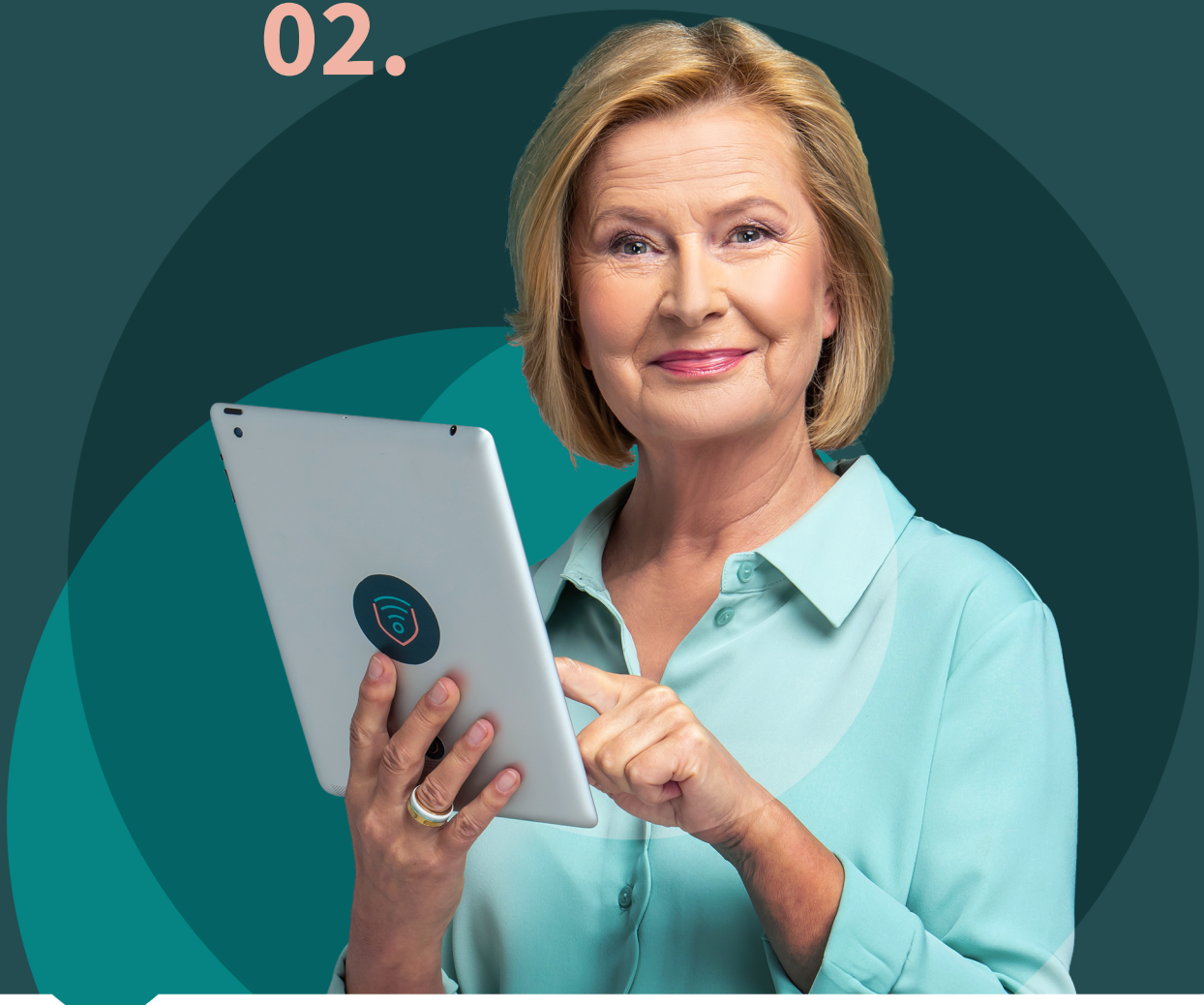
SENIORZE
spotkajmy się w sieci

E-mail i media społecznościowe?

Wszystko, co musisz wiedzieć
o bezpiecznej komunikacji w sieci.

Poradnik dla seniora

02.



Partner kampanii:

WARSZAWSKI INSTYTUT BANKOWOŚCI

Fundusze Europejskie Polska Cyfrowa

KPRM

NASK

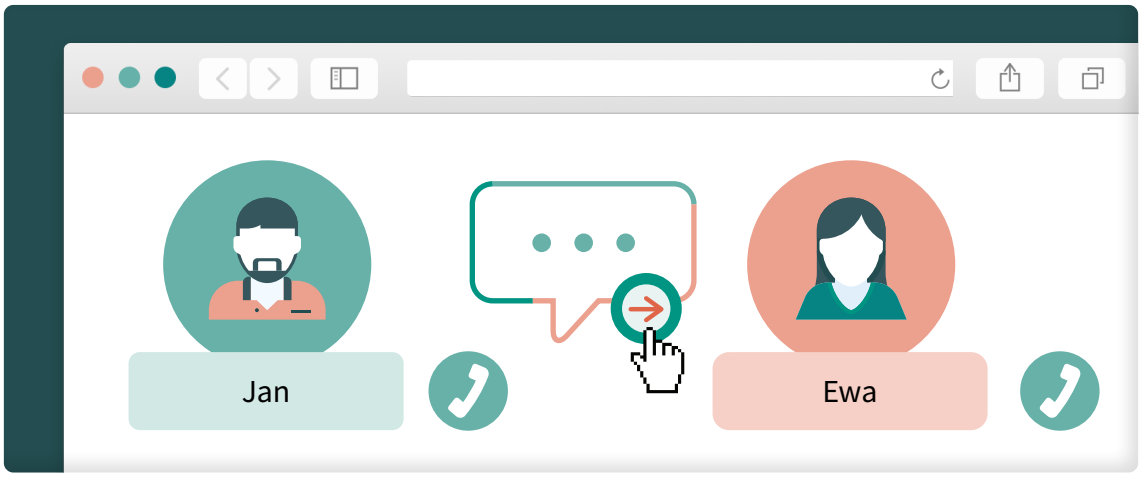
Unia Europejska
Europejski Fundusz Rozwoju Regionalnego

WITAJ!

W tym przewodniku przeprowadzimy Cię przez najważniejsze wątki związane z bezpiecznym komunikowaniem się w internecie. Jeśli chcesz dowiedzieć się więcej – *kliknij w aktywny link* i zobacz pozostałe broszury oraz filmy instruktażowe z Barbarą Bursztynowicz. Jeżeli coś będzie dla Ciebie niejasne albo wzbudzi Twoje wątpliwości – zwróć się **do bliskich o pomoc**.

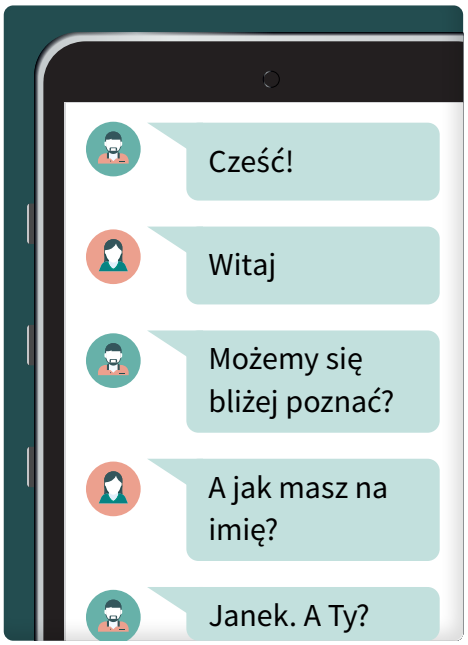
Barbara to osoba, która nabyła już trochę doświadczenia w internecie. Kiedy więc w filmie *„E-mail i media społecznościowe, czyli o bezpiecznej komunikacji w internecie”*, otrzymała na skrzynkę e-mail kolejne powiadomienie o wygranym konkursie, od razu wiedziała, że powinna je zignorować. Wysyłanie komuś takich informacji przypomina wrzucanie niechcianych ulotek do czyjejś skrzynki pocztowej. Barbara wie też, że za pomocą kilku kliknięć może sprawić, że nie będzie już otrzymywała takich internetowych ulotek od nieproszonych nadawców.
Ma też świadomość, że **nie może ufać wszystkim wiadomościom**, jakie dostaje, nawet jeżeli wysyłają je zaufane osoby czy instytucje. Zawsze zwraca również uwagę na to, **co publikuje w mediach społecznościowych**.

Za pomocą internetu można **szybko i wygodnie** skontaktować się z bliskimi osobami, znajomymi, rodziną albo dowolną instytucją czy firmą. Warto przy tym pamiętać, że nie zawsze osoba, która podaje się za kogoś, kogo znamy lub komu ufamy, rzeczywiście nią jest. Nie należy też wierzyć we wszystko, co ktoś komunikuje w internecie. Zawsze trzeba zachować **ostrożność** i gdy tylko zajdzie taka potrzeba – prosić bliskich o wsparcie.



Nie ufaj bezgranicznie internetowej społeczności

O CO CHODZI Z TYMI MEDIAMI SPOŁECZNOŚCIOWYMI?



Za pomocą **mediów społecznościowych** i **komunikatorów** można rozmawiać z dowolnie wybraną osobą i w dowolnie wybranym czasie oraz miejscu. Z narzędzi tych korzystamy często, gdy chcemy wysłać komuś prywatną wiadomość, bo akurat nie mamy możliwości do tej osoby zadzwonić czy porozmawiać z nią bezpośrednio.

Z kolej gdy mamy ochotę podzielić się czymś z szerszym gronem odbiorców, np. swoimi zainteresowaniami albo przemyśleniami, możemy napisać wpis *(treść publikowana w mediach społecznościowych w formie **tekstu, zdjęcia, animacji, filmu czy linku**)* lub komentarz. Media społecznościowe służą nie tylko do rozmów z **bliskimi, rodziną czy przyjaciółmi**, ale także z różnymi **społecznościami** (np. grupami zainteresowań), **firmami i organizacjami**.

Media społecznościowe to powszechne narzędzie do rozmów. Umożliwiają komunikację w bardzo szerokim zakresie. Jako że sami wybieramy społeczność, z którą się kontaktujemy, mamy większe zaufanie do treści pojawiających się w wybranym przez nas serwisie. Zakładamy, że wszyscy są w niej szczerzy i nie mają złych intencji, gdy dzielą się swoimi przemyśleniami. Na **zaufaniu** do społeczności opieramy czasami przekonanie, że zachowanie bezpieczeństwa w mediach społecznościowych nie wymaga **szczególnej uważności**. Ale czy na pewno?

FAKE NEWS CZYLI NIEPRAWDZIWE WIADOMOŚCI

FAKE NEWS *(ang. – fałszywe wiadomości): **nieprawdziwa informacja**, rozpowszechniana na szeroką skalę w celu uzyskania z tego tytułu różnego rodzaju **korzyści**. Cechą charakterystyczną fałszywych wiadomości jest ich **sensacyjny charakter**, który prowadzi do wyrobienia u odbiorców określonego poglądu.*

Można rozumieć to zjawisko jako masowo rozprzestrzenianą za pomocą internetu plotkę, której celem jest **wzbudzenie silnych emocji u wielu odbiorców**. **Fałszywe wiadomości** najczęściej nie mają żadnego związku z rzeczywistością. Sieją dezinformację, która jest jednym z największych zagrożeń obecnych czasów. Na rozprzestrzenianiu się fałszywych informacji korzystają różne osoby, posiłkujące się manipulacją do osiągnięcia własnych zysków.

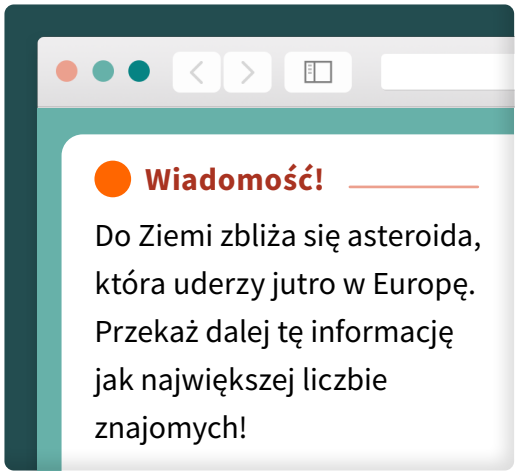
Fake news jest szczególnie powszechny w internecie, ponieważ za jego pośrednictwem można dotrzeć do bardzo **szerokiej grupy odbiorców w krótkim czasie i przy niewielkim wysiłku**. W mediach społecznościowych rozprzestrzenia się wyjątkowo szybko i czasami trudno zorientować się, kto jest autorem komunikatu. Dlatego, mimo że fake news funkcjonuje na różnych płaszczyznach, jest szczególnie niebezpieczny właśnie tutaj.

Jak go rozpoznać?

Najczęściej są to publikacje zawierające **tendencyjne nagłówki oraz grafiki**, które przykuwają uwagę odbiorcy i próbują kształtować jego przekonania. Innym przejawem tego zjawiska mogą być wpisy, w których ktoś powołuje się na dane liczbowe, ale nigdzie nie wskazuje ich **źródła**. Nie tylko tego typu treści, ale też wszystkie inne, które mają charakter opiniotwórczy, powinny być zawsze **weryfikowane** przez odbiorcę w innych źródłach, zanim się im zaufa.

A zatem, aby chronić się przed fałszywymi wiadomościami, szczególnie w mediach społecznościowych, należy zawsze wnikliwie zapoznać się z poruszanym tematem i sięgnąć do **innych źródeł**. Nie zaszkodzi też dwa razy się zastanowić, zanim weźmiemy udział w gorącej dyskusji dotyczącej sensacyjnych treści – to może być fake news!

Warto też pamiętać, że fake newsy krążą nie tylko w mediach społecznościowych. Zjawisko to występuje w **całym internecie**, np. w formie artykułów o krzykliwych nagłówkach, które wprowadzają w błąd, bo dopiero po przejściu na stronę okazuje się, że z tekstu nic nie wynika i jest to na przykład **ukryta reklama albo próba wyłudzenia danych**.



Sytuację dodatkowo komplikuje to, że każde nasze działanie, np. reakcja na taki fake news, zostaje **zapamiętane** w sieci – internet nie zapomina.

PRYWATNOŚĆ W MEDIACH SPOŁECZNOŚCIOWYCH A ŚLAD CYFROWY

ŚLAD CYFROWY *– informacje o nas, które zostają zapisane na serwerze. Ślady cyfrowe dzielą się na te podawane przez nas, np. dane osobowe oraz na informacje o wykonywanych przez nas czynnościach w internecie.*

SERWER *(za: „Słownik Języka Polskiego PWN"): „W sieciach komputerowych: komputer lub program przeznaczony do obsługi użytkowników przez udostępnianie ich komputerom swoich zasobów i wykonywanie otrzymanych poleceń".*

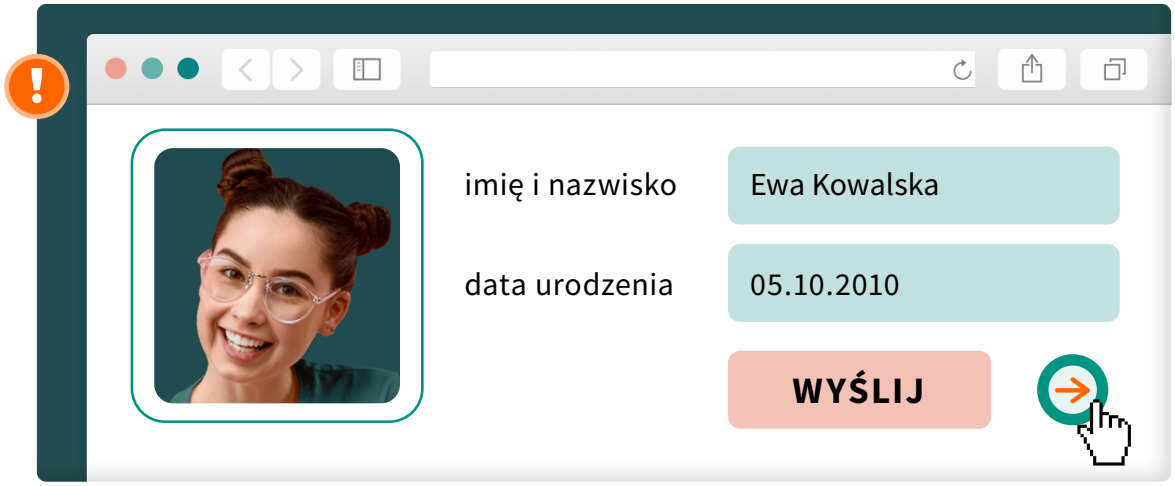
Jak to rozumieć?

Najprościej mówiąc – wszystko, co robimy w internecie, zostawia ślad. (Dowiedz się więcej na ten temat z *filmu pt. „Bądź CYBERBEZPIECZNY 2020: Odc. 3. To, co robisz w internecie jest dostępne NA ZAWSZE i DLA KAŻDEGO"*). Wyobraź sobie, że podczas zakładania konta w mediach społecznościowych podajesz **datę swoich urodzin** albo **miejsce zamieszkania**. Takie informacje są stale przechowywane przez właściciela konkretnej strony albo aplikacji. Posiada on swego rodzaju zbiór wiadomości o wszystkich użytkownikach, często nawet wtedy, gdy usuną oni swoje konta. Dane pozostają zapisane w specjalnym miejscu, a **dostęp** do nich na ogół ma nie tylko właściciel aplikacji, ale też na przykład reklamodawcy.

Wyobraź sobie, że

publikujesz w mediach społecznościowych **zdjęcie z rodziną**, np. z wnukami. Takie zdjęcie również, po jego usunięciu, pozostaje w posiadaniu **właściciela serwisu**. Dlaczego? Ponieważ zamieszczasz te treści w przestrzeni, którą on udostępnia. Dlatego, nawet gdy skasujesz zdjęcie lub inne treści i nie będą one widoczne dla Ciebie ani członków Twojej społeczności, to **dane historyczne**, czyli co i kiedy zostało opublikowane, niezmiennie będą zapisane na **serwerze**, czyli w miejscu, do którego ma dostęp właściciel strony.

Jakie niesie to zagrożenia i o czym w związku z tym należy pamiętać? Zanim poda się gdzieś dane osobowe, trzeba przede wszystkim dobrze **zastanowić się**, czy nie ma ryzyka, że zostaną one wykorzystane przez reklamodawców albo przejęte przez inne niepowołane osoby. Warto przemyśleć, jakie zdjęcia publikujemy w internecie, a jeśli nie przedstawiają tylko nas – wcześniej **uzyskać zgodę** osoby, która znajduje się na fotografii. Nawet skasowane fotografie nie znikną całkowicie z sieci.



Jeśli więc nie chcesz, aby jakieś informacje na temat Ciebie lub Twoich bliskich były wykorzystane – **nie podawaj ich**. Pamiętaj też o odpowiednich *ustawieniach prywatności* i możliwości korzystania z wyszukiwarki w **trybie prywatnym**.
A jeśli jesteś już aktywny w sieci i mniej lub bardziej regularnie publikujesz tam zdjęcia czy filmy, na których jesteś nie tylko Ty, ale też Twoi bliscy przeczytaj też *artykuł pt. „Sharenting i wizerunek dziecka w sieci”* o zagrożeniach związanych z udostępnianiem treści o dzieciach lub wnukach.

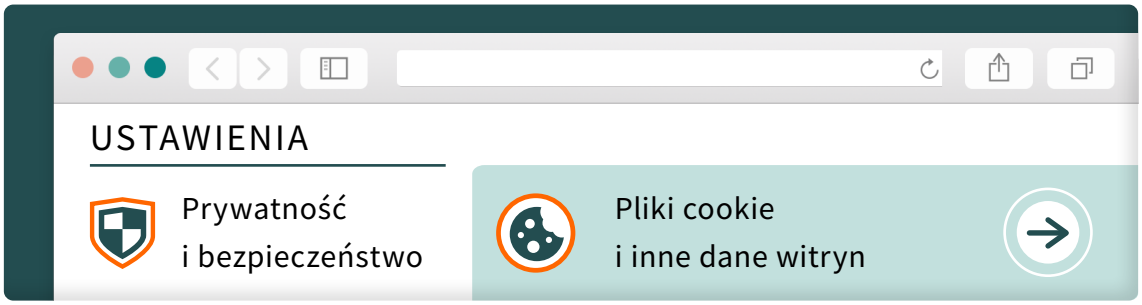
No dobrze, ale czym właściwie są te ustawienia prywatności?

> ***USTAWIENIA PRYWATNOŚCI*** *to zbiór ustawień, dających możliwość ograniczenia grupy odbiorców, do których trafią komunikowane przez nas treści.*

Ostrożność w internecie nie oznacza od razu, że mamy rezygnować z korzystania z jego dobrodziejstw. Może chciałbyś, żeby Twoje posty w mediach społecznościowych wyświetlały się jedynie zaufanemu gronu odbiorców, a nie wszystkim użytkownikom sieci? Wolałabyś też, żeby obce osoby nie mogły znaleźć Twojego profilu w serwisie społecznościowym i żeby wiadomości pisali do Ciebie tylko znajomi? Wystarczy, że wejdziesz w zakładkę **ustawienia** i **zaznaczysz potrzebne pola** (np. „widoczne tylko dla znajomych” zamiast „widoczne dla wszystkich”), następnie **zapiszesz zmiany** – i gotowe!

Podobnie jest w całym internecie. Jeżeli nie chcesz, aby informacje o tym, co wyszukujesz w sieci, były gromadzone – wejdź w ustawienia **wyszukiwarki**, z której korzystasz, zaznacz odpowiednie opcje (np. „blokuj pliki cookies") i zapisz zmiany. Gdy nie chcesz, aby **strony internetowe** gromadziły informacje na Twój temat – nie akceptuj **warunków korzystania** z tak zwanych **plików cookies** *(ang. ciasteczka – małe pliki, w których zamieszczona jest np. informacja o odwiedzanej przez nas stronie internetowej)*. To od Ciebie zależy, kto i jak skorzysta z udostępnianych przez Ciebie informacji.

Zawsze też możesz zmienić zdanie. Jeżeli podasz swoje dane na jakiejś stronie, **masz prawo do skontaktowania się z danym serwisem i poproszenie o ich usunięcie**.



PAMIĘTAJ

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

1. Traktuj **z dystansem** informacje, które pojawiają się w internecie, szczególnie w mediach społecznościowych.
2. Zanim wyrobisz sobie opinię na podstawie udostępnionych przez kogoś materiałów, a co więcej – wyrazisz ją – **zastanów się dwa razy**. Przed wdaniem się w dyskusję zweryfikuj prawdziwość podawanych informacji.
3. Przed każdą **publikacją, wysłaniem lub udostępnianiem treści w sieci**, szczególnie w mediach społecznościowych, zastanów się, czy jest to dobry pomysł i czy Twoje działanie nie stanowi dla nikogo problemu lub zagrożenia.
4. Decyduj, kto powinien mieć **dostęp do informacji** na Twój temat i zawsze pamiętaj o **ustawieniach prywatności**.

Poczta w internecie jak w skrzynce pocztowej?

KIEDY KORESPONDENCJA PRZENOSI SIĘ DO INTERNETU

Poczta e-mail jest równie popularnym środkiem komunikacji co media społecznościowe. Ma jednak bardziej **formalny** charakter oraz często nieco **dłuższy czas oczekiwania na odpowiedź**.

E-mail służy do komunikacji z bliskimi, różnymi firmami i instytucjami. Dzięki poczcie elektronicznej możemy skontaktować się np. ze sklepem internetowym, który przekaże nam najświeższe informacje odnośnie do złożonego zamówienia, otrzymamy też wiadomość z potwierdzeniem rejestracji konta na portalu pacjenta czy o założeniu nowego konta w banku.

Internetowa skrzynka pocztowa to duże ułatwienie w komunikacji we współczesnym świecie i warto ją założyć. Należy jednak pamiętać, że nawet jeżeli wydaje nam się, że dysponujemy wystarczającymi zabezpieczeniami lub ufamy narzędziu, z którego korzystamy, zawsze trzeba zachować **ostrożność**.

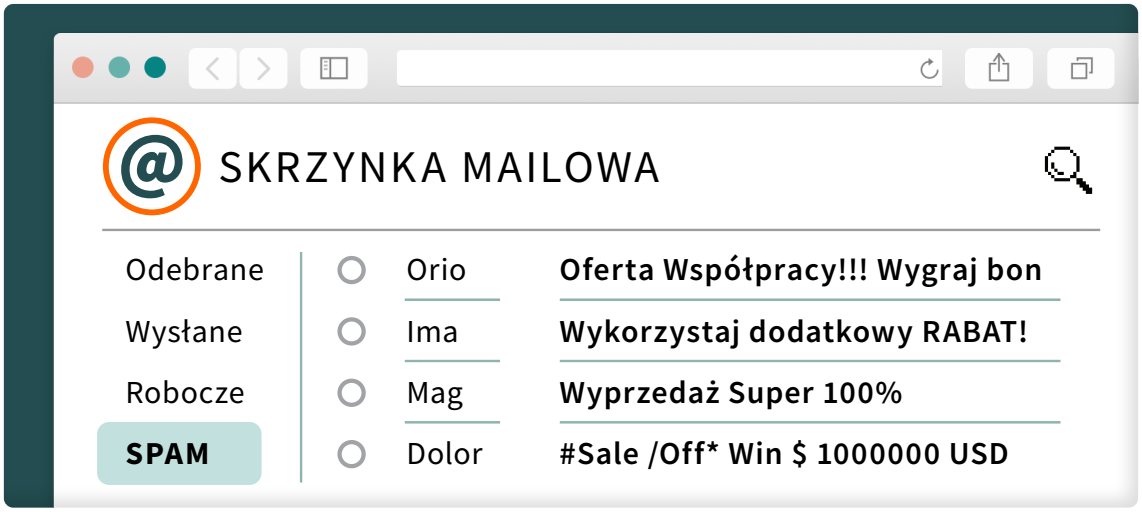
INTERNETOWE ULOTKI, CZYLI SPAM

W broszurze na temat bezpiecznej rozrywki w internecie *„Spektakl i film? Wszystko, co musisz wiedzieć o bezpiecznej rozrywce w sieci”* jest mowa o **phishingu** *(ang. fishing – wędkowanie)*. To zjawisko, na które narażeni są także użytkownicy poczty e-mail. Oszuści podszywając się pod zaufanego nadawcę, wysyłają e-maile, które na pierwszy rzut oka nie wzbudzają podejrzeń odbiorcy. Po wnikliwej analizie wiadomości dowiadujemy się jednak, że za jej pomocą cyberprzestępcy chcą uzyskać dostęp do naszych kont bankowych lub skłonić nas do pobrania zawirusowanego pliku. (Dowiedz się więcej o zagrożeniach związanych z korzystaniem z poczty e-mail – obejrzyj *film pt. „Bezpieczeństwo online: Odc. 1 – Niebezpieczne strony”*). Phishing w kontekście poczty elektronicznej jest częścią szerszego zjawiska – tak zwanego spamu.

> **SPAM** *to niepożądana wiadomość wysyłana na masową skalę, najczęściej (choć nie tylko) za pomocą poczty elektronicznej.*

Spam otrzymany pocztą e-mailową można porównać do, przytoczonych na początku poradnika, **niechcianych ulotek z niezaufanego źródła, zapychających skrzynkę pocztową**. Zaliczają się do niego zarówno natarczywe treści **reklamowe**, jak i groźne próby **naciągnięcia** czy **wyłudzenia**.

Nowocześniejsze i bardziej zaawansowane serwisy poczty e-mail oferują w ramach posiadanego konta pocztowego specjalne katalogi, które niczym pudełka albo segregatory, porządkują wiadomości różnego rodzaju. Zawierają kilka **kategorii katalogów**, np. wiadomości odebrane czy **wiadomości typu „spam”**. Takie **katalogi** nie tylko doskonale organizują elektroniczną korespondencję i pomagają się w niej szybko odnaleźć, ale także zwiększają nasze bezpieczeństwo. Podejrzane wiadomości trafiają od razu do specjalnych folderów, w związku z czym użytkownik nie ma z nimi styczności.



Żadne rozwiązania nie są jednak doskonałe, ponieważ oszuści stale udoskonalają swoje techniki, dostosowując działania do rozwijającej się technologii. Dlatego, może zdarzyć się, że wiadomość z próbą **wyłudzenia naszych pieniędzy** lub zawierająca **wirusa** do pobrania, wcale nie trafi do folderu „spam”. W związku z tym zawsze należy zachować ostrożność.

Może też zdarzyć się sytuacja odwrotna – że do folderu z wiadomościami typu spam wpadnie wiadomość od zaufanego nadawcy, na którą czekamy. Lepiej jednak, aby program działał nadmiernie ostrożnie niż niewystarczająco skutecznie. Po skontaktowaniu się z osobą, na której wiadomość czekamy i wejściu w folder „spam”, w każdej chwili możemy **oznaczyć korespondencję jako bezpieczną**. Samo wejście do folderu niczym nie grozi – nie oznacza jeszcze otwarcia potencjalnie groźnych wiadomości.

Dlaczego warto uważać na spam i postawić na pocztę e-mail, która za nas schowa niechciane wiadomości do specjalnego folderu? Ponieważ spam to wiadomości, które mogą być źródłem licznych zagrożeń.

Dlatego należy zawsze mieć **ograniczone zaufanie** do przychodzących wiadomości. Nie tylko do tych z **błędami** i nawołujących do **natychmiastowego działania**, ale także tych, w których adresat powołuje się na **zaufanego nadawcę**, a wiadomość nie sprawia na pierwszy rzut oka wrażenia podejrzanej.

PAMIĘTAJ

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

1. **Zwróć uwagę**, czy serwis Twojej poczty elektronicznej oferuje wyłapywanie i odkładanie wiadomości typu spam do **specjalnego katalogu**.

2. Pamiętaj, że wiadomości typu spam mogą zawierać wirusa lub mieć na celu wyłudzenie od Ciebie informacji. Dlatego nic **nie pobieraj i nie podawaj** żadnych danych wrażliwych w odpowiedzi na tego typu e-maile.

3. Zawsze miej **ograniczone zaufanie** do przychodzących wiadomości – szczególnie, gdy ktoś w mailu powołuje się na **zaufaną instytucję albo markę** oraz wtedy, gdy wiadomość nie pojawia się w folderze „spam”.

4. Jeżeli w mailach pojawiają się **błędy**, a wiadomości nawołują do natychmiastowego **wykonania jakiegoś działania** – powinno to wzbudzić Twoje **podejrzenia**.

Spotkanie w sieci jak w rzeczywistym świecie?

ŚWIAT WIRTUALNY JAK REALNY

Możliwe, że czytając o kontaktowaniu się za pomocą mediów społecznościowych oraz poczty e-mail myślisz sobie: „No dobrze, ale ja jednak wolę zobaczyć i usłyszeć drugą osobę". Internet oferuje powszechne rozwiązania, **często darmowe**, które umożliwiają **komunikowanie się** nie tylko za pomocą tekstu pisanego, ale też **obrazu i dźwięku**. Do dyspozycji mamy **programy i platformy**, które dzięki dostępowi do internetu umożliwiają tak zwane wideospotkania. W tym celu stworzono wiele **zaufanych narzędzi** niewymagających żadnego pobierania ani instalacji – wystarczy przeglądarka internetowa.

WIDEOSPOTKANIA *– spotkania w świecie cyfrowym, które za pomocą dostępu do kamery i mikrofonu wbudowanych w urządzenie oraz dostępu do internetu umożliwiają zobaczenie i usłyszenie rozmówcy.*

Takie rozwiązania są powszechne, a w ramach wideorozmowy można też **udostępniać** drugiej stronie **swój ekran komputera** (wtedy użytkownik zamiast wizerunku rozmówcy lub poza nim widzi jego ekran) oraz najróżniejsze **pliki**. Oczywiście trzeba przy tym zachować niezbędne zasady bezpieczeństwa.

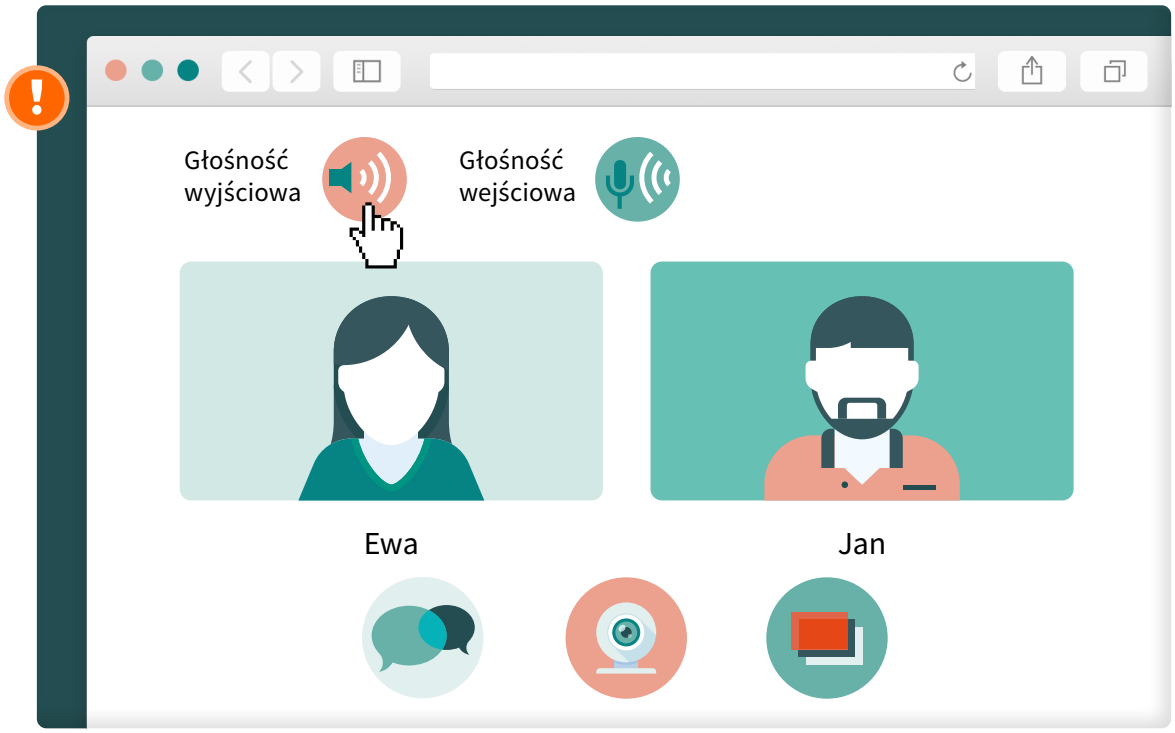
WIDZIMY SIĘ I SŁYSZYMY

Żeby się widzieć i słyszeć, **potrzebujemy kamery, głośników** oraz **połączenia internetowego**. Obecnie coraz rzadziej mówi się o kamerach internetowych, ponieważ większość osób korzysta z laptopów, tabletów czy smartfonów, które mają już wbudowane bardzo wysokiej jakości kamery.

KAMERA INTERNETOWA *– kamera, która umożliwia prowadzenie wideospotkania i dzielenie się z innym użytkownikiem swoim obrazem.*

Kamerę internetową można też dokupić w wielu miejscach i z łatwością zainstalować. Aby zachować pełne bezpieczeństwo, należy pilnować tego, żeby była **zasłonięta lub wyłączona, gdy z niej nie korzystamy** – sprzęt komputerowy coraz częściej ma wbudowaną specjalną **zaślepkę**, która pozwoli Ci zasłonić kamerę kiedy z niej nie korzystasz. Co właściwie mogłoby się stać, gdybyśmy nie zachowali niezbędnych środków ostrożności? Ktoś, kto zdobył dostęp do naszego urządzenia, mógłby wykraść **hasła do logowania** na nasze konta albo nas **podglądać**, czego nie musimy być nawet świadomi.

Żeby nawzajem się słyszeć, musimy mieć włączoną **głośność wyjściową i wejściową** na naszym urządzeniu.



Jeżeli mimo spełnienia tych warunków wystąpią niepowodzenia, może to oznaczać, że głośniki wbudowane w nasz laptop czy smartfon nie działają poprawnie, albo że źle podłączyliśmy słuchawki, z których postanowiliśmy korzystać podczas wideorozmowy. Podobnie jak w przypadku kamery, warto pamiętać, że możemy nieumyślnie nie wyjść z rozmowy i wciąż być na linii, mimo że uznaliśmy ją za zakończoną.

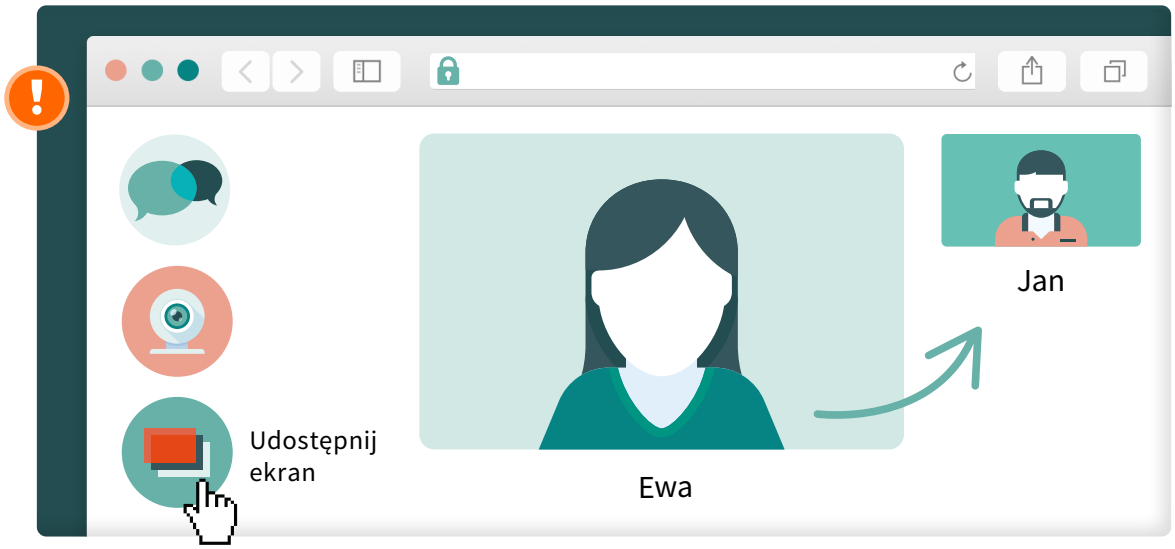
Zanim po zakończeniu rozmowy oddalisz się od komputera, upewnij się, że rozmowa została zakończona, a Twoja kamera jest zasłonięta.

Skoro mowa o bezpieczeństwie wszystkich elementów potrzebnych do przeprowadzenia wideorozmowy, to pamiętajmy, żeby **sieć, z której korzystamy, była bezpieczna**. Przykładowo, jeżeli jesteśmy w kawiarni i używamy tamtejszego połączenia internetowego, warto wiedzieć, że hakerzy mogą z łatwością włamać się do sieci i przejąć dostęp do danych osób, które z niej korzystały. Dlatego lepiej korzystać ze swojego internetu lub po prostu z zaufanego i pewnego źródła, szczególnie w przypadku wideorozmów. Wróćmy jednak do kwestii udostępniania ekranu lub plików.

***Udostępnienie** czegoś komuś w internecie oznacza podzielenie się w sieci z innym użytkownikiem jakąś treścią.*

Udostępnianie ekranu, szczególnie w kontekście wideorozmowy odbywającej się w czasie rzeczywistym, to wyświetlanie się użytkownikowi lub użytkownikom, z którymi prowadzimy rozmowę, zawartości naszego ekranu. Przykładowo – otwieramy na naszym komputerze pokaz slajdów ze zdjęciami i w tym samym czasie widzą je dokładnie inne osoby z konwersacji w taki sam sposób, jak gdyby siedziały obok nas. Natomiast **udostępnianie plików** to nic innego jak przesłanie ich za pomocą narzędzia do wideorozmowy pozostałym uczestnikom spotkania.

Tutaj powinna zaświecić nam się lampka, bo pokazanie komuś swojego ekranu w trakcie prowadzonej rozmowy albo wysyłanie i pobieranie plików powinno odbywać się nie tylko w sytuacji, **gdy połączenie jest bezpieczne**, ale też kiedy **osoba, z którą rozmawiamy, jest zaufana**. Jeżeli prowadzimy wideorozmowę w domowym zaciszu, z zaufanego połączenia i programu oraz z bliskimi osobami – nie musimy się obawiać. Jeśli cokolwiek budzi nasz niepokój – lepiej skontaktujmy się z kimś, kto pomoże nam sprawdzić, czy wszystko jest w porządku.



PAMIĘTAJ

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

1. Po zakończonej wideorozmowie zasłaniaj **kamerę** i **wyłączaj głośność wejściową**.
2. Zawsze korzystaj z **zaufanych programów** do wideokonferencji i **zaufanego połączenia internetowego**.
3. Zwracaj uwagę na to, **jakie pliki udostępniasz**. Za każdym razem zastanów się, czy pokazanie komuś swojego ekranu będzie dobrym rozwiązaniem.

Nawiązywanie nowych znajomości

CZY W INTERNECIE MOŻNA NAWIĄZAĆ PRAWDZIWĄ ZNAJOMOŚĆ?

Wiemy już trochę o bezpiecznym korzystaniu z internetu, ale co z poznawaniem nowych osób i szukaniem w internecie miłości albo przyjaźni na całe życie? W sieci znajdziesz **portale randkowe**, które powstały z myślą o osobach poszukujących nowych relacji. Wystarczy znaleźć **zaufany** portal (kierując się **opiniami** innych użytkowników i wszystkimi **zasadami**, o jakich dotychczas była mowa), założyć na nim **konto**, uzupełnić **informacje o sobie** i rozpocząć poznawanie nowych osób.

CZUJNOŚĆ PRZEDE WSZYSTKIM

Mimo że wielu osobom w bardzo różnym wieku udało się już w ten sposób zawrzeć znajomość, zawsze trzeba pozostać **czujnym**. Podobnie jak w świecie rzeczywistym, tak samo w wirtualnym, funkcjonują oszuści matrymonialni.

OSZUŚCI MATRYMONIALNI *to osoby, które wchodzą z nami w relację tylko po to, aby wykorzystać ją do własnych celów. Działając w internecie, mogą np. próbować zawrzeć z nami bliższą znajomość po to, aby* ***wyłudzić*** *od nas pieniądze. Oszuści uwodzą osoby korzystające z portali randkowych, stosując techniki oparte na* ***grze na emocjach****.*

Dlatego **nie przekazuj nigdy pieniędzy** osobie poznanej w internecie, nawet jeżeli masz wrażenie, że dobrze się już znacie i wszystko o sobie wiecie. Twoje pieniądze mogą przepaść równie szybko i bezpowrotnie, jak internetowa znajomość.

PAMIĘTAJ

Po wnikliwym zapoznaniu się z tym podrozdziałem wiesz już, żeby zawsze pamiętać o **ograniczonym zaufaniu** do **nowo poznanych osób w internecie**.

Co już wiesz o bezpiecznej komunikacji w sieci?

- Wiesz, czym jest ***FAKE NEWS*** i potrafisz go zdemaskować dzięki wnikliwemu weryfikowaniu informacji.
- Wiesz, jak bezpiecznie prowadzić ***WIDEOKONFERENCJE***.
- Wiesz, na co uważać, aby zachować ***PRYWATNOŚĆ*** swoją i bliskich w mediach społecznościowych i internecie.
- Wiesz, na co uważać, podczas szukania ***NOWYCH ZNAJOMOŚCI*** w internecie.
- Wiesz, z czym wiąże się ***SPAM*** i jak uchronić się przed zagrożeniami związanymi z pocztą e-mail.

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