antywirusowe i przed czym mogą nas uchronić. Wiemy też, że nie są niezawodne. Po co jeszcze warto sięgnąć, aby źródła z których korzystamy, były weryfikowane pod kątem bezpieczeństwa?

ZWERYFIKOWANE ŹRÓDŁA

ZWERYFIKOWANE ŹRÓDŁA *to takie, w których nasze programy zabezpieczające nie znalazły żadnych zagrożeń.*

Jak wiesz z poprzedniego podrozdziału, programy antywirusowe stale monitorują treści i ostrzegają, kiedy jakieś pliki lub strony nie są bezpieczne. W takim przypadku zawsze otrzymujemy bardzo czytelny komunikat. Warto jednak pamiętać, że czasami nawet najlepsze programy mogą się pomylić i uznać jakiś plik za niebezpieczny, choć wcale taki nie jest. Dlatego, jeśli antywirus błędnie pokazał, że coś jest niebezpieczne – możemy dodatkowo zweryfikować takie źródło i jeśli jesteśmy pewni, że pochodzi od zaufanej osoby lub instytucji (bo np. potwierdziliśmy to dodatkowo telefonicznie) – nie obawiać się.

Dobrze jest korzystać z **zaufanych przeglądarek internetowych**, które **weryfikują strony internetowe** i **ostrzegają przed niebezpiecznymi adresami**. Dlatego, podobnie jak w przypadku programu antywirusowego, przed podjęciem decyzji o korzystaniu z wybranej przez nas przeglądarki, warto zapoznać się z jej możliwościami oraz opiniami użytkowników. Korzystajmy z takich przeglądarek, które będą nas **informowały o potencjalnych zagrożeniach**.

Pamiętaj

– możesz mieć wiele zainstalowanych i aktywnych przeglądarek, a nawet korzystać z różnych jednocześnie, ale program antywirusowy możesz mieć tylko jeden. Nie wszędzie więc działa zasada im więcej – tym lepiej. Zainstalowanie dwóch lub więcej programów antywirusowych na jednym urządzeniu może prowadzić do konfliktów między nimi i tym samym do zmniejszenia bezpieczeństwa.

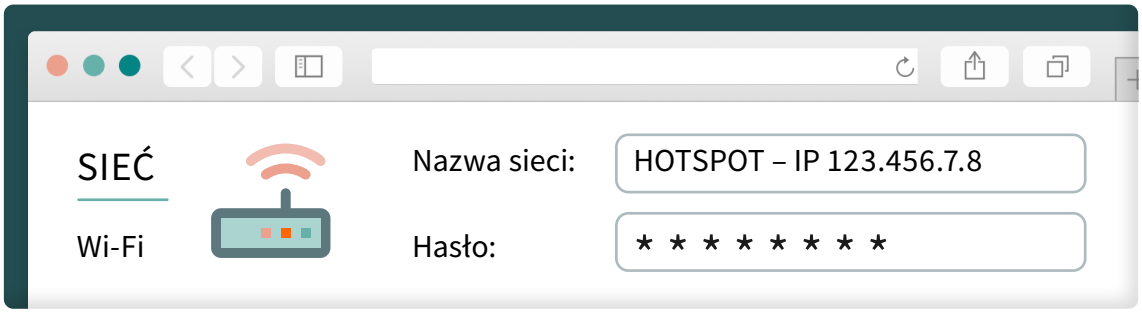
Skoro mowa o przeglądarkach – warto wspomnieć, że informacje o tym, jakie strony przeglądamy, są stale zapisywane. Jeżeli więc nie chcemy, aby wyszukiwarka pamiętała nasze działania, możemy na bieżąco **usuwać historię wyszukiwania** lub korzystać z **przeglądarki w trybie prywatnym**. Wszystko ma jednak swoje wady i zalety. Gdy korzystamy z tego specjalnego trybu, system nie podpowiada nam automatycznie możliwych wyszukiwań treści najbardziej pasujących do naszych preferencji.

TRYB PRYWATNY *– funkcja w przeglądarce internetowej, za pomocą której możemy przeglądać treści w sieci bez zapamiętywania ich przez narzędzie, z którego korzystamy.*

Korzystanie z przeglądarki w trybie prywatnym to nic trudnego! Wystarczy wejść w ulubioną przeglądarkę, a następnie w menu wybrać pozycję „nowe okno w trybie prywatnym". W ramach ćwiczeń możesz wyszukać informacje o skrócie klawiszowym, za pomocą którego okno prywatne będzie się otwierało od razu po uruchomieniu przeglądarki.

Skąd brać wiedzę o tym, które narzędzia i aplikacje są bezpieczne? Korzystając z **opinii innych użytkowników**, mamy większą pewność, że instalowane przez nas oprogramowanie czy aplikacja jest bezpieczne. Pamiętajmy o tym, instalując je nie tylko na komputerze stacjonarnym lub laptopie, ale także na urządzeniu mobilnym.

Do zweryfikowanych źródeł internetowych poza bezpiecznymi stronami należy też **sieć, z której korzystamy**. Tu szczególnie ważne jest **silne hasło** – dzięki niemu z Twoją siecią połączą się tylko te osoby, którym świadomie przekażesz dane do logowania, a nie niepowołani użytkownicy.



(Dowiedz się więcej na temat bezpiecznego korzystania z sieci – obejrzyj film pt. *„Bądź cyberbezpieczny zawsze. Odc. 1 – Cyberbezpieczeństwo zaczyna się w domu"*). Więcej o zweryfikowanych źródłach możesz także przeczytać w broszurze pt. *„Spektakl i film? Wszystko, co musisz wiedzieć o bezpiecznej rozrywce w sieci. Poradnik dla seniora"*.

PAMIĘTAJ

Po wnikliwym zapoznaniu się z tym podrozdziałem wiesz już, o czym musisz zawsze pamiętać.

1. Przed wybraniem programu antywirusowego zapoznaj się z **opiniami** innych internautów i zdecyduj, czy zależy Ci na wersji płatnej, czy **darmowej**. Pamiętaj, aby zawsze pobierać oprogramowanie z **oficjalnej strony dostawcy**.
2. Pobierz i na bieżąco **aktualizuj** program antywirusowy. Często **skanuj** przy jego pomocy cały system, zarówno na komputerze, jak i na smartfonie.
3. Przy **weryfikacji źródeł** treści internetowych polegaj na tym, co podpowiadają Ci **program antywirusowy** oraz **przeglądarka**.
4. Jeżeli nie chcesz, aby informacje na temat Twoich wyszukiwań były widoczne, korzystaj z **prywatnego trybu w przeglądarce** lub **usuwaj historię** wyszukiwania.

Jeszcze bezpieczniej

ZASŁONIĘTE OKNO DO PRYWATNOŚCI

Zabezpieczenia w sieci to nie tylko programy **zainstalowane przez nas na urządzeniu** albo **wbudowane w nie automatycznie**. To także **zewnętrzne urządzenia, które możemy podłączyć**. Warto korzystać ze wszystkich dostępnych narzędzi zwiększających bezpieczeństwo w sieci. Można do nich zaliczyć np. „zaślepkę", która przysłania kamerę, kiedy jej nie używasz.

ZAŚLEPKA KAMERY to drobne i proste w swojej konstrukcji narzędzie, mierzące około kilku centymetrów, które z łatwością i od ręki można nałożyć na kamerę urządzenia. Odsuwa się ją lub zdejmuje w dowolnym momencie, gdy chcemy skorzystać z kamery.

Innymi słowy, zaślepka kamery to coś, czym **zasłaniamy i w dowolnym momencie odsłaniamy kamerę** wbudowaną w urządzenie, takie jak laptop. Możesz też zrobić własne zabezpieczenie, po prostu zasłaniając kamerę np. kawałkiem kartki samoprzylepnej czy plastrem.

Wyobraź sobie, że

uczestniczysz w wideokonferencji, ale nie chcesz, żeby inni jej uczestnicy Cię widzieli. Jak to zrobić? Oczywiście możesz kliknąć w odpowiedni **przycisk z przekreśloną ikoną kamery** w danym programie do wideokonferencji. Możesz też wyłączać udostępnianie obrazu swojej kamery w ustawieniach urządzenia. Kiedy jednak następnym razem będziesz chciał, żeby inni Cię widzieli, będziesz musiał wrócić do ustawień i je zmienić. W przypadku zaślepki kamery jedyne, o czym musisz pamiętać, to żeby ją odsłonić lub zasłonić. Wygodne, prawda?

Czemu warto zasłaniać kamerę? Bo ktoś mógłby włamać się do naszego systemu i uzyskać dostęp do tego, co widać w zasięgu kamery wbudowanej w nasze urządzenie.

Żeby mieć całkowitą pewność, że nikt nas nie tylko nie widzi, ale też nie słyszy, kiedy już zakończymy naszą wideokonferencję – zawsze po zakończeniu spotkania możemy wejść w **ustawienia** systemu i **wyłączyć głośność wejściową**.

PODWÓJNY ZAMEK

Inna jeszcze forma zabezpieczenia – to taka, którą narzucają serwisy wymagające logowania – np. **uwierzytelnianie dwuskładnikowe**.

Uwierzytelnianie dwuskładnikowe sprawia, że logowanie się do naszych kont w internecie jest bezpieczniejsze. Jeżeli na przykład chcemy założyć konto e-mail i wybieramy serwis, z którego będziemy korzystać – zwróćmy uwagę, czy oferuje taką funkcję.

UWIERZYTELNIANIE DWUSKŁADNIKOWE LUB DWUSTOPNIOWE – polega na tym, że aby uzyskać dostęp do naszego konta w jakimś serwisie, potrzebne jest podanie nie tylko hasła, ale także drugiego składnika, takiego jak np. kod otrzymany za pomocą wiadomości SMS. Jeżeli ktoś zdobył nasze hasło i chce dostać się do naszego konta, dzięki temu dodatkowemu zabezpieczeniu nie będzie w stanie się tam zalogować.

Uwierzytelnianie dwuskładnikowe staje się coraz powszechniejsze i jest najczęściej stosowane przez **bankowość internetową**, **media społecznościowe**, **pocztę e-mail** czy **usługi internetowe**. Drugim składnikiem może być np. specjalny, jednorazowy kod SMS wysłany na Twojego smartfona czy kod z listy, którą bank udostępnił tylko Tobie, jako właścicielowi konta. W różnych miejscach jako drugi składnik jest też często wykorzystywany adres skrzynki pocztowej.

Zdarza się też tak, że **drugi składnik** różni się w zależności od serwisu czy usługi.

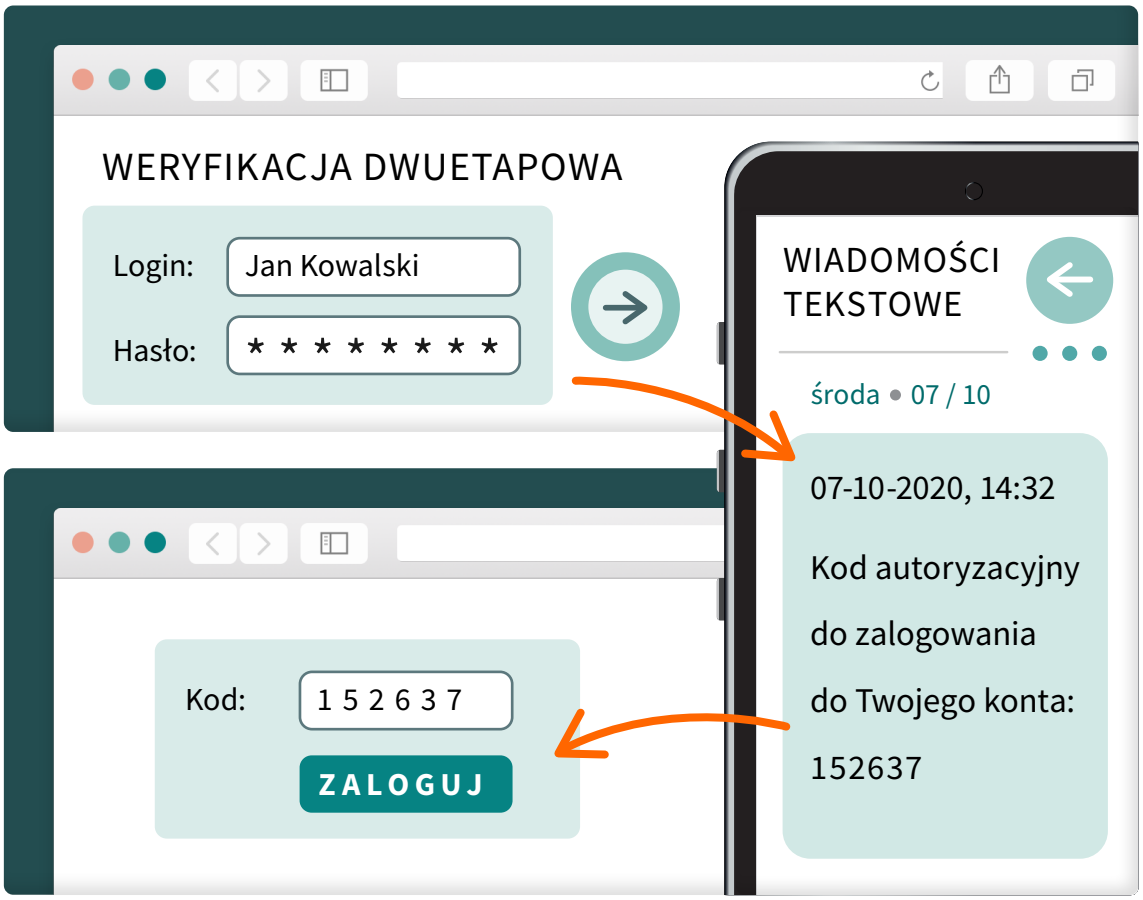
Wyobraź sobie, że

chcesz się zalogować na swoje konto w mediach społecznościach z nowego urządzenia, na którym Twoje hasło nie jest zapisane w pamięci komputera (zapisywanie haseł w pamięci komputera nie należy do najbezpieczniejszych rozwiązań – lepiej tego nie rób). Wpisujesz hasło, a następnie urządzenie wysyła SMS z jednorazowym kodem jako drugim składnikiem uwierzytelnienia. Jeśli jednak nie masz smartfona pod ręką, możesz też wybrać, że Twoim drugim **kluczem** będzie wysłany na pocztę e-mail. Wtedy logujesz się na swoją skrzynkę e-mailową, przepisujesz kod w odpowiednie pole w serwisie społecznościom, do którego chcesz się zalogować. I gotowe!

Nawet jeżeli ktoś zna Twoje hasło, np. do portalu społecznościowego, to jeśli masz różne hasła w różnych miejscach, nie będzie mógł włamać się do Twojej skrzynki mailowej po kod uwierzytelniający. Nie zdobędzie też kodu, który otrzymasz w wiadomości SMS, gdy będzie próbował zalogować się na Twoją pocztę e-mail. Dlatego to rozwiązanie jest tak przydatne – przejęcie Twojego podstawowego hasła nie oznacza jeszcze, że ktoś dostanie się do Twoich danych. Żeby jednak uniknąć sytuacji, w której ktoś próbuje się zalogować na Twoje konta – pamiętaj o tym, żeby **wszędzie ustawiać inne hasła**. Jeżeli chcesz poznać bardziej szczegółowe informacje na ten temat – zachęcamy do przeczytania tekstu pt. *„Konfigurowanie uwierzytelniania dwuskładnikowego (2FA)”* na stronie *gov.pl*.

Dwuskładnikowe uwierzytelnianie jest szczególnie ważne, gdy chodzi o Twoje **finanse** lub **pliki prywatne**, np. zdjęcia. Jeżeli więc korzystasz z chmury do przechowywania zdjęć, filmów, dokumentów urzędowych czy innych treści, które chcesz zabezpieczyć przed dostępem innych osób, koniecznie pamiętaj o tym typie uwierzytelniania.

> **CHMURA** *(za: „Słownik języka polskiego PWN”) – „wirtualne miejsce w internecie umożliwiające przechowywanie dowolnych danych oraz szybki dostęp do nich z dowolnego urządzenia połączonego z siecią”.*



Dla Ciebie to tylko dodatkowa chwila, a dla Twoich danych – znaczne zwiększenie bezpieczeństwa. Brak takiego uwierzytelniania wiąże się z większą dostępnością oszustów do naszego konta, np. bankowego, mailowego czy w mediach społecznościowych. Wieloskładnikowość **zmniejsza ryzyko wyłudzeń naszych danych i dostępu do nich. Podwójny zamek w drzwiach naszego domu** daje nam większe poczucie bezpieczeństwa niż jeden, prawda?

PAMIĘTAJ

Po wnikliwym zapoznaniu się z tym podrozdziałem wiesz już, o czym musisz zawsze pamiętać.

1. Korzystaj z **zaślepki kamery** – kupionej lub domowej – i odsłaniaj ją tylko w razie potrzeby.
2. Aby uniknąć sytuacji przejęcia Twoich danych – stosuj wszędzie **inne hasła do logowania**.
3. Pamiętaj, żeby tam, gdzie jest to możliwe, **ustawiać uwierzytelnianie dwuskładnikowe** i korzystać z niego. Jeżeli jest też taka możliwość – jako drugi składnik wybierz więcej niż jedno rozwiązanie.

Do kogo się zgłosić w przypadku podejrzanych sytuacji w internecie

Zabezpieczenia stanowią absolutną podstawę, ale może się zdarzyć, że nawet najbardziej zaawansowane ustawienia nie uchronią Cię przed atakiem, bo hakerzy właśnie stworzą wirusa, który omija wszystkie aktualne zabezpieczenia. Dlatego trzeba być gotowym na każdą okoliczność i wiedzieć, kiedy i do kogo się zwrócić.

Co jeszcze może się zdarzyć? Możesz też mieć wszystkie niezbędne zabezpieczenia, ale zdarzy się, że akurat zapomnisz zaktualizować program antywirusowy albo zasłonić kamerę. Ktoś może wysyłać do Ciebie niewłaściwe treści albo podszywać się w mediach społecznościowych pod kogoś, kogo znasz. Nawet pomimo najlepszych systemów i zabezpieczeń mogą mieć miejsce próby wyłudzenia. W takich sytuacjach pamiętaj, że są odpowiednie instytucje, do których możesz się **zwrócić po pomoc**.

DO BLISKICH I NIE TYLKO

W sytuacji problemowej lub podejrzanej zachowaj spokój i skontaktuj się z **członkiem rodziny**, ze **znajomym** czy nawet z **sąsiadką**. Poznaj obiektywny punkt widzenia, który może być bardzo pomocny w poznaniu i rozwiązaniu problemu.

DO BANKU I NA POLICJĘ

Co jeśli Twoje obawy okażą się słuszne i ktoś niepożądany zdobędzie dostęp do Twoich danych? Albo jeśli zobaczysz, że po wykonaniu jakiejś czynności w internecie z Twojego konta zniknęła niespodziewana kwota? Nie wahaj się, od razu zadzwoń do **banku**, a zaraz potem skontaktuj się z **policją**.

Nawet jeżeli nie masz stuprocentowej pewności, że zaszło coś podejrzanego – lepiej **zablokuj kartę**, dzwoniąc na **międzybankową infolinię +48 828 828 828**. Podobnie jeśli chodzi o **dokument tożsamości** – powinieneś go **zastrzec** zawsze wtedy, gdy masz podejrzenie, że ktoś przechwycił Twoje dane osobowe – nie zwlekaj. Pamiętaj o powiadomieniu policji (numery kontaktowe: **112** lub **997**).

Dzięki natychmiastowemu działaniu możesz uchronić się przed sytuacją, w której ktoś **ukradnie pieniądze z Twojego konta**, a nawet weźmie **kredyt**, korzystając z Twoich danych.

Jeżeli nie znasz numeru kontaktowego do swojego banku, otwórz przeglądarkę, wpisz w wyszukiwarkę nazwę banku i frazę „kontakt". Zobaczysz numer, który od razu możesz wybrać na ekranie smartfona.

Bardziej zaawansowanym użytkownikom internetu polecamy też artykuł pt. *„Urząd Ochrony Danych Osobowych informuje, co zrobić w przypadku kradzieży tożsamości"*.

DO UOKIK I RZECZNIKA OCHRONY KONSUMENTA

Osobom mniej biegłym w internecie może się wydawać, że sieć rządzi się zupełnie innymi prawami niż niewirtualna rzeczywistość. Warto wiedzieć, że tak jak w realnym świecie, tak w wirtualnym **konsumenci** mogą liczyć na pomoc instytucji, których zadaniem jest ochrona ich praw. Są nimi **Urząd Ochrony Konkurencji i Konsumentów (UOKiK)** oraz **Rzecznik Ochrony Konsumenta** – funkcjonują oni także dla konsumentów **internetowych**.

Zgodnie z informacjami na oficjalnej stronie internetowej *Urzędu Ochrony Konkurencji i Konsumentów* pierwszą linią kontaktu dla tzw. spraw prostych, niewymagających analizy dokumentów jest infolinia konsumencka, dostępna pod numerami **+ 48 801 440 220** oraz **22 290 89 16** i czynna od poniedziałku do piątku w godzinach **8:00–18:00**. Robiłeś zakupy przez internet i zostałeś poddany nieuczciwym praktykom? Zadzwoń pod ten numer i dowiedz się, co powinieneś dalej zrobić.

Sprawami wymagającymi analizy dokumentów zajmuje się **konsumenckie centrum e-porad** oraz **wojewódzkie inspektoraty inspekcji handlowej**. Jeśli na wskazanej stronie internetowej nie znajdziesz potrzebnych informacji, napisz wiadomość e-mail korzystając z danych kontaktowych dostępnych na tych stronach.

ZESPÓŁ CERT POLSKA (CSIRT NASK)

Na stronie *www.cert.pl* można zapoznać się z aktualnościami na temat bezpieczeństwa w sieci oraz dowiedzieć się o najważniejszych cyberzagrożeniach. Portal daje też możliwość zgłaszania różnego rodzaju niebezpiecznych zdarzeń w sieci – o których więcej poniżej. Od 28 sierpnia 2018 r. CERT Polska realizuje zadania CSIRT NASK – jednego z trzech zespołów reagowania na incydenty w sieci poziomu krajowego.

Jak zgłosić naruszenie w sieci?

Należy wejść w zakładkę „Zgłoś incydent" i następnie spośród czterech pozycji kliknąć w „osoba fizyczna/inne podmioty" (pozostałe to: operator usług kluczowych, dostawca usługi cyfrowej, podmiot publiczny). Następnie należy wybrać **typ zdarzenia**, które chcemy zgłosić: podejrzana wiadomość e-mail/SMS (podejrzane załączniki/SMS-y, phishing, szantaż), oszustwo (fałszywe sklepy internetowe i inne próby podszywania się), złośliwe oprogramowanie (próbki wirusów lub pliki zaszyfrowane ransomware), podatności (błędy w oprogramowaniu lub aplikacjach internetowych), nielegalne treści (zgłoszenia przeznaczone dla zespołu Dyżurnet.pl), inne (wszystkie inne incydenty niepasujące do poprzednich kategorii). Po kliknięciu wyświetli się nam poniżej odpowiedni **formularz**. Gdy go wypełnimy, możemy **wysyłać zgłoszenie jednym kliknięciem**.

Widzisz zagrożenie w sieci? Reaguj, zgłoś do CERT Polska! Chroń swoje dane i pieniądze!

Zgłoszenie incydentu pomoże skuteczniej walczyć z cyberzagrożeniami. Dzięki temu dane – zarówno Twoje, jak i innych użytkowników będą bezpieczniejsze. Warto, abyśmy wszyscy czuli się odpowiedzialni za nasze wspólne bezpieczeństwo w internecie.

Zgłoszenie incydentu zajmie tylko chwilę, a znaczenie dla tworzenia bezpiecznego internetu ma ogromne! Zapraszamy na *www.cert.pl*.

Numer kontaktowy do zespołu CERT: **22 380 82 74**.
Adres mailowy: *info@cert.pl*

PAMIĘTAJ

Po wnikliwym zapoznaniu się z tym podrozdziałem wiesz już, o czym musisz zawsze pamiętać.

1. W przypadku nietypowych sytuacji zachowaj zawsze **czujność**, ale też **spokój**.
2. Nie miej oporów, żeby dzwonić do **bliskich**, którzy lepiej od Ciebie znają się na internecie.
3. Zawsze pamiętaj o tym, aby w pierwszej kolejności zminimalizować szkody, **zastrzegając dokumenty w banku** (np. gdy podejrzewasz, że wyciekły Twoje dane osobowe, znajdujące się także na Twoim dowodzie osobistym), a następnie **poinformować o zdarzeniu policję**.
4. Pamiętaj, że instytucje działające w świecie rzeczywistym obejmują też zdarzenia w świecie wirtualnym. W przypadku nieuczciwych praktyk sprzedawcy zadzwoń do **UOKiK**.
5. Pamiętaj także o zgłaszaniu zdarzeń w sieci na specjalnej stronie **CERT NASK**.

PAMIĘTAJ O WAŻNYCH NUMERACH

Infolina międzybankowa **+48 828 828 828**

Urząd Ochrony Konkurencji i Konsumetów UOKiK
od poniedziałku do piątku w godz. 8:00–18:00
+48 801 440 220 oraz **22 290 89 16**

CERT Polska (zgłaszanie podejrzanych zdarzeń
i ataków w sieci) **22 380 82 74**

Co już wiesz o bezpiecznej komunikacji w sieci?

- Wiesz, **z jakich zabezpieczeń** korzystać w sieci (programy i dodatkowe narzędzia) oraz jak zabezpieczyć swoje logowanie.
- Wiesz, **do kogo się zwrócić** w sytuacji zagrożenia, oszustwa lub po prostu podejrzenia o nieuczciwym działaniu.
- Wiesz też, że w różnych sytuacjach potrzebne są **różne reakcje**, a rozwiązania w internecie i poza nim wcale tak bardzo się nie różnią.

Gratulacje,
to już
kolejny etap
za Tobą!

Zobacz pozostałe filmy instruktażowe i broszury na temat bezpiecznego korzystania z internetu:

- **na stronie internetowej kampanii** „Seniorze – spotkajmy się w sieci”:

  https://www.gov.pl/seniorze-spotkajmy-sie-w-sieci

Po więcej informacji na temat bezpieczeństwa w sieci możesz się udać:

- **na stronę gov.pl**, na której znajduje się dużo ciekawych materiałów na temat korzystania z sieci oraz cyberbezpieczeństwa:

  https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo

- **na stronę cert.pl**, gdzie można dowiedzieć się o najważniejszych cyberzagrożeniach i zgłosić różnego rodzaju niebezpiecznych zdarzeń w sieci:

  https://www.cert.pl/

- **na stronę System DOKUMENTY ZASTRZEŻONE**, z której możesz czerpać informacje o aktualnych zjawiskach związanych z bezpieczeństwem dokumentów – w tym bankowości internetowej:

  https://dokumentyzastrzezone.pl/category/aktualnosci/

- **na kanał Fundacji Warszawski Instytut Bankowości**, na którym znajdziesz bardzo dużo edukacyjnych filmów, związanych między innymi z bezpieczeństwem seniora w sieci:

  https://www.youtube.com/channel/UC0hP7yAJ58bkWJnsnf-hHhw

Seniorze

– spotkajmy się w sieci i korzystajmy z niej **bezpiecznie**.
Teraz widzisz, jakie to proste!

Publikacja powstała w ramach kampanii „Seniorze – spotkajmy się w sieci”.
Kampania została zrealizowana przez Ministerstwo Cyfryzacji (obecnie: KPRM) i Państwowy Instytut Badawczy NASK we współpracy z Warszawskim Instytutem Bankowości – laureatem konkursu pt. „(Nie)Bezpieczni w sieci – konkurs dla NGO na najlepszą kampanię edukacyjną”. Jest ona współfinansowana ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa.

Konsultacja merytoryczna:
Fundacja Warszawski Instytut Bankowości
Departament Cyberbezpieczeństwa Ministerstwa Cyfryzacji (obecnie: KPRM)

Redakcja i korekta językowa:
Zespół Programów Edukacyjno-Informacyjnych,
Państwowy Instytut Badawczy NASK

Layout, projekt okładki i skład:
Bringmore Advertising

Państwowy Instytut Badawczy NASK
ul. Kolska 12
01-045 Warszawa

Wydanie I
Warszawa 2020

Partner kampanii:

WARSZAWSKI INSTYTUT BANKOWOŚCI

Fundusze Europejskie Polska Cyfrowa

KPRM

NASK

Unia Europejska Europejski Fundusz Rozwoju Regionalnego

SENIORZE
spotkajmy się w sieci

Zobacz i pokaż bliskim

www.gov.pl/seniorze-spotkajmy-sie-w-sieci

Partner kampanii:

WARSZAWSKI INSTYTUT BANKOWOŚCI

Fundusze Europejskie Polska Cyfrowa

KPRM

NASK

Unia Europejska
Europejski Fundusz Rozwoju Regionalnego