Projekt IDCAP: Poprawa kompetencji cyfrowych u osób dorosłych

Numer projektu: 2018-1-PL01-KA204-051003

Tożsamość cyfrowa

Indeks

1. Wprowadzenie

W odniesieniu do tożsamości cyfrowej lub internetowej tożsamość cyfrowa jest informacją, która reprezentuje osobę fizyczną lub innego agenta zewnętrznego. Zewnętrznym agentem może być również pojedyncza maszyna, system i/lub aplikacja. ISO/IEC 24760-1 definiuje tożsamość jako "zbiór atrybutów związanych z konkretną jednostką"[1]. Obecnie mówimy o tożsamości jako o poszczególnych atrybutach podmiotu, który zastąpił termin "agent". W tym dokumencie będziemy odnosić się do tożsamości cyfrowej jedynie jako do tożsamości osoby fizycznej.

Tutaj przedstawimy podstawy zarządzania Twoją cyfrową tożsamością i dlaczego warto ją chronić. Następnie zobaczymy jak zarządzać kontem internetowym oraz jakie są kluczowe kroki w tym procesie. W dalszej części przedstawimy podstawy bezpieczeństwa i prywatności w Internecie. Na koniec pokrótce omówimy kwestie związane ze śladem cyfrowym i tożsamością online.

[1] ISO/IEC 24760-1: Ramy zarządzania tożsamością - Część 1: Terminologia i pojęcia". ISO. 2011.

2. Zarządzanie tożsamością cyfrową

Zarządzanie cyfrowymi przekaźnikami tożsamości opiera się na zasadach zgodnych z mniej lub bardziej znanymi mechanizmami, które zostały opracowane dla tożsamości niecyfrowej. Choć może się to wydawać skomplikowane, warto pomyśleć o swojej karcie identyfikacyjnej. Prosząc o otrzymanie dowodu osobistego, organ wydający go potwierdza od innych organów Twoje urodziny, numer podatkowy, numer obywatela (jeśli dotyczy), zrobi Ci nowe zdjęcie itp. W świecie cyfrowym twoja cyfrowa tożsamość może być tak prosta, jak twoja nazwa użytkownika i hasło lub może mieć o wiele więcej poziomów skomplikowania, które mają zagwarantować, że właścicielem tej konkretnej tożsamości jesteś ty i tylko ty. Poziomy te mogą obejmować oddzielny e-podpis, token do "losowego" wygenerowania danego kodu cyfrowego, potwierdzenie SMS-em lub wysłanie kodu na konkretny telefon komórkowy (o którym wiadomo, że jest zarejestrowany na konkretną osobę), identyfikację głosową, odpowiedź na konkretne pytanie (jak na przykład Jak miałeś na imię?), walidację odcisków palców i wiele innych. Wszystkie te poziomy mają na celu zagwarantowanie, że tylko konkretna osoba jest uprawniona do wykonywania niektórych czynności w świecie cyfrowym.

Wiele osób uważa te poziomy za trudne do zrozumienia, mylące i frustrujące. Mogą mieć rację, ale z drugiej strony należy zrozumieć, że świat cyfrowy jest bezpośrednią reprezentacją świata fizycznego i nikt nie chciałby, aby ich "cyfrowe" pieniądze wypływały z ich "prawdziwego" konta bankowego. Instytucje, a zwłaszcza banki, stawiają różne poziomy bezpieczeństwa nie po to, by denerwować użytkowników, ale by chronić ich tożsamość i zapewnić prawo do operacji i transakcji. Jednocześnie coraz więcej usług oferowanych jest za pośrednictwem telefonu komórkowego. Obejmują one tak szeroki zakres, że jako ilustrację wymienimy tu tylko kilka z nich. Pomyśl o nich jak o usługach, które mają bezpośredni wpływ na

Twoje "prawdziwe" konto bankowe. Niektóre z tych usług mogą być świadczone za pośrednictwem smartfonów (w zależności od kraju zamieszkania):

- Płatność za parkowanie za pomocą wiadomości SMS
- Płatność rachunku w supermarkecie
- Płacenie rachunków za dom
- Bezpośredni przelew pieniężny poprzez dedykowaną, autoryzowaną aplikację bankową

3D uwierzytelniona płatność kartą VISA lub Master Card - po podaniu numeru karty, jej ważności i kodu zabezpieczającego, system wysyła SMS z 6-cyfrowym kodem na zweryfikowany wcześniej telefon komórkowy, który doda jeszcze jedną warstwę ochrony transakcji dokonanych kartą.

Bilety na transport lądowy i karty pokładowe na samoloty
Z "Apple pay" i "Google Wallet" Twój telefon komórkowy staje się portfelem dla wszelkich płatności, które obsługują płatności NFC lub magnetyczne. Pozwala on nawet na otrzymywanie płatności z różnych stron internetowych, sklepów i użytkowników.

Zrozumiałe jest, dlaczego tak ważne jest właściwe zarządzanie swoją cyfrową tożsamością i dlaczego trzeba ją energicznie chronić.

3. Zarządzanie kontem internetowym

Jako część twojej cyfrowej tożsamości twoje konto internetowe jest pierwszym i w wielu przypadkach nieuniknionym krokiem. Zazwyczaj jest ono połączone z usługami poczty elektronicznej, takimi jak Googe's Gmail, Yahoo mail, Microsoft e-mail, itp. Po utworzeniu takiego konta masz do niego dołączone co najmniej dwie zmienne: swoją nazwę użytkownika i hasło. Obecnie większość z tych usług wymaga dołączenia i weryfikacji numeru telefonu komórkowego do każdego konkretnego konta. W ten

sposób masz 3 atrybuty konta tożsamości cyfrowej - nazwę użytkownika, hasło i numer telefonu komórkowego. W wielu przypadkach ta weryfikacja bez pytania i w celu dalszej ochrony dodajemy nie tylko numer telefonu, ale również unikalny numer produkcyjny telefonu komórkowego o nazwie IMEI - International Mobile Equipment Identity. Numer ten, który jest nadawany podczas produkcji, jest niezbędny do zezwolenia na używanie telefonu komórkowego również w sieci komórkowej. Informacje te są zaszyfrowane i przechowywane w bezpiecznym miejscu przez dostawców usług internetowych, ale nadal w niektórych rzadkich przypadkach mogą zostać skradzione lub niewłaściwie wykorzystane (jak w przypadku Facebooka i Cambridge Analytica, gdzie miliony użytkowników "dane zostały przekazane firmie w celu zrobienia ukierunkowanej reklamy w celach politycznych). Oto kilka wskazówek, które pomogą Ci w uzyskaniu cyfrowej tożsamości:

Nazwa użytkownika: wybierz nazwę użytkownika, która wyraźnie Cię reprezentuje. Pomyśl, że możesz używać tego konkretnego adresu e-mail w przyszłości, a zabawne nazwy nie zawsze są dobrze przyjęte. Twoja nazwa użytkownika będzie stała przed znakiem @ Twojego maila, więc imiona takie jak easygirl@, toughguy@, your nightmare@ nie tylko mają być unikane, ale w ogóle powinieneś ich unikać. Wybierając swoją nazwę użytkownika nie umieszczaj liczb takich jak data urodzin czy urodziny Twoich bliskich.

Hasło: Użyj kombinacji małych liter, wielkich liter, cyfr i znaków specjalnych jak #,$,&,|, ~. Zrób to co najmniej 8 znaków i zmieniaj często swoje hasło. Jeśli masz dostęp do swojego cyfrowego konta przez telefon komórkowy, użyj odcisku palca lub innej formy uwierzytelnienia. Nie "pamiętaj" swojego hasła do konta w przeglądarce.
Nawet jeśli nie jest to wymagane, dodaj wyraźnie swój telefon komórkowy do swojego konta i ustaw go jako urządzenie domyślne w celu odzyskania zapomnianych haseł. Zajrzyj do ustawień swojego konta i ustaw

odzyskiwaną pocztę elektroniczną i numer telefonu, aby jeszcze lepiej uwierzytelnić swoją tożsamość. Nie używaj tego samego hasła do innych kont, takich jak te w sieciach społecznościowych lub grach.

4. Kwestie bezpieczeństwa i prywatności

Niektóre serwery i aplikacje mogą gromadzić obszerne informacje o konkretnym zastosowaniu i potencjalnie mogą być powiązane z osobą fizyczną i jej cyfrowymi nawykami przez Internet. Na poziomie UE PKBR (ogólne rozporządzenie o ochronie danych) próbuje sobie z tym poradzić, ale nadal zaleca się użytkownikom, aby uważali, co i gdzie dzielą się i robią przez Internet, a zwłaszcza niektóre portale społecznościowe.

W celu przetwarzania treści cyfrowych istnieje wiele edytorów zdjęć i filmów, podczas gdy media społecznościowe zapewniają zazwyczaj możliwość sprawdzania pisowni tekstu w języku angielskim. Na cyfrowych zdjęciach (i filmach wideo) można dodawać różne filtry, zmieniać nasycenie, kontrast itp. Możesz korzystać z tych, które zostały dostarczone wraz z urządzeniem lub zainstalować ten, który najbardziej Ci się podoba. Pamiętaj, że większość darmowych edytorów online ma zazwyczaj pewne ograniczenia i musisz kupić jeden, aby odblokować wszystkie funkcje. Te usługi oprogramowania często dodają do Twojego zdjęcia lub filmu pisemny znak, że materiał został stworzony przy użyciu tego oprogramowania, co może Ci się nie podobać. Eksperymentujcie i sprawdzajcie, aż znajdziecie ten, który spełnia wasze potrzeby.

Jak podkreślono w badaniu OECD z 2016 r.[2] "Nie *jest możliwe całkowite wyeliminowanie zagrożeń dla bezpieczeństwa cyfrowego podczas prowadzenia działań, które opierają się na środowisku cyfrowym. Można jednak zarządzać tym ryzykiem, to znaczy można je ograniczyć do akceptowalnego poziomu w świetle wchodzących w grę interesów i korzyści oraz kontekstu*". Istnieją jednak dość rozsądne i stosunkowo proste kroki, które osoba fizyczna lub organizacja może podjąć, aby osiągnąć zadowalający poziom bezpieczeństwa cyfrowego i ochrony prywatności. Obejmują one m.in. mocne hasła, ścisłą politykę dostępu do Internetu, zdrowy rozsądek w przeglądaniu Internetu, edukację i szkolenia w zakresie najbardziej powszechnych wątków, ustanowienie polityki dotyczącej danych osobowych i ochrony danych osobowych. Mimo to UE narzuca najwyższe standardy ochrony danych osobowych i prywatności na świecie.

Jako osoba fizyczna, istnieją proste kroki w celu ograniczenia możliwości naruszenia prywatności. Należy zawsze uważnie przeczytać politykę dotyczącą plików cookie każdej strony internetowej, serwisu internetowego, wiadomości i platform mediów społecznościowych. W przypadku, gdy nie chcesz być śledzony (to znaczy, że niektóre strony internetowe zbierają dane o Twoich nawykach przeglądania, jak często odwiedzasz daną stronę, jakie reklamy klikniesz, jakich informacji szukasz w internecie itp.), możesz skorzystać z prywatnego okna przeglądarki, które jest oferowane przez prawie wszystkie aplikacje do przeglądania, takie jak Google Chrome, Mozilla Firefox, Microsoft Internet Explorer itp.

Po stronie bezpieczeństwa, nigdy nie należy używać tych samych haseł do różnych aplikacji internetowych, takich jak poczta elektroniczna, platformy mediów społecznościowych i strony internetowe, które wymagają logowania. Zachowaj silne hasło z 10 lub więcej znaków, w tym cyfry, duże i

[2] MANAGING DIGITAL SECURITY AND PRIVACY RISK, OECD DIGITAL ECONOMY PAPERS No 254, https://www.oecd-ilibrary.org/docserver/5jlwt49ccklt-en.pdf?expires=1591780736&id=id&accname=guest&checksum=AF002079529F4DE263769B3FBEB40035.

małe litery i znaki specjalne, takie jak &, #, $, ^, itp. Z reguły nie zapisuj swoich haseł do przeglądarki, ale staraj się je zapamiętać lub zbudować je zgodnie z regułą, którą sam sformułowałeś. Na przykład:

#MyFamilyName4websiteName~mY_first.name$.

Chociaż może się to wydawać skomplikowane, łatwo jest zapamiętać regułę. W miarę możliwości dodaj swój telefon komórkowy jako alternatywę uwierzytelnienia i odzyskaj zapomniane lub skradzione hasło. W ten sposób dodasz jeszcze jedną warstwę ochrony osobistej, co zmniejszy ryzyko złośliwego wykorzystania Twoich danych online.

5. Cyfrowy ślad stopy

Ślad cyfrowy odnosi się do unikalnej, możliwej do prześledzenia cyfrowej aktywności danego użytkownika w Internecie. Termin ten można również znaleźć jako cyfrowy cień, ślad internetowy, cień cybernetyczny itp. Chociaż zazwyczaj termin ten jest stosowany w odniesieniu do osób fizycznych, może być on również stosowany w odniesieniu do organizacji, firm, korporacji, witryn usług cyfrowych itp. Istnieją dwa rodzaje śladu cyfrowego - aktywny i pasywny.

Pasywny ślad cyfrowy - termin ten odnosi się do danych zebranych bez wiedzy danej osoby. Nie muszą być one koniecznie ukrywane przez użytkownika. Aktywny ślad cyfrowy to ten, którym użytkownik świadomie dzieli się o sobie na ogół na portalach społecznościowych lub różnych stronach internetowych. Informacje o użytkowniku mogą być celowo lub nieumyślnie pozostawione, a następnie informacje te są aktywnie lub biernie gromadzone przez inne osoby. Na przykład, jeśli w swoim profilu w mediach społecznościowych zostawiłeś widoczny dla wszystkich swój adres e-mail, numer telefonu komórkowego, adres zamieszkania, miejsce pracy, adres internetowy swojej firmy itp. będzie to stosunkowo łatwe dla programu komputerowego lub osoby fizycznej do zbierania bardzo dużej

ilości informacji dla Ciebie. W niektórych przypadkach informacje te mogą również obejmować Twoje konta bankowe lub dokumentację podatkową, jeżeli dojdzie do naruszenia dokumentacji bezpieczeństwa.
Istnieje wiele badań, które pokazują, że około 70% wszystkich cyfrowych zachowań ludzi jest świadomych i odpowiedzialnych. Jednakże około 30% cyfrowego śladu każdej osoby może być w formie, która nigdy nie zostałaby celowo ujawniona publicznie. Pozostawia to sporo danych do analiz zachowań zakupowych, nawyków zakupowych w sieci, hobby i innych obszarów życia osobistego. O ile nie ma nic złego w analizach klientów na dużych bazach danych, o tyle analizy takie mogą być podstawą do kradzieży tożsamości, działalności przestępczej i naruszania prywatności.

O ile ślad cyfrowy nie jest tożsamością cyfrową lub cyfrową identyfikacją, o tyle treść i dane opisowe (zwane również metadanymi) mają duży wpływ na prywatność, zaufanie do Internetu i reputację cyfrową. Odciski palców w Internecie mogą być wykorzystywane przez firmy przy rekrutacji nowych pracowników, organy ścigania przy gromadzeniu danych o konkretnych osobach nie mogą być gromadzone w inny sposób, marketerzy - wyszukują rodzaj produktów, którymi są zainteresowani użytkownicy lub w celu zwiększenia zainteresowania użytkowników konkretnym produktem lub usługą. Serwisy społecznościowe są podstawowym źródłem takich informacji. W niektórych przypadkach platformy społecznościowe mogą zbierać dane z urządzenia użytkownika, nawet jeśli użytkownik o tym nie wie, za pomocą różnych czujników w telefonach komórkowych lub innych urządzeniach użytkownika. Na przykład Facebook i Google gromadzą duże ilości informacji o użytkowniku, które w połączeniu ze sobą mogą opisywać dość szczegółowo jego osobowość, zainteresowania, poglądy polityczne, zwyczaje i zainteresowania zakupowe itp.

6. Tożsamość online

Tożsamość online jest tożsamością, którą użytkownik decyduje się zbudować w Internecie, zwykle dla celów gry. Użytkownicy mogą zdecydować się na reprezentowanie siebie za pomocą awatarów (grafik w rozmiarze ikony), a nie swoich prawdziwych zdjęć. Użytkownicy mogą również używać pseudonimów zamiast swoich prawdziwych nazwisk. Tożsamość online może być nawet określana poprzez linki użytkownika do internetowej grupy osób. Tożsamość online jest kojarzona z prawdziwymi użytkownikami poprzez procedury autoryzacji, takie jak rejestracja i logowanie (nazwa użytkownika i hasło), a także poprzez określony adres IP maszyny lub urządzenia. Takie strony często instalują ciasteczka śledzące, które mogą dalej określać zachowanie użytkownika w sieci i łączyć go z rzeczywistą osobą. Ponieważ gra jest często, ale nie zawsze, skierowana do młodszej publiczności, która nie jest tak ostrożna w ochronie online, ważne jest, aby pojęcie tożsamości cyfrowej, tożsamości online i śladu cyfrowego być jak najbardziej jasne dla wszystkich korzystających z Internetu.

Tożsamość online może być dowolna, od Twoich danych uwierzytelniających (nazwa użytkownika i hasło) do konta w mediach społecznościowych, nazwy forum lub profilu kupującego na danej stronie internetowej. Obejmuje ona również historię przeglądania, adres IP, aktywność wyszukiwania, itp. Ludzie i organizacje mogą być zainteresowani Twoją identyfikacją online w celach całkowicie legalnych lub nielegalnych (hakerzy). Niektóre firmy muszą znać Twoją historię przeglądania stron lub historię wyszukiwania, aby zaoferować Ci jako reklamę bardziej ukierunkowane produkty lub usługi, związane z Twoimi potrzebami i zainteresowaniami. Inne mogą być zainteresowane nielegalnym celem kradzieży Twoich danych, numeru karty kredytowej, itp.

Istnieją różne sposoby ochrony Twojej tożsamości online, takie jak silne hasła, nie udostępnianie zbyt wielu danych osobowych na portalach społecznościowych, korzystanie z trybu incognito przeglądarki, korzystanie

z wirtualnych sieci prywatnych, szyfrowanie komunikacji itp. Im więcej uwagi poświęca się swojej tożsamości online, tym bardziej jest ona chroniona.

7. Podsumowanie

Wprowadziliśmy podstawowe pojęcia i wiedzę z zakresu zarządzania tożsamością cyfrową i kontem internetowym. Podążając za tymi kluczowymi pojęciami, opisaliśmy, jakie są kwestie bezpieczeństwa i prywatności użytkowników. Na koniec wprowadziliśmy, czym jest ślad cyfrowy i tożsamość online.

Zaproponowaliśmy również łatwe i zrozumiałe metody postępowania z hasłami, uwierzytelnianiem, tożsamością cyfrową, prywatnością i przeglądaniem stron internetowych. Gdy dana osoba lub organizacja podąży za tymi tezami, może w znacznym stopniu ograniczyć wszelkie zagrożenia w sieci. Jak zawsze nie ma rozwiązań, które obejmowałyby wszystkie przypadki i zdrowy rozsądek, a także ustanowienie zasad na poziomie organizacyjnym, które pomogłyby zwalczać złośliwe działania w sieci i zwiększyć zaufanie do korzystania z Internetu i platform cyfrowych jako całości.

Wreszcie zajęliśmy się kwestią tożsamości w Internecie i wskazaliśmy zarówno na to, co ona obejmuje, jak i jak chronić się przed nielegalnym wykorzystywaniem swojej tożsamości.

Bibliografia:

https://www.zdnet.com/article/identity-management-101-how-digital-identity-works/

https://www.forbes.com/sites/forbestechcouncil/2019/06/07/a-beginners-guide-to-online-privacy-12-important-tips/#5092374e53ed

https://assets.mozilla.net/pdf/IHPbriefs_Online_Privacy_March_2017.pdf

https://www.commonsense.org/education/digital-citizenship/topic/digital-footprint-and-identity

https://www.oecd-ilibrary.org/docserver/5jlwt49ccklt-en.pdf?expires=1591780736&id=id&accname=guest&checksum=AF002079529F4DE263769B3FBEB40035