Dane osobowe pozostawiamy w różnych miejscach: w social mediach, w sklepie internetowym, w formularzu subskrypcji, w aplikacji lojalnościowej. Dane to także zbiór informacji przekazywanych przez przeglądarki i aplikacje, z których korzystamy (w tym adres IP, język, lokalizacja, rodzaj urządzenia), a także pliki cookies.

Ochrona tożsamości w internecie to:

1. Ograniczanie ilości pozostawianych danych.
2. Zabezpieczanie danych osobowych przed nieautoryzowanym dostępem i wykorzystaniem przez nieuprawnione osoby.

Pamiętaj!

Żadne urządzenie nie gwarantuje 100% bezpieczeństwa w sieci. Bezpieczeństwo w cyberprzestrzeni w dużej mierze zależy od nas samych i naszego postępowania.

Można powiedzieć, że nie ma nic złego w pozostawianiu danych w sieci. Jednak brak dbałości o właściwe zabezpieczenie danych może przynieść nieprzewidziane skutki. Ktoś może bezprawnie wejść w posiadanie danych osobowych i wykorzystać je wbrew naszej wiedzy i woli. Bezprawnie pozyskane dane mogą posłużyć do podszywania się i tworzenia np. fałszywych profili w internecie, a nawet prób wyłudzania pieniędzy czy rozsyłania złośliwego oprogramowania. Dane osobowe powinny być chronione, ponieważ ich poznanie ułatwia cyberprzestępcom przygotowanie i przeprowadzanie różnego rodzaju ataków.

W jaki sposób najczęściej można narazić się na utratę danych osobowych?

Ponad 90% cyberataków opiera się na interakcji z użytkownikiem. Najczęściej cyberprzestępcy nakłaniają do otwarcia załącznika otrzymanego w wiadomości w poczcie elektronicznej albo kliknięcia w link (łącze) znajdujący się w treści maila.

Uwaga!

Uważaj na reklamy i oferty w mediach społecznościowych!
Twoją czujność powinny obudzić: nieprawdopodobnie atrakcyjna cena, komunikaty o ograniczonej ilości towaru *(Zostały ostatnie sztuki!)* lub ograniczony okres oferty *(Tylko dziś!)*. Takie działania mogą być celowe. Ich zadaniem może być wywarcie presji, byś jak najszybciej - bez zwłoki i zastanowienia kliknął w wyświetlany komunikat, który może przenieść Cię na fałszywą stronę.

Uważaj na podejrzane strony internetowe!
To jedno z głównych zagrożeń, z jakimi każdy użytkownik może się zetknąć podczas korzystania z internetu. Takie strony mogą zawierać złośliwe oprogramowanie, phishing lub inne formy cyberprzestępstwa, które mogą prowadzić do utraty prywatnych danych, a także pieniędzy.

Zawsze sprawdzaj, czy strona nie jest fałszywa!
Wpisz adres strony do wyszukiwarki i zweryfikuj, czy są dostępne dane kontaktowe, regulamin sklepu oraz adres administratora RODO. Pamiętaj, że prawidłowy adres witryny powinien być poprzedzony skrótem: https://.

Nigdy nie podawaj swoich haseł czy PIN-ów!
Nie podawaj swoich haseł do logowania ani PIN-ów do kart na żadnej niezidentyfikowanej stronie. Nie wysyłaj haseł ani PIN-ów SMS-em, ani nie wpisuj ich do jakichkolwiek formularzy przesłanych na Twoją skrzynkę mailową.

Ślad cyfrowy
To ogół pozostawianych przez użytkownika danych i informacji w sieci, np. w formie wiadomości mailowych, formularzy, postów, komentarzy, publikowanych zdjęć i filmów.

EDUKACJA NBP
NBP.PL/EDUKACJA

NARODOWY BANK POLSKI

JAK CHRONIĆ TOŻSAMOŚĆ W INTERNECIE?

Internauci lubią surfować w sieci... a internet lubi dane internautów.

Tożsamość to zbiór cech, które odróżniają nas od innych w społeczeństwie, inaczej mówiąc - identyfikacja.W erze internetu często posługujemy się terminem „tożsamość cyfrowa".

Tożsamość cyfrowa
To zbiór danych uwidocznionych przez użytkownika w internecie.

Dane osobowe:
To dane, które pozwalają zidentyfikować osobę, której one dotyczą, tj. imię i nazwisko, data urodzenia, adres zamieszkania, PESEL, numer i seria dowodu osobistego, numer telefonu, numer karty kredytowej czy konta bankowego.

Dane społeczne:
Np. uczący się, pracujący, emeryt. Status rodzinny np. członek rodziny.

Dane wizualne:
Wizerunek osoby, np. fotografia lub podobizna utrwalona cyfrowo.

Dane biometryczne:
Odcisk palca (wzór linii papilarnych), obraz twarzy czy zdjęcie tęczówki oka.

Najpopularniejsze rodzaje cyberataków

Phishing

Na czym to polega: to podszywanie się (z wykorzystaniem socjotechnik) pod zaufane instytucje lub osoby, które zna ofiara cyberprzestępstwa, w celu wyłudzania poufnych informacji i danych osobowych.

Techniki: przesyłanie spreparowanych wiadomości e-mail, SMSów, powiadomień w komunikatorach i połączeniach telefonicznych.

Cele: Uzyskanie dostępu do danych osobowych, a następnie użycie ich do uzyskania korzyści – najczęściej finansowych.

⚠ Przykłady ku przestrodze:

1. Ktoś chce pożyczyć od Ciebie niewielką kwotę, otrzymujesz wiadomość: „Zabrakło mi do biletu, prześij BLIK-iem”.
2. Otrzymujesz komunikat, że kończy się subskrypcja na płatny kanał streamingowy: „Opłata tylko do końca dnia – w innym przypadku kanał zostanie wyłączony”.
3. Otrzymujesz SMS: „W celu odbioru przesyłki, konieczna jest dopłata. Dopłać 1,23 zł, aby odebrać przesyłkę”.

Cechy wiadomości, które mogą wskazywać na phishing:

1. Nadawca nigdy nie kontaktował się z tobą w taki sposób, jak w przypadku tej wiadomości.
2. Wiadomość zawiera prośbę o podanie poufnych informacji, takich jak hasło, numer karty kredytowej czy dane osobowe.
3. Wiadomość jest napisana w sposób nakłaniający do natychmiastowego działania.
4. Do wiadomości dołączony jest załącznik (plik) lub link.
5. Wiadomość może zawierać niepoprawne formy gramatyczne (niepoprawna odmiana wyrazów, błędy ortograficzne), albo stylistyczne (np. przestawione wyrazy).

Fałszywe strony

Na czym to polega: Fałszywe strony internetowe są specjalnie stworzone, by podszywać się pod prawdziwe. Dlatego wyglądają niemal identycznie. Najczęściej wyłudzają dane. Mogą też udawać strony z ofertami lub usługami, jednak zakupy z takich witryn nigdy nie zostaną dostarczone.

Techniki: Fałszywe reklamy z ofertami często obiecują niezwykle niskie ceny produktów klasy premium. Po kliknięciu z taką reklamę, przenoszą na złośliwe strony, które wyłudzają dane. Zorganizowane na szeroką skalę kampanie reklamują takie strony na popularnych portalach lub w mediach społecznościowych.

Cele: Wyłudzenie pieniędzy lub danych osobowych.

⚠ Przykłady ku przestrodze:

1. Reklama słuchawek bezprzewodowych premium, które kosztują …tylko 30 zł! Po kliknięciu należy podać swoje imię, nazwisko, numer telefonu, adres e-mail i adres zamieszkania.
2. Reklama w popularnym komunikatorze: „Masz szczęście – wygrałeś smartfon. Oferta ważna tylko do końca dnia.Wypełnij formularz zgłoszeniowy”.

Zwróć uwagę na te cechy!

1. Czy adres strony, na którą wchodzisz, jest na pewno poprawny? Z pozoru adres może wydawać się identyczny, jednak po uważnym przeczytaniu można znaleźć zamienioną kolejność liter, wyrazów lub inne celowe błędy, np. www.pkobq.pl, www.face-bok.pl.
2. Niebezpieczne strony internetowe często proszą o poufne informacje, takie jak hasła, numery kont bankowych lub dane osobowe. Żadna strona internetowa nie powinna prosić o takie informacje. Jeśli tak się dzieje, należy natychmiast ją opuścić i poszukać alternatywnych źródeł informacji (np. skorzystać z wyszukiwarki internetowej Google, bing).

Atak na hasła

Na czym to polega: Odgadywanie, łamanie lub dopasowywanie hasła do konta bankowego, poczty elektronicznej lub konta w mediach społecznościowych.

Techniki: Metodą prób i błędów z wykorzystaniem oprogramowania o dużej mocy obliczeniowej. Z wykorzystaniem haseł pochodzących z wycieków lub stosując hasła ze słowników haseł.

Cele: Naruszenia lub przejęcie konta, zablokowanie użytkownika poprzez zmianę hasła, w celu gromadzenia poufnych informacji na temat użytkownika, by następnie wykorzystywać je do kradzieży tożsamości.

⚠ Przykład ku przestrodze:

Twoje hasło zostało ujawnione w trakcie wycieku danych w popularnym sklepie internetowym. Jeśli stosujesz to samo hasło do wielu kont – przestępcy, którzy wykradli dane w jednym miejscu, łatwo mogą dostać się również do twoich pozostałych kont chronionych tym samym hasłem, takich jak np. poczta elektroniczna, profile w mediach społecznościowych czy konto bankowe.

Najczęściej popełniane błędy:

1. Twoje hasło jest krótkie i łatwe do odgadnięcia lub złamania, np. 123456, Patryk2010, Qwerty789.
2. To samo hasło stosujesz do każdego konta.
3. Przechowujesz hasło w przeglądarce, aby szybciej się logować.

Pamiętaj!

Przy zmianie hasła używaj za każdym razem zupełnie innych znaków niż wcześniej zastosowane.