CYBER
RESCUE

Bezpieczne Social Media

CYBER RESCUE

SPIS TREŚCI

NOTKA OD NAS 1

Drogi Czytelniku!

Fakt – media społecznościowe są już stałym elementem naszego życia. Niezależnie czy je uwielbiasz czy nie cierpisz, ich obecność w naszej codzienności jest niezaprzeczalna. Różne formy interakcji, łatwy dostęp do komunikacji, możliwość wymiany opinii, dzielenia się wiedzą, źródło nowinek ze świata, a ostatnio również robienie zakupów – ten szeroki wachlarz możliwości przyciąga nawet sceptyków.

Stale rosnąca popularność social mediów ma też swoją ciemną stronę. To wyjątkowo kuszące dla cyberoszustów środowisko, zapewniające anonimowość i potencjalne rzesze odbiorców. Właśnie z tego powodu dziś chcemy podzielić się z Tobą garścią przydatnych rad i podpowiedzieć jak bezpiecznie odnaleźć się w tej części cyfrowego świata.

To lektura dla każdego! Niezależnie do jakiej grupy wiekowej należysz i z ilu platform korzystasz – będzie to dla Ciebie doskonały przewodnik po socialowej cyberprzestrzeni.

Mamy nadzieję, że nasz eBook pomoże Ci uporządkować wiedzę, którą już posiadasz, a jednocześnie rozwieje wszystkie wątpliwości, jakie możesz mieć, korzystając ze swoich ulubionych social mediów.

Miłej lektury!

CYBER RESCUE

WSTĘP 2

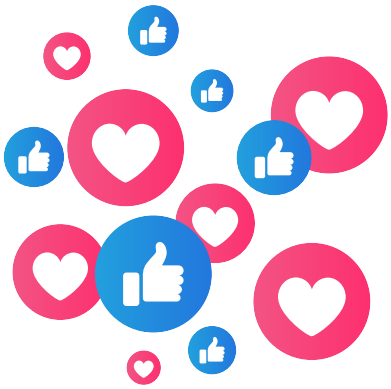
W dzisiejszym dynamicznym świecie, gdzie technologia odgrywa kluczową rolę w naszym codziennym życiu, media społecznościowe stały się integralną częścią cyfrowej egzystencji. Bez wątpienia te platformy umożliwiają nam łatwą komunikację, dzielenie się wspomnieniami czy utrzymywanie kontaktów z przyjaciółmi i rodziną na całym świecie. Jednak równocześnie stwarzają nowe wyzwania, związane z prywatnością, bezpieczeństwem online oraz potencjalnie negatywnym wpływem na nasze zdrowie psychiczne.

Badania wskazują, że blisko 80% użytkowników Internetu w wieku od 16 do 64 lat jest aktywnych na co najmniej jednej platformie społecznościowej*.

Paradoksalnie, tylko niewielki odsetek z użytkowników zdaje sobie sprawę z potencjalnych zagrożeń, związanych z nieodpowiednim korzystaniem z tych mediów. W tym eBooku chcemy zwrócić Twoją uwagę właśnie na te kwestie. Czytając go, poznasz nie tylko ciekawe dane statystyczne, ale przede wszystkim dostaniesz sporo bardzo praktycznych porad, jak bezpiecznie korzystać z social mediów!

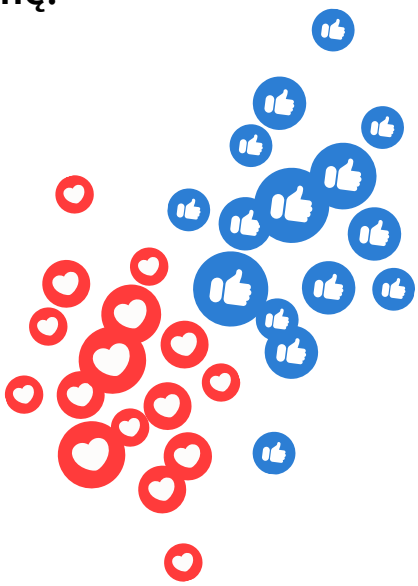
*Źródło: blog.hootsuite.com "The 50+ Important TikTok Stats Marketers Need to Know", 2024

CO TO SĄ SOCIAL MEDIA? 3



Media społecznościowe, nazywane też platformami lub sieciami społecznościowymi, to witryny i aplikacje, które umożliwiają użytkownikom tworzenie treści, ich udostępnianie i wymianę.

To miejsca, gdzie ludzie mogą się ze sobą komunikować, dzielić zdjęciami, filmami, myślami i doświadczeniami. Ich kluczową cechą jest dwustronność komunikacji – korzystający nie tylko odbierają treści, ale także sami je generują i udostępniają.



Początki mediów społecznościowych sięgają lat 90. XX wieku, kiedy powstały pierwsze platformy, umożliwiające zakładanie profili, tworzenie list znajomych i wymianę wiadomości. Jednak prawdziwy przełom nastąpił w pierwszej dekadzie XXI wieku, gdy narodziły się prawdziwe społecznościowe giganty, z których korzystamy do dziś.

SOCIAL MEDIA

Istniejące platformy proponują użytkownikom różne perspektywy. Do tych najpopularniejszych należą multizadaniowcy, dzięki którym zrobisz i znajdziesz praktycznie wszystko. Przykładem takiego serwisu jest Facebook, skupiający różnorodne społeczności, proponujący nie tylko podstawowe funkcje (np. rozmawianie i interakcje ze znajomymi), ale oferujący też tworzenie grup tematycznych, dyskusje na forach, a nawet zakupy.

Innym, coraz wyraźniejszym trendem są portale, kreujące bardziej precyzyjne społeczności, skupiające się na konkretnych zainteresowaniach i formatach. Do tej grupy możemy zaliczyć np. Instagram, przeznaczony dla miłośników fotografii, LinkedIn, skupiający profesjonalistów i TikTok, celujący w entuzjastów krótkich filmów. Każdy z tych serwisów ma swoje unikalne cechy i przyciąga różne grupy użytkowników.

POZNAJ NAJPOPULARNIEJSZE PLATFORMY!

FACEBOOK

Założony w 2004 roku przez Marka Zuckerberga, zaczynał jako platforma społecznościowa skierowana głównie do studentów, w tej chwili otwarta dla każdego. Użytkownicy mogą tworzyć profile, wrzucać aktualności oraz komunikować się za pomocą wiadomości, ale także tworzyć grupy zainteresowań, prowadzić otwarte lub zamknięte fora dyskusyjne, a nawet robić zakupy.

INSTAGRAM

Założony w 2010 roku przez Kevina Systroma i Mike'a Kriegera. Początkowo koncentrował się na dzieleniu się zdjęciami, a z czasem rozwinął się także w platformę do udostępniania krótkich filmów.

PINTEREST

Portal założony w 2010 roku przez Bena Silbermanna, Paula Sciarra i Evana Sharpa. Umożliwia użytkownikom odkrywanie, zbieranie i udostępnianie inspirujących obrazów i pomysłów na różnorodne tematy, takie jak moda, gotowanie, projektowanie wnętrz, sztuka czy podróże.

TIKTOK

Uruchomiony w 2016 roku przez chińską firmę ByteDance, stał się jednym z najgorętszych trendów w świecie mediów społecznościowych. Platforma skupia się na krótkich, kreatywnych filmach, umożliwiając użytkownikom szybkie dzielenie się swoją twórczością.

YOUTUBE

Założony w 2005 roku przez Steve'a Chen, Chad'a Hurleya i Jawed'a Karima. To jedna z największych platform wideo na świecie. Od chwili powstania stał się domem dla miliardów filmów, twórców treści i różnorodnych społeczności.

LINKEDIN

Założony w 2002 roku, to platforma społecznościowa skoncentrowana na środowisku zawodowym. Służy do nawiązywania kontaktów biznesowych, poszukiwania pracy oraz dzielenia się wiedzą i osiągnięciami branżowymi.

SNAPCHAT

Uruchomiony w 2011 roku przez Evana Spiegela, Bobby'ego Murphy'ego i Reggiego Browna, zrewolucjonizował sposób, w jaki ludzie dzielą się treściami wideo. To platforma, która skupia się na efemerycznych treściach, znikających po krótkim czasie.

X (DAWNIEJ TWITTER)

Założony w 2006 roku przez Jacka Dorseya, Evana Williamsa, Noaha Glassa oraz Biza Stone'a. Charakteryzuje się krótkimi wiadomościami tekstowymi, tzw. "tweetami" o maksymalnie 280 znakach. Jest to popularne miejsce do udostępniania informacji, np. wiadomości.

CYBER RESCUE

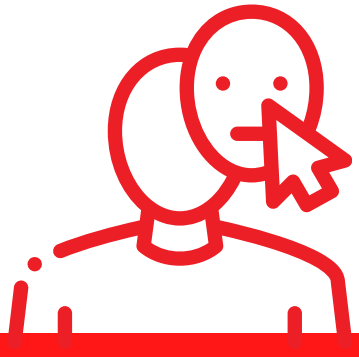
ZAGROŻENIA W SOCIAL MEDIACH 4

Zagrożenia związane z cyberbezpieczeństwem stanowią poważne wyzwanie dla użytkowników social mediów. W tym rozdziale przedstawiamy ich rodzaje i proponujemy praktyczne rozwiązania, które pomogą Ci zminimalizować ryzyko.

Poznaj najpopularniejsze metody cyberłobuzów!

PHISHING

Podszywanie się pod osobę lub instytucję. Takie ataki stają się coraz bardziej zaawansowane, oszuści wykorzystują m.in. fałszywe profile, linki i wiadomości. Użytkownicy są narażeni na próby wyłudzenia danych logowania czy informacji osobistych. Możesz przez to stracić kasę!



DEEPFAKE

Technologia, polegająca na manipulowaniu treściami wideo i audio, np. podkładanie głosu do nagrania. Dzięki niej można z ogromną skutecznością podszyć się pod celebrytów, polityków lub nawet kogoś nam bliskiego! Grozi dezinformacją i wyłudzeniami: danych i pieniędzy.

WIRUSY

Złośliwe oprogramowanie, które może być rozprzestrzeniane w zwykłych wiadomościach, trafiających do nas np. na Messengerze lub mailowo. Zaczyna się od kliknięcia w link, uruchamiający pobranie, a nawet włączenie lub instalację niezweryfikowanego pliku. Ściągnięcie na urządzenie wirusa grozi np. zyskaniem dostępu do naszego sprzętu przez przestępców.

WYCIEKI DANYCH

To zagrożenia związane z dostępem hakerów do prywatnych danych i rozmów użytkowników. W ich konsekwencji mogą zostać ujawnione hasła do kont lub osobiste zdjęcia i informacje!

Najważniejsze, to umieć rozpoznać zagrożenie, z którym mamy styczność. Nigdy nie pobieraj plików, których się nie spodziewasz, dokładnie weryfikuj wiarygodność informacji, które znajdujesz i nie udostępniaj zbyt wielu danych na swój temat!

O TYM WIĘCEJ W KOLEJNYM ROZDZIALE!

NIE MASZ PEWNOŚCI, CZY LINKI LUB WIADOMOŚCI SĄ BEZPIECZNE? PODEŚLIJ JE DO NAS!

CYBER RESCUE

CO UDOSTĘPNIAĆ, CZEGO UNIKAĆ? 5

Dzielenie się treściami w mediach społecznościowych jest kluczowym elementem interakcji online, ale jednocześnie niesie ze sobą ryzyko, związane z Twoim bezpieczeństwem i prywatnością.

Co możesz udostępniać?

INSPIRUJĄCE I CIEKAWE TREŚCI, KTÓRYMI CHCESZ PODZIELIĆ SIĘ Z INNYMI

WAŻNE WYDARZENIA Z ŻYCIA*

PRZEMYŚLENIA I OPINIE Z POSZANOWANIEM DLA RÓŻNORODNYCH PUNKTÓW WIDZENIA, UNIKAJĄCE AGRESJI I HEJTU

* Możesz pochwalić się ślubem lub narodzinami swojej pociechy, ale nie dziel się szczegółami (miejscami lub datami)! Więcej o tym znajdziesz w naszym poradniku “Cyberbezpieczny Dzieciak”.

Oczywiście naszym celem nie jest demonizowanie social mediów i namawianie Cię do kompletnego ich porzucenia! Wszystko dla ludzi, jednak podczas ich użytkowania warto zachować zdrowy rozsądek i logicznie przemyśleć ewentualne konsekwencje. Przykład: osobiste wydarzenia udostępniaj tylko najbliższym! Dlaczego? W ten sposób minimalizujesz ryzyko. Jeśli oszust nie będzie w stanie za dużo się o Tobie dowiedzieć, nie stworzy spersonalizowanego ataku hakerskiego!

Czego nigdy nie wrzucać?

Informacji wrażliwych, np. szczegółów na temat swojego życia prywatnego (adres zamieszkania, numer telefonu, ważne daty, lokalizacje)
Dlaczego? Mogą zostać wykorzystane do spersonalizowanych ataków. Przestępcy, korzystając z socjotechniki i zdobytych informacji, często próbują wzbudzić niepokój oraz obawę o utratę środków pieniężnych, np. wysyłając maile z próbą szantażu.

Szczegółów, dotyczących planów wyjazdowych czy obecności w określonych miejscach, aby uniknąć ryzyka kradzieży.
Czasami oszuści korzystają z tych informacji, by zaplanować przestępstwo. Chodzi tu nie tylko o włamanie do domu, ale także o fałszywe maile, podszywające się np. pod hotel, do którego się wybierasz.

Zdjęć lub skanów dokumentów i kart płatniczych.
Takie informacje NIGDY nie powinny się znaleźć na Twoim profilu i w konwersacjach! Cyberprzestępcy korzystają z web scrapingu, czyli techniki automatycznego pobierania informacji, dostępnych publicznie w różnych serwisach. Co to znaczy? Wrażliwe dane trafią w ich ręce! Mogą prowadzić do kradzieży Twoich oszczędności, a nawet próby wzięcia kredytu na Twoje dane!

CYBER RESCUE

TWORZYMY BEZPIECZNY PROFIL 6

Bezpieczny profil w mediach społecznościowych to taki, którego użytkownik podejmuje świadome i skuteczne kroki, żeby chronić swoją prywatność.

PRYWATNOŚĆ 1

Każda platforma oferuje różne opcje konfiguracji, pozwalające kontrolować widoczność Twoich danych. Sprawdź ustawienia prywatności i wybierz kto może widzieć Twoje informacje osobowe, zdjęcia i posty.

Wejdź w Ustawienia, następnie w zakładkę "Kontrola prywatności". Tam określisz kto może widzieć i komentować twoje informacje, posty, zdjęcia.

Możesz zmienić ustawienia konta na prywatne, wtedy tylko Twoi obserwatorzy będą mogli zobaczyć co publikujesz! Wystarczy, że wejdziesz w Ustawienia, następnie "Kontrola prywatności" i wybierzesz "Konto prywatne"

Wejdź w Menu i wybierz “Ustawienia i prywatność” i włącz albo wyłącz opcję „Konto prywatne”.

2 SILNE HASŁO

Upewnij się, że używasz silnych haseł logowania do swoich kont. Unikaj łatwych do odgadnięcia kombinacji, takich jak imiona czy daty urodzenia. Hasło powinno być niepowtarzalne, trudne do odgadnięcia i składać się z minimum kilkunastu znaków.

CYBER RESCUE

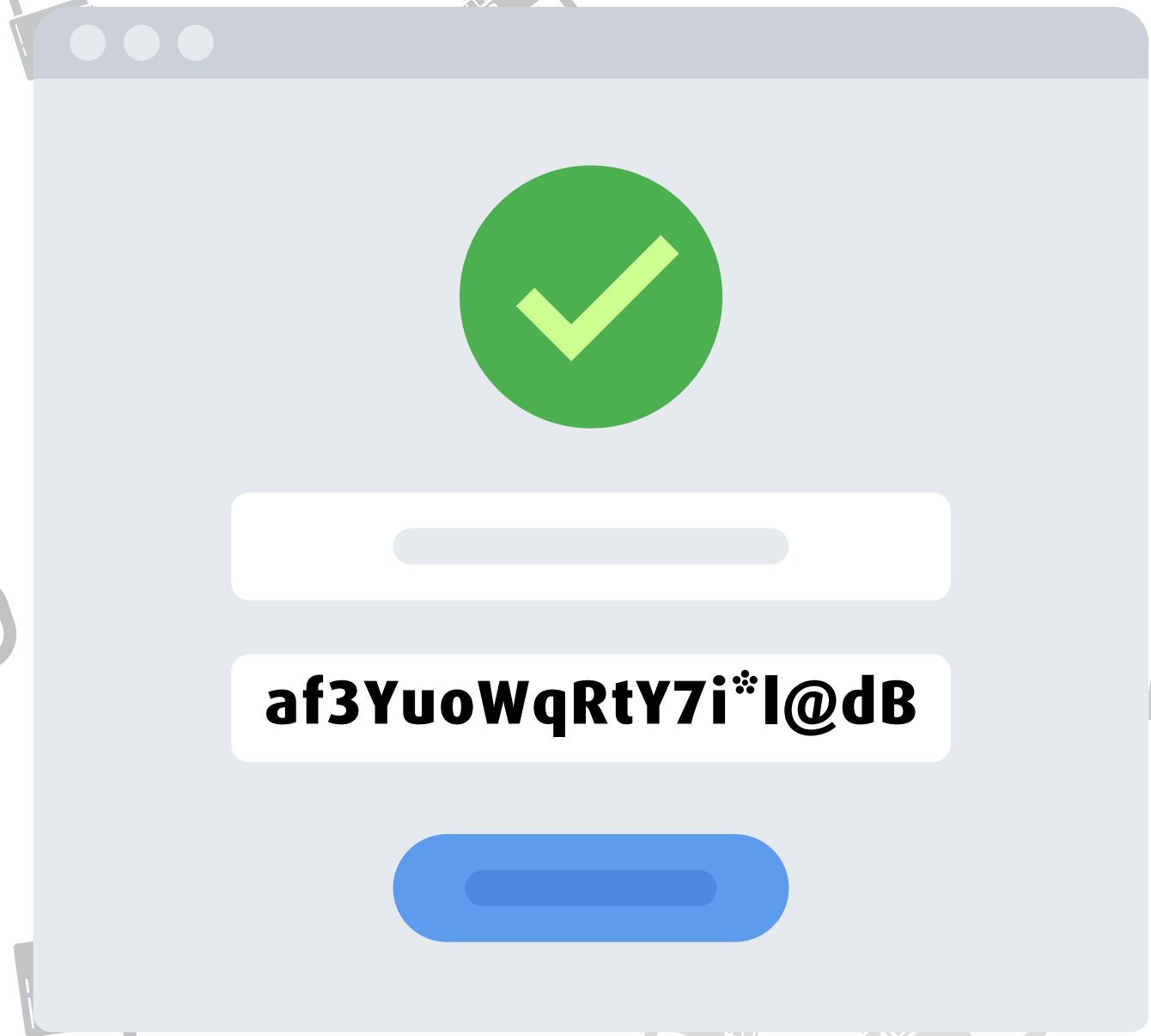
SŁABE HASŁO

TAKICH NIE UŻYWAJ!

CYBER RESCUE

SILNE HASŁO

PRZYKŁAD DOBREGO HASŁA, MOŻESZ JE PRZECHOWYWAĆ W MENADŻERZE HASEŁ, NP. BITWARDEN



DODATKOWE ZABEZPIECZENIE 3

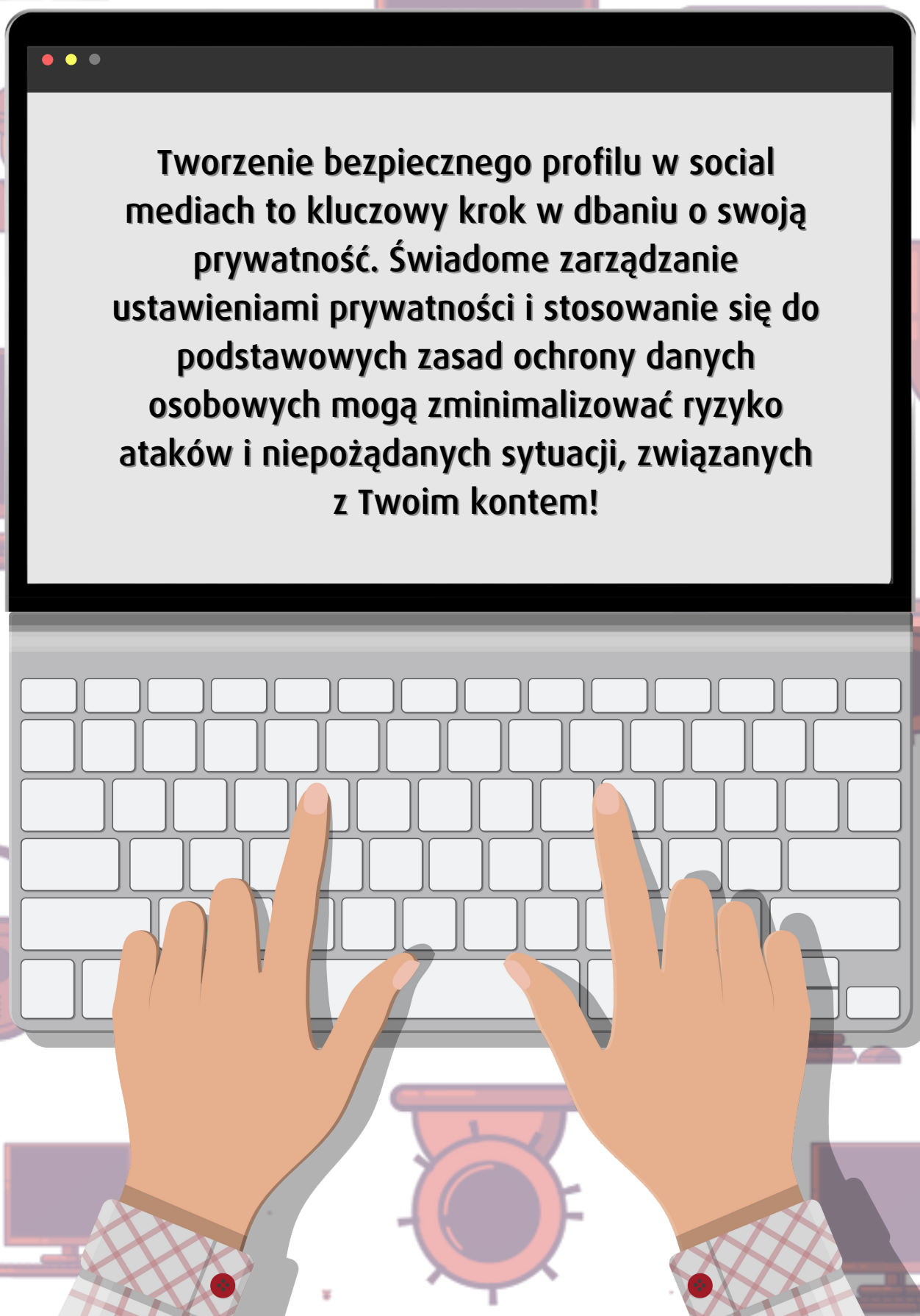
Włącz weryfikację dwuetapową (2FA) wszędzie, gdzie to możliwe!

Co to takiego? Dodatkowa warstwa bezpieczeństwa, używana w celu podwójnego potwierdzenia tożsamości właściciela konta. Najczęściej dostępna jest w Ustawieniach danego serwisu, w sekcji Bezpieczeństwo lub Zabezpieczenia. Możesz ją uruchomić m.in. na Facebooku, Instagramie, czy swojej poczcie. Korzystanie z niej jest bardzo proste - podczas logowania z nowego urządzenia, oprócz wpisania hasła, konieczne będzie wprowadzenie specjalnego kodu, otrzymanego na telefon, mailowo lub potwierdzenia w specjalnej aplikacji, do której dostęp masz tylko Ty (np. Google Authenticator).

Dlaczego to takie ważne? W sytuacji, gdy Twoje hasło zostanie ujawnione, np. na skutek wycieku i ktoś spróbuje się zalogować na konto, nie będzie mógł potwierdzić drugiego etapu weryfikacji.

4 DODATKOWE ZABEZPIECZENIE

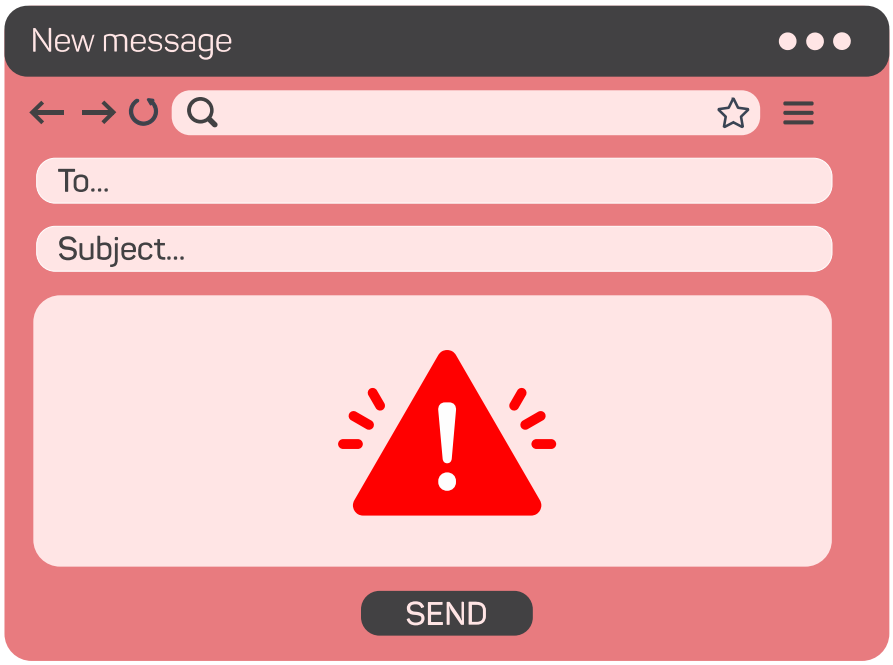
Regularnie sprawdzaj aktywność swojego konta. Wiele platform (np. Facebook, Instagram) oferuje funkcje monitorowania przez powiadomienia o nowym logowaniu, dzięki którym można wykryć nieautoryzowany dostęp lub inne podejrzane działania. Reaguj natychmiast, jeśli coś wydaje Ci się podejrzane! Zakończ nieznane sesje logowania, zmień hasło i zabezpiecz inne konta, gdzie masz te same dane do logowania.


Tworzenie bezpiecznego profilu w social mediach to kluczowy krok w dbaniu o swoją prywatność. Świadome zarządzanie ustawieniami prywatności i stosowanie się do podstawowych zasad ochrony danych osobowych mogą zminimalizować ryzyko ataków i niepożądanych sytuacji, związanych z Twoim kontem!

BEZPIECZNA KOMUNIKACJA 7

W MIARĘ WZROSTU POPULARNOŚCI KOMUNIKATORÓW INTERNETOWYCH, DBANIE O POUFNOŚĆ ROZMÓW STAJE SIĘ NIEZWYKLE ISTOTNE.

Wiele serwisów wprowadza narzędzia, umożliwiające zabezpieczanie wiadomości (np. konieczność podania kodu PIN do Messengera po zalogowaniu się na innym urządzeniu). Musisz jednak pamiętać, że Twoje bezpieczeństwo jest przede wszystkim w Twoich rękach! Podczas prowadzenia interakcji online, zawsze zalecamy zasadę ograniczonego zaufania.



CYBER RESCUE

O TYM MUSISZ PAMIĘTAĆ!

1

Unikaj klikania w linki i otwierania załączników z nieznanych źródeł. Nie wchodź też w linki od znajomych, jeśli nie umawiasz się z nimi, że coś wyślą! W takich plikach i odnośnikach może czyhać na Ciebie złośliwe oprogramowanie! Jeśli odbiorca nie jest Ci dobrze znany, a treść wydaje się podejrzana, nie reaguj! Pamiętaj, że każdy wątpliwy materiał (link, mail, plik, wiadomość) - możesz przesłać nam do weryfikacji :)

2

Regularnie sprawdzaj i przeglądaj aplikacje oraz gry, które mają dostęp do Twojego konta, np. na Facebooku. Niektóre z nich mogą żądać dostępu do zbyt wielu danych. Usuwaj te, których nie używasz lub którym nie ufasz. O tym jakie dane zbierają aplikacje, dowiesz się w ich opisie w Google Play lub AppStore.

3

Bądź ostrożny wobec atrakcyjnych konkursów i promocji. Nigdy nie podawaj w nich prywatnych informacji ani namiarów na swoją kartę płatniczą! Wiele oszustw związanych z phishingiem (czyli podszywaniem się pod osobę lub instytucję) zaczyna się właśnie od fałszywych konkursów.

4

Dbaj o to, kto ma wgląd w Twój profil. Akceptuj wyłącznie zaproszenia od osób, które znasz osobiście. Pamiętaj, że im mniej użytkowników ma dostęp do Twojego profilu, tym mniejsze ryzyko naruszenia Twojego bezpieczeństwa.

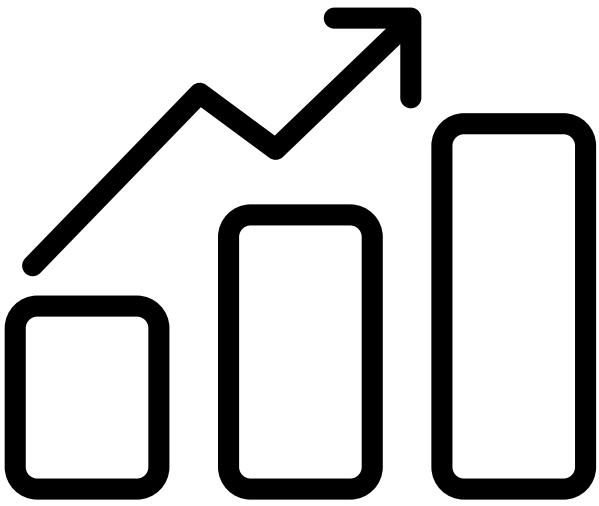
SM JAKO NARZĘDZIE BIZNESOWE

8

Social media to nie tylko platformy do dzielenia się zdjęciami i informacjami osobistymi. To też potężne narzędzia biznesowe, umożliwiające firmom dotarcie do swoich obecnych i potencjalnych Klientów, budowanie marki i nawiązywanie interakcji z fanami. W tym rozdziale przyjrzymy się w jaki sposób media społecznościowe mogą skutecznie pomóc Twojemu biznesowi, co warto robić z profilu firmowego, a czego bezwzględnie unikać.

Jakie treści pomogą zbudować Twoją markę?

Publikuj treści, które są nie tylko związane z Twoją branżą, ale także wartościowe dla Twojej publiczności. Porady, informacje biznesowe, ciekawostki czy inspiracje - to wszystko buduje zaangażowanie i lojalność Klientów! Odpowiadaj na komentarze, pytania i opinie. Media społecznościowe są okazją do nawiązania relacji, więc aktywna interakcja z użytkownikami jest kluczowa. Twórz konkursy, ankiety i pytania, żeby zaangażować społeczność.



Jak bezpiecznie korzystać z profilu firmowego na platformach społecznościowych, bez narażania działalności na straty?

Zadbaj o edukację, swoją i Pracowników. Zanim Twoja firma podbije platformy społecznościowe, rozważ przejście szkolenia z bezpiecznego, biznesowego użytkowania social mediów. Zagrożeń jest ogrom, a zdobycie profesjonalnej wiedzy i świadomość w temacie aktualnych ryzyk, pozwolą uniknąć wielu potencjalnych nieprzyjemności.

Jeśli nie prowadzisz konta firmowego samodzielnie, ogranicz dostęp do funkcji administratora Twojego profilu, udostępniając ją wyłącznie niezbędnym Pracownikom. Zadbaj, żeby każda osoba miała przypisane odpowiednie uprawnienia, zgodne z jej stanowiskiem i rolą w firmie.

Przygotuj plan działania w przypadku incydentu, związanego z cyberbezpieczeństwem. Jeśli Twoje konto padnie ofiarą ataku, natychmiastowe działanie i wdrożenie planu mogą pomóc zminimalizować szkody!

HEJT I CYBERPRZEMOC 9

HEJT

Hejt (z ang. hate - nienawiść) to synonim "hejterstwa", czyli agresywnych i obraźliwych działań wobec innych użytkowników Internetu. Może przybierać różne formy, takie jak publiczne krytykowanie, poniżanie, obrażanie i rozpowszechnianie fałszywych informacji na temat konkretnej osoby lub grupy ludzi.

Hejt jest powszechnie spotykany w mediach społecznościowych, gdzie anonimowość i dystans sprawiają, że niektórzy ludzie czują się bezkarnie. Agresja online niszczy nie tylko osobę, która jest celem ataków. Dewastuje również całe grupy i społeczności, istniejące w cyfrowym świecie.

CYBERPRZEMOC

Cyberprzemoc obejmuje szeroki zakres szkodliwych działań, prowadzonych przy wykorzystaniu Internetu i urządzeń podłączonych do sieci. Z roku na rok można zaobserwować rosnącą skalę problemu, który prowadzi do poważnych konsekwencji w świecie rzeczywistym. Najczęściej przybiera formę słowną, np. złośliwych komentarzy, memów lub nagrań wideo.

Osoby stosujące cyberbullying często są przekonane o swojej anonimowości, co sprawia, że czują się bezkarne. Poza tym, sytuację utrudnia fakt, że cyberprzestępcy w każdej chwili mogą zaatakować, a ofiara nie ma możliwości ucieczki - wszak jej profil jest cały czas dostępny w sieci.

Jakie są najczęstsze formy cyberprzemocy? Mogą to być m.in.:

- publikowanie poniżających, ośmieszających treści
- włamania na konta portali społecznościowych
- podszywanie się
- wykluczanie z internetowych społeczności
- nękanie wiadomościami, np. na Messengerze

Statystyki mowią, że...

Co piąty nastolatek mierzy lub mierzył się z przemocą w Internecie. Ankietowani najczęściej wymieniali wyzywanie (29,7%), ośmieszanie (22,8%) i poniżanie (22%)*. To dramatyczne statystyki, bo wszyscy doskonale wiemy, że każdy człowiek zasługuje na szacunek!

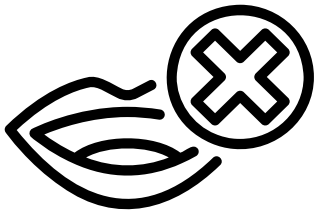
W walce z cyberprzemocą kluczowa jest ochrona prywatności. Dlaczego jest to tak ważne? Osoby hejtujące i nękające innych często korzystają z informacji udostępnionych na profilu ofiary. Łatwo temu zapobiec, ograniczając dostęp do prywatnych informacji, podkręcając ustawienia prywatności na platformach społecznościowych i unikając publikacji swoich wrażliwych danych.

*Źródło: Raport UNICEF

Jeśli padniesz ofiarą hejtu, nie bagatelizuj problemu! Zbieraj dowody - nie usuwaj wiadomości z pogróżkami, dokumentuj kontakt (tutaj niezwykle przydatne mogą okazać się screeny z widocznymi nazwami użytkowników). Warto również notować, kiedy doszło do każdej negatywnej interakcji.

Oprócz tego, zawsze blokuj agresorów i raportuj incydenty administracji platformy! Każdy serwis społecznościowy daje możliwość zgłoszenia konta lub postu. Takie działanie pomaga administracji kontrolować przestrzeganie zasad społeczności przez użytkowników. Jak to działa? Najczęściej musisz kliknąć przy poście opcję “Więcej” i “Zgłoś materiały”. Następnie wybierasz powód zgłoszenia z dostępnej listy i wysyłasz zgłoszenie. W odpowiedzi otrzymasz powiadomienie o aktualizacji, z informacją czy serwis zdecydował się usunąć materiały. Niektóre portale, np. Facebook, w oknie zgłoszenia, proponują użytkownikom zablokowanie profilu autora i wyciszenie udostępnianych przez niego treści.

Zgłaszając nieregulaminowe treści i profile dokładasz solidną cegiełkę do fundamentu bezpieczeństwa serwisu! Pamiętaj, że platformy społecznościowe mają obowiązek zapewniać swoim użytkownikom bezpieczne i komfortowe środowisko!



Nie ignoruj też możliwości zgłoszenia sprawy na policję. Zrób zrzut ekranu krzywdzącej wiadomości i dołącz go do zawiadomienia o popełnieniu przestępstwa. Hejt i wszelka cyberprzemoc są karalne i należy z nimi walczyć!

Prowadzisz stronę na Facebooku? Grupę? A może tworzysz treści, które docierają do mas? Buduj społeczność opartą na wsparciu i wzajemnym szacunku. Ustalaj zasady i konsekwentnie przestrzegaj ich stosowania.

Wspieraj osoby, które padły ofiarą hejtu i promuj kulturalne interakcje wśród swoich odbiorców. Nie toleruj jakichkolwiek śladów prześladowania, naśmiewania, obrażania, wulgaryzmów. Jeśli widzisz wśród swoich fanów/followersów/Klientów takie zachowania - nie bój się podejmować radykalnych kroków.

Banuj, blokuj i zgłaszaj wszystkie konta zaangażowane w taką aktywność. Dzięki wspieraniu dobrych praktyk i nietolerowaniu łamania zasad, masz realny wpływ na przeciwdziałanie hejtowi i cyberprzemocy. Pamiętaj, że podstawowe reguły cyberprzestrzeni, jak wzajemny szacunek, empatia i kultura interakcji, nawet gdy nie zgadzamy się z czyimś stanowiskiem, są solidnym fundamentem świata online.

PODZIĘKOWANIE 10

Drogi Czytelniku,

Dotarliśmy do końca! Mamy nadzieję, że lektura naszego eBooka ugruntowała i wzbogaciła Twoją wiedzę o social mediach. Liczymy też, że nasze wskazówki o bezpiecznym funkcjonowaniu w społecznościach online przełożą się na potężne zminimalizowanie zagrożeń, jakie możesz w tym świecie spotkać.

Jeśli masz ochotę poznać więcej ciekawostek z cyberprzestrzeni, koniecznie zajrzyj na naszego bloga (https://cyberrescue.info), gdzie regularnie publikujemy pomocne materiały. Znajdziesz tam m.in. nasze pozostałe eBooki:

- Jak weryfikować sklepy internetowe?
- Poradnik CyberBezpieczny Senior
- Poradnik CyberBezpieczny Dzieciak

Zapraszamy też na nasze social media, gdzie na bieżąco ostrzegamy przed aktualnymi zagrożeniami w sieci!

Masz pytania lub potrzebę doprecyzowania? Odezwij się do nas na Messengerze (facebook.com/cyberrescue.me).

Dziękujemy Ci za poświęcony nam czas!

Team CyberRescue