

Jak możesz ocenić poziom zagrożeń dla Swojej prywatności i zapobiec naruszeniu Twojej cyfrowej tożsamości i danych?

06.07.2023

Każdy, kto korzysta z Internetu, jest narażony na zagrożenia związane z cyberbezpieczeństwem i prywatnością. Im bardziej jesteś świadomy tych zagrożeń oraz potencjalnego niewłaściwego wykorzystania Twojej tożsamości i danych, tym bardziej prawdopodobne jest, że unikniesz zagrożeń, które mogą zaszkodzić Twojej reputacji lub finansom. Podczas korzystania z sieci musisz stawić czoła wielu trudnym zadaniom, w tym prawidłowej ocenie poziomu zagrożenia – lub określeniu, jakie czynniki mogą narazić Cię na niebezpieczeństwo online i jak mogą wpłynąć na Twoją prywatność. Dlatego zespół Bitdefender przygotował poradnik, dzięki któremu będziesz bardziej świadomy cyberzagrożeń i dowiesz się, jak przygotować się na potencjalną

Jak możesz ocenić poziom zagrożeń dla swojej prywatności i zapobiec naruszeniu Twojej cyfrowej tożsamości i danych

Bitdefender®

kradzież danych.

Jak możesz ocenić poziom zagrożeń dla swojej prywatności – najważniejsze zagrożenia

W świecie opartym na danych Twoja tożsamość cyfrowa ma większe znaczenie niż myślisz i często jest najbardziej narażona na kradzież i niewłaściwe wykorzystanie przez hakerów, oszustów i inne strony trzecie. Dlatego zanim zaczniemy tworzyć model zagrożeń dla swojej prywatności, przypomnijmy sobie, jakie rodzaje danych mogą mieć najbardziej szkodliwe skutki, jeśli wpadną w niepowołane ręce:

- Poufne dane obejmujące imię i nazwisko, numer telefonu, adres fizyczny, adresy e-mail, hasła, adresy IP, numer ubezpieczenia oraz numery prawa jazdy i paszportu. Połączenie tych danych może pozwolić cyberprzestępcom na przeprowadzanie przestępstw związanych z kradzieżą tożsamości.
- Dane dotyczące płatności związane z transakcjami finansowymi, takie jak numery kart kredytowych i debetowych, numery kont bankowych i kody PIN, które umożliwiają złośliwym podmiotom uzyskanie dostępu do Twoich kont finansowych, przelewanie środków lub dokonywanie zakupów w Twoim imieniu.
- Dane dotyczące zdrowia, w tym historia medyczna, dane ubezpieczenia zdrowotnego, wizyty w szpitalu i recepty, które mogą umożliwić oszustom między innymi kradzież tożsamości medycznej.

Jak możesz ocenić poziom zagrożeń dla swojej prywatności i zapobiec naruszeniu Twojej cyfrowej tożsamości i danych

Bitdefender®

Określenie poziomu zagrożenia bezpieczeństwa w pięciu prostych krokach

Aby lepiej ocenić swoje potrzeby w zakresie prywatności i bezpieczeństwa oraz chronić swoją tożsamość, musisz określić potencjalne wektory zagrożenia, prawdopodobieństwo ataków oraz konsekwencje stania się ofiarą cyberprzestępców.

Zacznij od ustalenia aktywów, które chcesz chronić

Twoje urządzenia i konta internetowe przechowują cenne dane, takie jak informacje finansowe, dane związane z pracą, ważne dokumenty, rodzinne filmy wideo i inne poufne pliki. Powinieneś mieć jasny obraz, jakiego rodzaju dane chcesz chronić i kto ma do nich dostęp oraz podjąć niezbędne kroki, aby uniemożliwić innym przeglądanie ich.

Spróbuj zidentyfikować potencjalne zagrożenia lub osoby trzecie, które mogą chcieć uzyskać dostęp do Twoich urządzeń i danych

Może to obejmować hakerów, byłego partnera, brokera danych, konkurenta, prześladowcę lub inne złośliwe osoby. W zależności od wyników analizy możesz właściwie rozwiązać wszelkie problemy związane z bezpieczeństwem.

Określ prawdopodobieństwo ataku

Jak możesz ocenić poziom zagrożeń dla swojej prywatności i zapobiec naruszeniu Twojej cyfrowej tożsamości i danych

Bitdefender®

„Większość internautów niekoniecznie czuje się zagrożona, fałszywie wierząc, że nie mogą stać się celem oszustów i cyberprzestępców. Pozbądź się postawy „mnie to się nie może przytrafić” i przestań zakładać, że Twoje konta nie zawierają żadnych informacji, które można wykorzystać. Jeśli jesteś aktywnym obywatelem cyfrowym, załóż, że Twoje dane zostaną ostatecznie ujawnione online, niekoniecznie z Twojej winy (naruszenia danych i wycieki z organizacji i firm)” – mówi Mariusz Politowicz z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Jakie są bezpośrednie i długoterminowe konsekwencje naruszenia Twojej cyfrowej tożsamości?

Hakerzy mogą uzyskać dostęp do Twoich danych poprzez luki w zabezpieczeniach, złośliwe ataki lub przypadkowe ujawnienie. Gdy Twoje dane lub aktywa zostaną ujawnione, cyberprzestępcy mogą popełnić oszustwo, podszyć się pod Ciebie i zrujnować Twoją zdolność kredytową lub reputację.

Jaki jest twój plan zapobiegania i jak możesz złagodzić potencjalne konsekwencje

Niestety obecnie nie ma doskonałego protokołu, który byłby w stanie w pełni zabezpieczyć Twoją tożsamość, finanse i dane. Jednak nadanie priorytetu bezpieczeństwu cyfrowemu i nadążanie za najnowszymi narzędziami bezpieczeństwa oraz prywatności może pomóc zminimalizować ryzyko stania się ofiarą cyberataku.

Jak możesz ocenić poziom zagrożeń dla swojej prywatności i zapobiec naruszeniu Twojej cyfrowej tożsamości i danych

Bitdefender®

Co powinieneś zrobić, aby zminimalizować ryzyko stania się cyberofiara?

- Zmniejsz liczbę informacji udostępnianych online i chroń poufne dane.
- Uważaj, gdzie klikasz – pobieranie plików z niezweryfikowanych źródeł naraża Ciebie i Twoje urządzenia na zagrożenia bezpieczeństwa, które mogą zaszkodzić Twojej prywatności i finansom.
- Zwiększ bezpieczeństwo swoich haseł – hasła to pierwsza linia obrony przed atakami polegającymi na przejęciu konta, które mogą zaszkodzić Twoim finansom lub reputacji. Możesz także zainstalować menedżera haseł, który pomoże Ci zarządzać poświadczeniami konta.
- Aktualizowanie urządzeń i oprogramowania sprawia, że są one mniej podatne na ataki.
- Monitorowanie wycieków danych może pomóc złagodzić wszelkie potencjalne zagrożenia.
- Wdrożenie planu reagowania na naruszenia bezpieczeństwa danych – ponieważ firmy i organizacje znajdują się pod ciągłym ostrzałem cyberprzestępców, szybkie reagowanie i łagodzenie

Jak możesz ocenić poziom zagrożeń dla swojej prywatności i zapobiec naruszeniu Twojej cyfrowej tożsamości i danych

Bitdefender®

potencjalnych konsekwencji naruszeń danych stało się kluczowe dla konsumentów.

- Korzystaj ze skutecznego systemu antywirusowego, aby zapobiegać złośliwym atakom, phishingowi i oszustwom.

Źródło: <https://bitdefender.pl/jak-mozesz-ocenic-poziom-zagrozen-dla-swojej-prywatnosci/>

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.

Data udostępnienia: 06.07.2023

Z pozdrowieniami Piotr Rozmiarok

E-mail: piotr.r@marken.com.pl | Tel. bezpośredni: 570 400 019

Informacje o firmie Bitdefender

Bitdefender to rumuński dostawca rozwiązań z zakresu cyberbezpieczeństwa oraz światowy lider chroniący miliony użytkowników. Bitdefender jest częstym zdobywcą wielu branżowych nagród i uznaną światową marką. Od 2001 roku konsekwentnie dostarcza najwyższej jakości produkty służące do zapewnienia bezpieczeństwa zarówno użytkownikom domowym, jak i wielkim korporacjom i rządowym instytucjom. Bitdefender jest znany ze swojej innowacyjności oraz wyposażania swojego oprogramowania w najnowsze technologie, takie jak uczenie maszynowe, heurystyka oraz EDR i XDR.

Jak możesz ocenić poziom zagrożeń dla swojej prywatności i zapobiec naruszeniu Twojej cyfrowej tożsamości i danych

Bitdefender[®]