SENIORZE
spotkajmy się w sieci

Spektakl i film?

Wszystko, co musisz wiedzieć
o bezpiecznej rozrywce w sieci.

Poradnik dla seniora

01.

Partner kampanii:

WARSZAWSKI INSTYTUT BANKOWOŚCI

Fundusze Europejskie Polska Cyfrowa

KPRM

NASK

Unia Europejska
Europejski Fundusz Rozwoju Regionalnego

WITAJ!

W ramach kampanii „Seniorze – spotkajmy się w sieci” przygotowaliśmy dla Ciebie cykl materiałów edukacyjnych – filmów instruktażowych i broszur, dzięki którym będziesz bezpieczniej poruszać się po internetowej rzeczywistości. Jeżeli coś będzie dla Ciebie niejasne albo wzbudzi Twoje wątpliwości – **zwróć się do bliskich o pomoc**. Na pewno z chęcią będą Cię wspierać w Twoich internetowych odkryciach. W tym przewodniku przeprowadzimy Cię przez najważniejsze wątki związane z bezpiecznym korzystaniem z rozrywki w internecie. Jeśli chcesz dowiedzieć się więcej – zajrzyj na *stronę kampanii* i sprawdź pozostałe broszury oraz filmy instruktażowe z Barbarą Bursztynowicz.

Pamiętasz, jak w filmie *„Spektakl i film, czyli o bezpiecznej rozrywce w internecie”* Barbara wybierała się na spektakl, który był transmitowany w sieci? Znajoma wysłała jej **link do strony internetowej opery**. Sytuacja była dla Barbary podejrzana, ponieważ od dawna nie rozmawiała z koleżanką, od której dostała adres witryny (przykładowo – **adres witryny** to „www.stronainternet...” z obrazka poniżej). Dlatego najpierw skontaktowała się ze znajomą. Upewniła się, że osoba, z którą pisze, jest tą, za którą się podaje. Potem zwróciła baczną uwagę na przesłany link, czyli ciąg znaków rozpoczynający się od „https”. Po kliknięciu w link użytkownik przenosi się do konkretnej strony internetowej. Link nie wzbudził jej podejrzeń, mogła więc spokojnie w niego kliknąć i przejść wirtualnie do strony, na której pokazywane są spektakle.

Internet umożliwia korzystanie z szerokiego dostępu do legalnej rozrywki. Zawsze jednak należy zachować czujność. Świadomość istniejących zagrożeń pozwala na uniknięcie niebezpieczeństw, które mogą się zdarzyć także w wirtualnym świecie, takich jak **próby przejęcia naszych danych wrażliwych** (takich jak dane ujawniające pochodzenie, poglądy, przekonania itp.) **czy wyłudzenia poufnych informacji** (np. PESEL, login, hasło, numer konta bankowego, seria i numer dowodu osobistego). Z kolejnych stron dowiesz się, jak postępować, aby móc bezpiecznie korzystać z rozrywki w internecie.

Co ma wspólnego spektakl i phishing?

SPEKTAKL I FILM, CZYLI CO OFERUJE INTERNET

Internet umożliwia powszechny dostęp do rozrywki. W sieci znajdziesz ulubiony film albo odcinek serialu, który zdarzyło Ci się przegapić. W domowym zaciszu obejrzysz też transmisję spektaklu. Wybierzesz się w wirtualną podróż po wystawie w galerii sztuki czy muzeum. Przeczytasz ciekawą powieść lub interesujący artykuł, a jeśli wolisz słuchowiska – znajdziesz tam też audiobook *(utwór pisany, znajdujący się na nośniku cyfrowym to **e-book**, a czytany przez lektora to **audiobook**. „Book" to z angielskiego książka).* A wszystko to – kiedy chcesz.

PHISHING I NIEUCZCIWE PRAKTYKI FINANSOWE

Każda strona internetowa, nawet ta zawierająca dostęp do rozrywki, może zostać wykorzystana przez przestępców działających w sieci, którzy **celowo wprowadzają odbiorcę w błąd** i narażają go na duże straty. Podobnie jak w życiu, także w internecie oszuści poszukują nowych sposobów na zdobycie naszych **danych wrażliwych**. Zjawiskiem, na które należy uważać, korzystając z rozrywki w internecie, jest **phishing**. To próba „**złowienia**" identyfikatorów i haseł użytkowników w celu uzyskania nielegalnego dostępu do ich danych i usług (w szczególności kont bankowości elektronicznej).

PHISHING *– rodzaj nieuczciwych działań, które opierają się na wykorzystywaniu technik socjotechnicznych w celu nakłonienia użytkowników do **odwiedzenia fałszywej witryny internetowej**. Użytkownicy podają na niej poufne informacje, takie jak dane logowania, a oszuści przejmują je. Inną techniką ataku phishingowego jest wysłanie **SMS-a z linkiem do fałszywej strony** lub wysłanie wiadomości e-mail zawierającej załącznik ze złośliwym oprogramowaniem. Kliknięcie w link lub pobranie załącznika najczęściej kończy się przejęciem naszych **danych do logowania do usług bankowości elektronicznej**.*

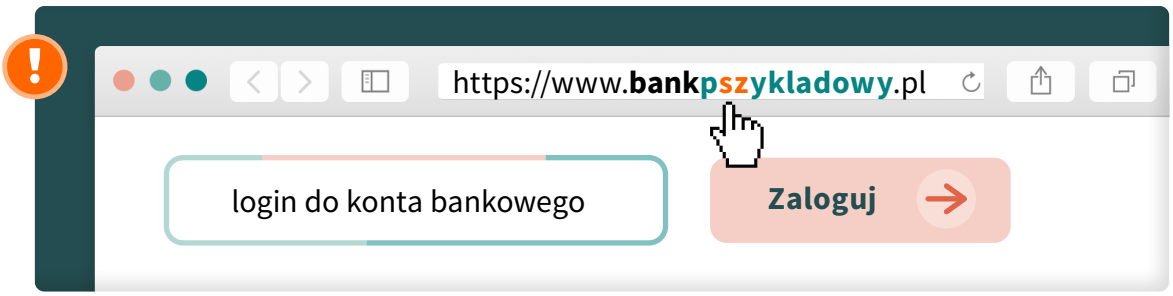
Jak to rozumieć?

Wyobraź sobie, że chcesz się wybrać na wirtualną wystawę do ulubionego muzeum. Wchodzisz na stronę internetową z przekonaniem, że to witryna znanej Ci instytucji. Widzisz pola, które wymagają podania Twoich danych osobowych, aby móc się zarejestrować i korzystać z tego, co oferuje strona. Pewnie dziwi Cię, że witryna wymaga przekazania wielu szczegółowych personalnych danych. No właśnie. W przypadku phishingu oszuści tworzą stronę internetową, która może być łudząco podobna do tej, którą znasz. Umieszczają na niej **pola do wpisania określonego zbioru informacji**. Gdy podamy dane i klikniemy przycisk akceptacji, oszuści przejmują nasze dane wrażliwe i mogą je dowolnie wykorzystać, np. uzyskać dostęp do naszych kont bankowych.

Innymi słowy, wchodzimy na stronę, o której myślimy, że jest zaufana, podajemy nasze poufne dane, oszuści je przejmują, a niedługo później stan naszego konta ulega zmianie. To zjawisko może dotyczyć **stron o bardzo różnej tematyce**.

Na co należy więc zwracać uwagę? Strona phishingowa ma inny adres niż właściwa strona – różni się najczęściej **literówką lub znakiem specjalnym** – dlatego należy uważnie czytać adresy stron i nie klikać w nic pospiesznie. Na takiej stronie znajdują się także pola do wpisywania danych poufnych. Dlatego zawsze, gdy witryna internetowa wymaga podania poufnych danych, jak PESEL lub hasło do konta bankowego, należy zastanowić się, czy będzie to bezpieczne. Pamiętajmy – gdy adres strony, czyli link, zawiera nietypowe elementy, np. znak szczególny w środku słowa – powinno to wzbudzić naszą podejrzliwość.

Coraz częściej adres na pierwszy rzut oka wygląda poprawnie, ale po dokładniejszym przyjrzeniu się widać, że podmienione zostały **pojedyncze znaki**. Przykładowo, gdy litera „m” zostanie zamieniona na dwie litery „r” i „n” (czyli po połączeniu „rn”) wygląda to bardzo podobnie do „m”. Żeby upewnić się, czy adres strony nie został zmanipulowany, można go przekopiować do edytora tekstu i dokonać zmian czcionki. *(Żeby dowiedzieć się więcej na ten temat, zobacz krótki film pt. „Cyberbezpieczeństwo w praktyce” odc. 2 – „Rodzaje Cyberzagrożeń”).*



Rodzajów nieuczciwych internetowych praktyk jest więcej. Zwiedzeni nimi, możemy nasze oszczędności przekazać na coś, co w rzeczywistości nie istnieje.

Wyobraź sobie, że

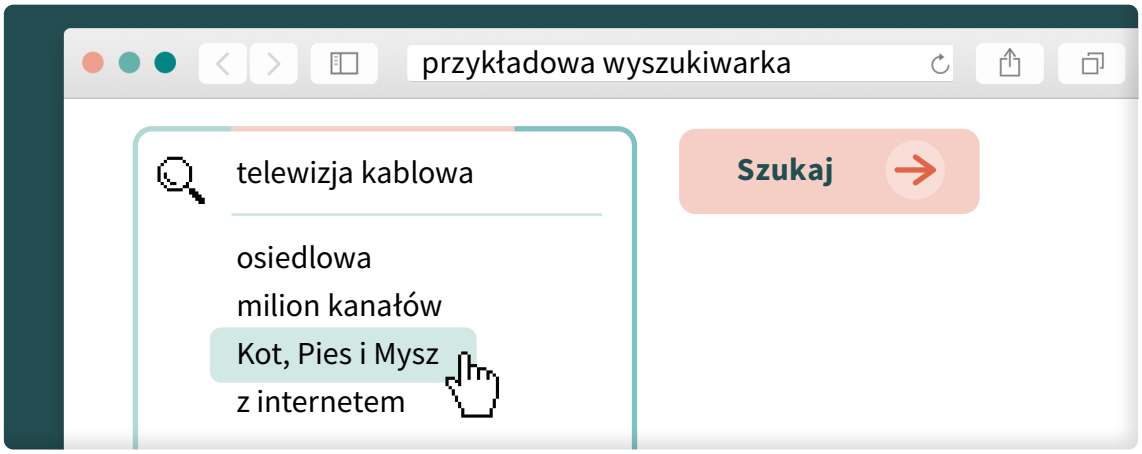
szukasz w sieci filmu, który od dawna masz w planach obejrzeć. Trafiasz na stronę oferującą legalny dostęp do rozrywki za dokonaniem opłaty. Niestety, po wykonaniu przelewu okazuje się, że dana pozycja filmowa wcale nie jest dostępna w serwisie, a strona proponuje obejrzenie czegoś innego.

Załóżmy, że

szukasz ulubionego serialu w internecie. Wyszukiwarka w odpowiedzi na Twoje zapytanie wyświetla listę stron. Widzisz, że są zaufane i że wyświetliły się w odpowiedzi na Twoje zapytanie o konkretny tytuł, więc przypuszczasz, że odnajdziesz tam upragniony serial. Zakładasz pochopnie płatne konto na danej stronie, po czym okazuje się, że wcale nie ma tam tego, czego szukasz.

O co tu chodzi? O to, że firmy mogą reklamować się też w wyszukiwarkach. Ich reklamy pokażą się, jeżeli wpiszemy określone słowa. Nie ma w tym nic złego, dopóki wyświetlają się w wynikach wyszukiwania naprawdę powiązanych z tym, co oferują. Dlatego **zanim założysz konto na jakiejś stronie** oferującej poszukiwaną przez Ciebie rozrywkę – upewnij się, że rzeczywiście znajdziesz tam to, czego szukasz.

Jak więc chronić się przed tego typu sytuacjami? Korzystać tylko z pewnych i polecanych stron, a przed odkryciem nowej skontaktować się z bliskimi w celu jej weryfikacji. Polecenia możesz zdobyć od bliskich, znajomych, rodziny czy innych użytkowników internetu.



PAMIĘTAJ

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

1. W pierwszej kolejności sprawdź, czy **adres** strony nie budzi Twoich podejrzeń.
2. Następnie zastanów się, czy na pewno chcesz **udostępnić informacje**, jakich wymaga strona (np. PESEL, numer konta bankowego).
3. Zawsze **dobrze się zastanów**, zanim wykonasz na stronie jakiekolwiek działanie. Spokojnie – masz tyle czasu, ile potrzebujesz. Nie ma pośpiechu.
4. Pamiętaj, aby skontaktować się z **bliskimi** w razie najmniejszych nawet wątpliwości.
5. Uważaj na nowe i nieznane strony z dostępem do rozrywki. Szukaj **sprawdzonych stron**, np. wykorzystując opinie innych użytkowników internetu.
6. Zanim założysz konto na jakiejś stronie – np. z filmami czy serialami – **upewnij się**, że rzeczywiście znajdziesz tam to, czego szukasz. Sprawdź wszystko dokładnie, zanim podejmiesz decyzję.

W parze z rozrywką idzie wiedza

ROZRYWKA I WIEDZA W INTERNECIE

W świecie cyfrowym możesz rozwijać pasje i zdolności. Kochasz gotować? Obserwuj najciekawsze blogi kulinarne. Fascynuje Cię technologia? Czytaj na bieżąco teksty na stronach poświęconych technologii. **Media społecznościowe** pełnią w tym wszystkim rolę kompendium wiedzy, bo za ich pomocą możemy śledzić ciekawe, najbardziej aktualne wydarzenia i szkolenia, wynajdować interesujące **blogi** i **strony internetowe** oraz na bieżąco dowiadywać się z nich nowych rzeczy.

Media społecznościowe *(za: „Słownik języka polskiego PWN”): „Technologie internetowe i mobilne, umożliwiające kontakt pomiędzy użytkownikami poprzez wymianę informacji, opinii i wiedzy”.*

Blog (za: „Słownik języka polskiego PWN”): „Dziennik prowadzony przez internautę na stronach WWW”.

Blog to strona internetowa prowadzona przez konkretnego użytkownika. Zawiera teksty o określonej z góry tematyce, np. na blogu podróżniczym zamieszczane są najczęściej wpisy ze zdjęciami, będące relacją z wyprawy autora. **Vlog** natomiast to filmowa wersja bloga. Nazwa powstała z połączenia słów „video” i „blog” – to znaczy, że zamiast artykułów, autor publikuje filmy. Blog różni się od serwisu rozrywkowo-informacyjnego osobistym charakterem, luźną formą i dbałością o komunikację z czytelnikami.

Serwisy informacyjno-rozrywkowe i blogi opierają się na **zaufaniu społeczności**. Im więcej znanych nam osób interesuje się jakąś witryną internetową, tym bardziej czujemy, że możemy zaufać jej autorowi. Linki prowadzące do treści na blogu są często publikowane w mediach społecznościowych, czyli na platformach, na których każdy użytkownik może podzielić się swoimi zdjęciami, filmami czy przemyśleniami.

WYSKAKUJĄCE BANERY I CICHE WIRUSY

Blogi i inne strony internetowe odkrywamy, eksplorując internetowe treści. Przy braku ostrożności i odpowiednich zabezpieczeń możemy trafić na złośliwe banery typu pop-up, które różnią się od zwykłych tego typu banerów tym, że sprowadzają na urządzenia wirusy.

ZŁOŚLIWE BANERY TYPU POP-UP *to szczególny przypadek banerów, które nagle i* ***niespodziewanie*** *pojawiają się na stronie internetowej. Kliknięcie w nie – najczęściej przypadkowe – sprawia, że wpadamy w sidła* ***złośliwego oprogramowania****.*

Załóżmy, że

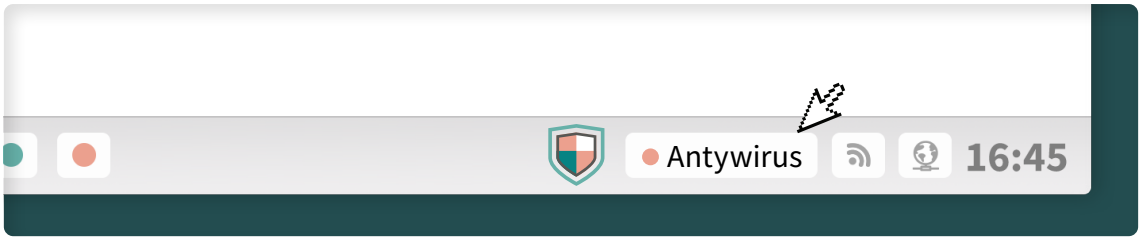
planujesz wybrać się niedługo na wycieczkę. Aby znaleźć inspiracje, szukasz ciekawych blogów podróżniczych albo stron internetowych o podróżach. Otwierasz przeglądarkę internetową, wpisujesz w wyszukiwarce np. „gdzie warto pojechać", naciskasz „enter" i klikasz w którąś z wyświetlonych pozycji. Strona nie budzi podejrzeń, aż nagle wyskakuje wielki baner na pół ekranu z podejrzaną treścią typu: „GRATULACJE! WYGRYWASZ SAMOCHÓD!!! KLIKNIJ TUTAJ!". Taki krzyczący niemal komunikat to jasny znak o zagrożeniu.

Co teraz? W przypadku zwykłych banerów typu pop-up szukamy na ich obrzeżach znaku „x", za pomocą którego zamyka się wyskakujący nagle komunikat.
W przypadku złośliwych banerów nie należy w nic klikać. Zamknij dane okno przeglądania i poszukaj innej strony. Jeżeli nie da się zamknąć danego okna, zamknij całą przeglądarkę i uruchom ją ponownie. Tym razem nie wchodź już na podejrzane strony internetowe.

WIRUS KOMPUTEROWY *– niepożądany program komputerowy, który utrudnia funkcjonowanie sprzętu oraz prowadzi do destrukcji znajdujących się na nim elementów. Przedostaje się na urządzenie użytkownika bez jego wiedzy. Powiela się i rozprzestrzenia na kolejne zasoby.*

Istnieją różne odmiany złośliwego oprogramowania, ale wystarczy wiedzieć, że istnieje wirus komputerowy, który niczym biologiczny wirus rozprzestrzenia się po sieci i urządzeniach, zdobywając dostęp do naszych zasobów. Występuje w bardzo różnych miejscach i w bardzo różnej postaci. Poza złośliwymi banerami typu pop-up można na niego trafić np. pobierając pliki z niezweryfikowanego źródła.

Przed wirusem komputerowym chroni **program antywirusowy**, o którym dowiesz się więcej z broszury **„Antywirus i zaślepka?”**. Pamiętaj, aby bardzo starannie selekcjonować to, w co klikasz, i nie robić nic bez namysłu. W przypadku banerów typu pop-up zamiast pochopnie klikać, poczekaj, aż strona internetowa się załaduje. Kontynuuj przeglądanie dopiero wtedy, gdy nie wyświetlą się żadne podejrzane treści.



PAMIĘTAJ

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

1. **Nie klikaj** w wyskakujące nagle banery typu pop-up ani żadne inne banery, które mają podejrzaną treść.
2. Po wejściu na stronę internetową spokojnie **poczekaj**, aż się załaduje, żeby nie kliknąć w nic przez przypadek.
3. Jeżeli zauważysz, że na Twoim urządzeniu występują podejrzane zmiany albo pliki, zachowaj spokój i **skontaktuj się z bliską osobą**, żeby ustalić dalsze działania.

Wystarczy wyszukać – rzecz o kłódkach

KTO SZUKA, NIE BŁĄDZI

Wyszukiwanie informacji na dowolny temat w dowolnym czasie i z dowolnego miejsca to wielka zaleta internetu. Otwórz zainstalowaną na Twoim urządzeniu przeglądarkę internetową. W pasku, umieszczonym na górze otwartej strony, wpisz hasło związane z informacją, jaką chcesz odnaleźć. Następnie kliknij w ikonę lupy, znajdującą się obok.

IKONA *(za: „Słownik języka polskiego PWN”): „W systemach operacyjnych lub programach komputerowych: obrazek symbolizujący program, plik lub operację”).*

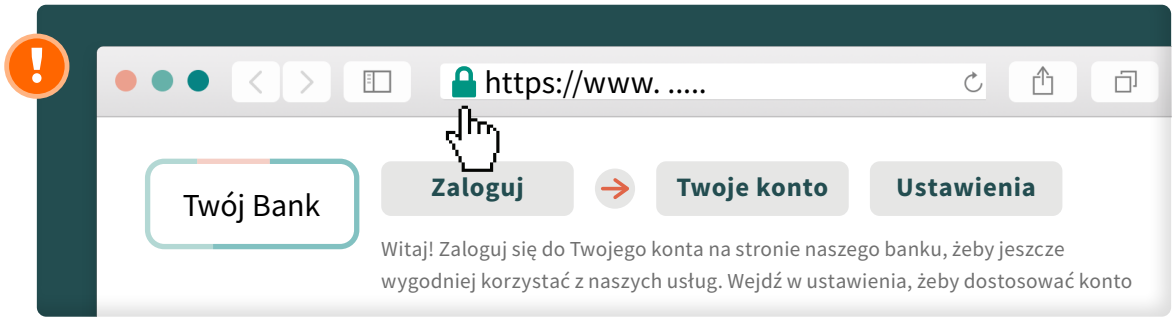
Szukanie informacji w internecie jest intuicyjne, bo podobnie odbywa się to zarówno z poziomu wyszukiwarki w przeglądarce, jak i z poziomu konkretnych już stron. Wyszukiwarka internetowa jest najczęściej punktem wyjścia do poszukiwań. Zamiast za pomocą wyszukiwarki, można też wpisywać interesujące nas treści od razu w polu adresu strony – na górze (**w miejscu z linkiem strony, czyli ciągiem znaków rozpoczynającym się od „https”**).

ZAUFANE STRONY INTERNETOWE, A TE Z KŁÓDKĄ

Wyobraź sobie, że

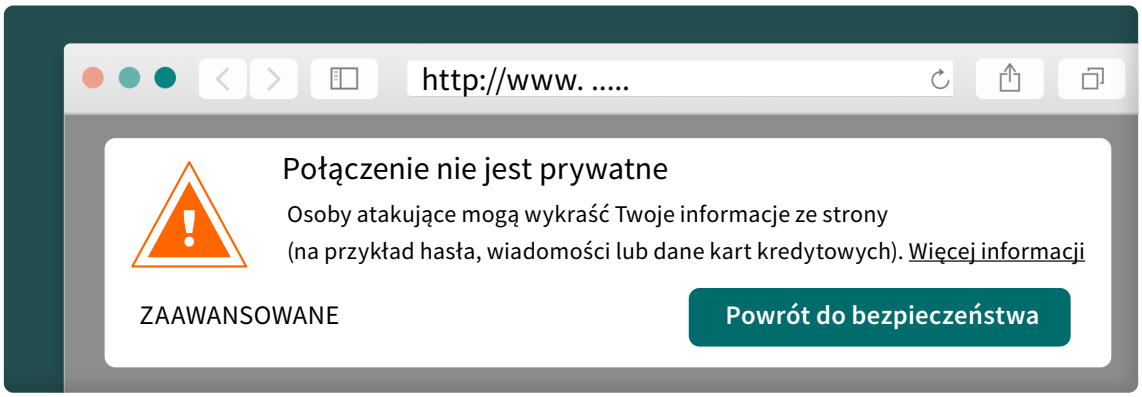
znajomy wysyła Ci np. link do transmisji spektaklu w komunikatorze lub za pomocą poczty e-mail. Załóżmy też, że wiesz już, że osoba, która do Ciebie napisała, jest tą, za którą się podaje, a link nie zawiera żadnych nietypowych elementów – np. błędów w zapisie. Możesz teraz kliknąć w link i przenieść się bezpośrednio do spektaklu lub skopiować link i wkleić go w pasek z adresem w wyszukiwarce. Ale czy to na pewno wszystko?

Warto jeszcze zwrócić uwagę, czy połączenie na danej stronie jest szyfrowane. Po otwarciu witryny, w której będziemy np. podawać nasze dane do logowania, powinniśmy w adresie www strony (link zaczynający się od „https”) zobaczyć **ikonę zielonej kłódki**. Po kliknięciu w nią, w zależności od rodzaju przeglądarki, z jakiej korzystamy, zobaczymy informacje o certyfikacie bezpieczeństwa i prawdziwości danej witryny. Cechą szczególną takiego połączenia będzie adres strony rozpoczynający się od **„https”** zamiast „http”. Dotyczy to każdej strony internetowej, która wymaga logowania i rejestracji, ale też innych witryn internetowych. *(Więcej informacji w filmie pt. „Bądź CYBERBEZPIECZNY 2020: Odc. 2. Fałszywe strony bankowe – zawsze sprawdzaj pasek adresu!”).*



Takie rozwiązanie powinno ochronić użytkowników przed oszustami, którzy – aby wyłudzić nasze dane i zyskać dostęp do naszych środków finansowych – tworzą **strony niezwykle podobne do tych prawdziwych**. *(Przypomnij sobie, czym jest phishing – wróć do informacji ze strony 4)*. Oczywiście oszuści mogą wpaść na sposób, aby obejść i to zabezpieczenie, np. stosując szyfrowanie komunikacji z ofiarą – kiedy również wyświetlana jest kłódka. Dlatego należy pamiętać, że poleganie **wyłącznie na kłódce nie będzie wystarczające**. Zawsze trzeba opierać się na dodatkowych sposobach weryfikacji, bo nigdy jeden sposób nie jest idealny.

Po weryfikacji linka oraz po kliknięciu w kłódkę i przeczytaniu podanych tam informacji należy zwrócić też uwagę na wygląd samej strony. Czy jest przyjazna w odbiorze i wykazuje dbałość o bezpieczeństwo naszych danych? Czy w internecie nie funkcjonuje już podobna do niej witryna?



Weryfikację bezpieczeństwa źródła warto też przeprowadzić z poziomu samej wyszukiwarki. O podejrzanej stronie poinformuje nas zainstalowany **program komputerowy** i sama **przeglądarka**. *(Więcej na ten temat w broszurze „Antywirus i zaślepka? Wszystko, co musisz wiedzieć o programach i narzędziach zwiększających Twoje bezpieczeństwo w sieci. Poradnik dla seniora”).*

PAMIĘTAJ

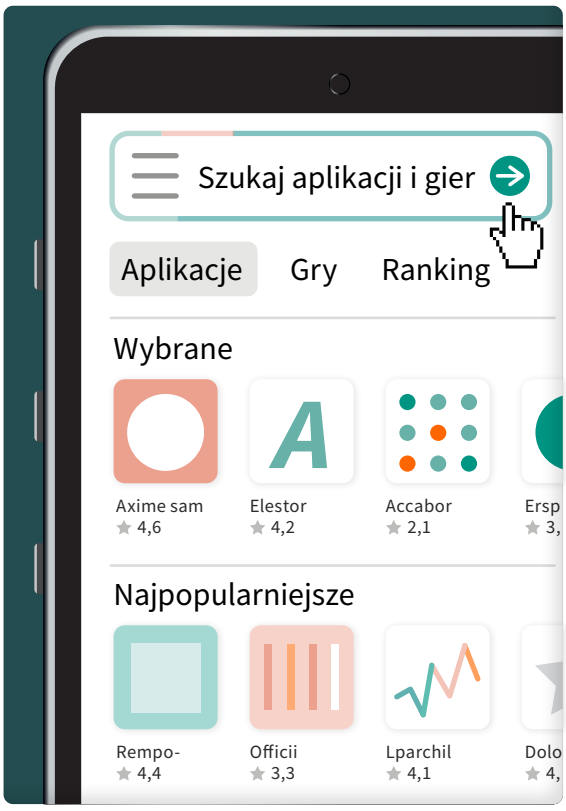
Po wnikliwym zapoznaniu się z tym podrozdziałem, wiesz już, o czym musisz zawsze pamiętać.

1. Sprawdzaj, czy w adresie strony internetowej nie ma **błędów ani literówek** oraz **nietypowych znaków**.
2. Zwróć uwagę, czy połączenie jest **szyfrowane** („https” zamiast „http” w pasku adresu) oraz sprawdź obecność ikony **zielonej kłódki** w wyszukiwarce dla danego linka.
3. **Przyjrzyj się** stronie – czy wzbudza Twoje zaufanie i czy dba o bezpieczeństwo Twoich danych?
4. Pamiętaj, że dostępne zabezpieczenia mogą nie być wystarczające, dlatego zawsze zachowaj zdrowy **rozsądek**.

Aplikacje aplikacjom nierówne

APLIKACJE MOBILNE, CZYLI CO?

Na koniec warto też wspomnieć o ułatwiających życie aplikacjach mobilnych. Żeby je pobrać, poproś bliskich o pomoc w znalezieniu na smartfonie **ikony ze sklepem z aplikacjami**. Określ interesującą Cię kategorię i eksploruj dostępne aplikacje lub wyszukaj konkretną, w taki sposób, jak wyszukujesz informacje w wyszukiwarce internetowej. Znajdź ciekawą grę albo program z fiszkami do nauki. Ty decydujesz, czy pobrać darmową, czy płatną wersję – w sklepie z aplikacjami wszystko powinno być czytelnie oznaczone.



APLIKACJA *(za: „Bezpieczeństwo online: Odc. 2 – Bezpieczeństwo aplikacji") to „ogólna nazwa oprogramowania działającego na urządzeniach przenośnych". (Dowiedz się więcej pod tym linkiem: z filmu pt. „Bezpieczeństwo online: Odc. 2 - Bezpieczeństwo aplikacji").*

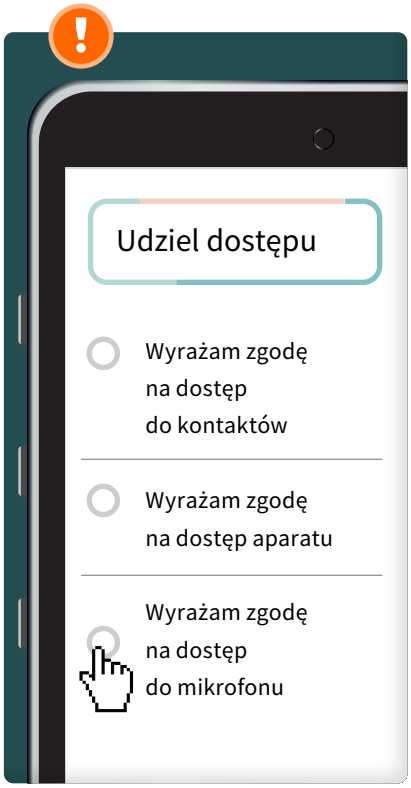
APLIKACJA MOBILNA *to rodzaj oprogramowania, które można łatwo i szybko pobrać na smartfona. Kategorie w sklepie z aplikacjami są szerokie i obejmują różne dziedziny, takie jak: gra, film, muzyka, nauka i inne.*

BEZPIECZNIE Z APLIKACJAMI

Zanim zainstalujesz aplikację na swoim telefonie, najpierw ją sprawdź – jej opis, opinie o niej – oraz dowiedz się, **jakich zgód od Ciebie wymaga**.

Wyobraź sobie,

że pobierasz taką z przepisami kulinarnymi, a ona żąda dostępu do Twojej kamery i kontaktów. Taka sytuacja od razu powinna wzbudzić Twoje podejrzenia. Podobnie, gdy chcesz zainstalować na smartfonie powszechnie znaną i używaną aplikację, która w sklepie nie ma żadnych opinii innych użytkowników i pobrań. Nie powinno się jednak skończyć na podejrzeniach, a na zrezygnowaniu z jej pobrania.



Podczas instalacji aplikacja najczęściej prosi o zgodę na dostęp do zasobów urządzenia, np. kontaktów, kamery, mikrofonu. Uważnie sprawdź, czy wszystko, o co prosi, rzeczywiście jest jej potrzebne do prawidłowego działania. Jeśli uważasz, że aplikacja wymaga dostępu do zbyt wielu funkcji – lepiej zrezygnuj z jej zainstalowania i używania. To Twoja **prywatność** i Twoja decyzja.

Pobieranie aplikacji powinno się przede wszystkim odbywać z dedykowanych do tego źródeł. W przypadku aplikacji mobilnych – będzie to odpowiedni dla Twojego telefonu **sklep z aplikacjami**. W innym wypadku możesz trafić na niebezpieczny plik, który wyrządzi ogromne szkody.

Pamiętaj o zachowaniu bezpieczeństwa, także po upływie czasu od zainstalowania na swoim urządzeniu aplikacji mobilnej. Używane aplikacje **aktualizuj** – dużym ułatwieniem będzie ustawienie **automatycznej aktualizacji** aplikacji mobilnych. Te programy, z których już nie korzystasz – **usuwaj**. Jakie zagrożenia niesie za sobą brak takich działań? Szpiegowanie, przechwycenie smartfona czy kradzież danych osobowych. Nie daj się też oszustom, którzy wyślą do Ciebie SMS-a z linkiem do zaktualizowania aplikacji – zawsze wyszukuj aktualizacje **samodzielnie** z oficjalnych źródeł. *(Chcesz wiedzieć więcej? Zobacz film pt. „Bezpieczeństwo działań w sieci: Odc. 2 – Aktualizuj system i aplikacje”)*. Program antywirusowy na smartfona to dodatkowa pewność, że dane na Twoim urządzeniu będą bezpieczne. *(Jeżeli chcesz wiedzieć więcej, zobacz film pt. „Bezpieczeństwo płatności: Odc. 2 – Aplikacje mobilne”)*.

W przypadku bezpłatnych aplikacji warto mieć na uwadze dwie kwestie. Pierwsza jest związana z udostępnionymi danymi, ponieważ autor aplikacji zarabia w takim wypadku na reklamach, jakie wyświetlają Ci się w pobranym programie. Druga to mechanizm naciągania finansowego, czyli pobierania opłat za dodatkowe funkcjonalności. Ale spokojnie – aby tego uniknąć, wystarczy wyłączyć możliwość zakupu w aplikacjach. *(Zobacz jak w filmie pt. „Bezpieczeństwo online: Odc. 2 – Bezpieczeństwo aplikacji”)*.

PAMIĘTAJ

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

1. Pobieraj aplikacje tylko ze **sprawdzonych źródeł**, czyli oficjalnych sklepów z aplikacjami dla Twojego smartfona.
2. Przed pobraniem aplikacji sprawdź dokładnie **opis, opinie** o niej oraz przeczytaj, na co **wyrażasz zgodę** i jakie **informacje udostępniasz**, np. kontakty, aparat czy album ze zdjęciami.
3. **Aktualizuj** używane aplikacje mobilne i usuwaj nieużywane.
4. Zainstaluj **program antywirusowy** na smartfona.
5. Rozważ **wyłączenie** możliwości zakupu w aplikacjach.

Co już wiesz o bezpiecznej rozrywce w sieci?

- Wiesz, czym jest ***PHISHING, ZŁOŚLIWE BANERY TYPU POP-UP I WIRUS KOMPUTEROWY***.
- Wiesz, na jakie formy ***NIEUCZCIWYCH PRAKTYK FINANSOWYCH I WYŁUDZEŃ*** w internecie trzeba uważać podczas korzystania z rozrywki, stron i blogów w internecie.
- Wiesz, jak sprawdzić, czy witryna internetowa jest ***BEZPIECZNA***.
- Wiesz, o czym pamiętać, pobierając ***APLIKACJĘ MOBILNĄ***.

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 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