Zabezpieczanie kont

Najsłabszym ogniwem w łańcuchu cyberbezpieczeństwa są prawie zawsze ludzie, a największym zagrożeniem dla Twojego własnego cyberbezpieczeństwa jesteś prawdopodobnie Ty i członkowie Twojej rodziny. W związku z tym cała technologia i wiedza techniczna na świecie nie przyniosą wiele korzyści, jeśli nie zajmiesz się również różnymi ludzkimi niedociągnięciami.

Uświadomienie sobie, że jesteś celem

Być może najważniejszym pierwszym krokiem w zabezpieczeniu się cyfrowo jest zrozumienie, że jesteś celem i że niecne strony mają ochotę włamać się do systemów komputerowych, kont dostępnych elektronicznie i wszystkiego, co tylko mogą dostać w swoje ręce. Nawet jeśli już zdajesz sobie sprawę, że jesteś celem, upewnij się, że w pełni zinternalizowałeś takie pojęcie. Ludzie, którzy naprawdę wierzą, że przestępcy chcą włamać się do ich komputerów i telefonów, zachowują się inaczej niż ludzie, którzy nie do końca doceniają tę rzeczywistość i których brak sceptycyzmu czasami prowadzi ich do kłopotów. Ponieważ członkowie Twojej rodziny również mogą wpływać na Twoje bezpieczeństwo cyfrowe, muszą również mieć świadomość, że są potencjalnymi celami. Jeśli Twoje dzieci podejmują nierozsądne ryzyko w Internecie, mogą nieumyślnie wyrządzić krzywdę nie tylko sobie, ale także Tobie i innym członkom rodziny. W niektórych przypadkach napastnikom udało się zaatakować pracodawców za pośrednictwem połączeń zdalnych, które zostały naruszone, ponieważ dzieci niewłaściwie używały komputerów w tych samych sieciach, co komputery, których pracownicy używali do pracy zdalnej. Zagrożeniem, jakie stwarzają takie ataki, zwykle nie jest to, że przestępca bezpośrednio ukradnie czyjeś pieniądze lub dane, ale raczej to, że jakaś strona będzie próbowała zaszkodzić celowi w inny sposób - sposób, który może ostatecznie przełożyć się na jakąś formę finansową, militarną, polityczne lub inne korzyści dla atakującego i (potencjalnie) jakiekolwiek szkody dla ofiary.

Zabezpieczanie kont zewnętrznych

Wcześniej omówiono, w jaki sposób można nabyć własne produkty technologiczne. Jednak korzystanie z tych produktów nie wystarczy, aby zapewnić Ci cyberbezpieczeństwo, ponieważ bez wątpienia dysponujesz danymi cyfrowymi o znacznej wartości, które są przechowywane poza Twoim fizycznym posiadaniem - to znaczy poza systemami danych i magazynami danych pod Twoją kontrolą. W rzeczywistości dane o każdej osobie żyjącej obecnie w zachodnim świecie są prawdopodobnie przechowywane w systemach komputerowych należących do wielu firm, organizacji, i agencji rządowych. Czasami systemy te znajdują się w obiektach organizacji, do których należą, czasami znajdują się we współdzielonych centrach danych, a czasami same systemy są maszynami wirtualnymi wynajmowanymi od zewnętrznego dostawcy. Ponadto niektóre takie dane mogą znajdować się w systemach chmurowych oferowanych przez stronę trzecią. Dane te można podzielić i podzielić na wiele różnych kategorii, w zależności od tego, jakimi ich aspektami dana osoba jest zainteresowana. następujący schemat:

* Konta i zawarte w nich dane, które użytkownik założył i kieruje

* Dane należące do organizacji, z którymi użytkownik dobrowolnie i świadomie wchodził w interakcję, ale użytkownik nie ma kontroli nad danymi

* Dane będące w posiadaniu organizacji, z którymi użytkownik świadomie nie nawiązał relacji

Rozwiązanie ryzyka związanego z każdym typem danych wymaga innej strategii.

Zabezpieczanie danych powiązanych z kontami użytkowników

Kiedy korzystasz z bankowości internetowej, robisz zakupy online, a nawet przeglądasz sieć, udostępniasz różnego rodzaju dane stronom, z którymi się kontaktujesz. Kiedy zakładasz i utrzymujesz konto w banku, sklepie, serwisie społecznościowym , dostawcy mediów lub inna strona internetowa, zyskujesz kontrolę nad znaczącymi ilościami danych dotyczących Ciebie, które strona przechowuje w Twoim imieniu. Oczywiście nie możesz w pełni kontrolować bezpieczeństwa tych danych, ponieważ nie są one w Twoim posiadaniu. To powiedziawszy, oczywiście masz również duży interes w ochronie tych danych - i nie naruszaniu ochrony danych, które ustanowiła strona hostująca konto. Chociaż każda sytuacja i konto ma swoje unikalne atrybuty, niektóre strategie mogą pomóc chronić Twoje dane przed osobami trzecimi. Oczywiście nie wszystkie pomysły przedstawione w poniższych sekcjach mają zastosowanie do każdej sytuacji, ale zastosowanie odpowiednich pozycji z menu do różnych kont i zachowań online może znacznie zwiększyć szanse na pozostanie w cyberbezpieczeństwie.

Prowadź interesy z renomowanymi stronami

Nie ma nic złego w wspieraniu małych firm - w rzeczywistości jest to godne podziwu. (Prawdą jest również, że wiele dużych firm doświadczyło poważnych naruszeń bezpieczeństwa). Ale jeśli na przykład szukasz najnowszego elektronicznego gadżetu, a jeden sklep, o którym nigdy nie słyszałeś, oferuje go ze znaczną zniżką od cen oferowanych w wszystkie znane sklepy, bądź ostrożny. Może istnieć uzasadniony powód zniżki - lub może to być oszustwo. Zawsze sprawdzaj strony internetowe sklepów, z którymi prowadzisz interesy, aby zobaczyć, czy coś nie wygląda na coś złego - i uważaj, jeśli tak jest.

Korzystaj z oficjalnych aplikacji i stron internetowych

W różnych sklepach z aplikacjami znaleziono klony oficjalnych aplikacji. Jeśli instalujesz aplikację bankową, kartę kredytową lub aplikację zakupową dla określonej firmy, upewnij się, że instalujesz oficjalną aplikację, a nie złośliwego podszywacza. Instaluj aplikacje tylko z renomowanych sklepów z aplikacjami, takich jak Google Play, Amazon AppStore i Apple App Store.

Nie instaluj oprogramowania od niezaufanych stron

Złośliwe oprogramowanie, które infekuje komputer, może przechwytywać poufne informacje zarówno z innych programów, jak i sesji internetowych uruchomionych na urządzeniu. Jeśli witryna oferuje bezpłatne kopie filmów, oprogramowania lub innych elementów, które normalnie są płatne, oferty mogą nie tylko być skradzionymi kopiami, ale także zadać sobie pytanie, w jaki sposób operator zarabia - może to być spowodowane rozpowszechnianiem złośliwego oprogramowania.

Nie rootuj swojego telefonu

Możesz ulec pokusie, aby zrootować telefon - jest to proces, który zapewnia większą kontrolę nad urządzeniem - ale takie działanie osłabia różne możliwości bezpieczeństwa urządzenia i może pozwolić złośliwemu oprogramowaniu na przechwycenie poufnych informacji z innych aplikacji na urządzeniu, co prowadzi do włamań na konto.

Nie podawaj niepotrzebnych poufnych informacji

Nie podawaj prywatnych informacji nikomu, kto ich nie potrzebuje. Na przykład nie podawaj swojego numeru ubezpieczenia społecznego żadnym sklepom internetowym ani lekarzom, ponieważ nie potrzebują go. Pamiętaj, że im mniej informacji o Tobie ma dana strona, tym mniej danych może zostać naruszonych i skorelowanych w przypadku naruszenia.

Korzystaj z usług płatniczych, które eliminują konieczność udostępniania numerów kart kredytowych dostawcom

Usługi takie jak PayPal, Samsung Pay, Apple Pay i tak dalej umożliwiają Ci zarabianie i płatności online bez konieczności podawania sprzedawcy faktycznego numeru karty kredytowej. Jeśli dostawca zostanie naruszony, informacje o Twoim koncie, które prawdopodobnie zostaną skradzione, są znacznie mniej prawdopodobne, aby doprowadzić do oszustwa (i być może nawet różnych form kradzieży tożsamości), niż gdyby faktycznie dane karty kredytowej były przechowywane u dostawcy. Co więcej, główne serwisy płatnicze mają armie wykwalifikowanych specjalistów ds. Bezpieczeństwa informacji, którzy pracują nad ich bezpieczeństwem, z którym dostawcy akceptujący takie płatności rzadko, jeśli w ogóle, mogą się dopasować.

W razie potrzeby użyj jednorazowych numerów wirtualnych kart kredytowych

Niektóre instytucje finansowe umożliwiają korzystanie z aplikacji (lub strony internetowej) w celu tworzenia jednorazowych, jednorazowych wirtualnych numerów kart kredytowych, które umożliwiają obciążenie prawdziwego konta karty kredytowej (powiązanego z numerem wirtualnym) bez konieczności podawania odpowiedniego sprzedaj swój prawdziwy numer karty kredytowej. Niektóre systemy wirtualnych kart kredytowych pozwalają również określić maksymalny dopuszczalny rozmiar obciążenia na konkretnym numerze karty wirtualnej na poziomie znacznie niższym niż na prawdziwej odpowiedniej karcie. Podczas gdy tworzenie jednorazowych numerów wymaga czasu i wysiłku i może być przesadą, gdy powtarzasz transakcje z renomowanym dostawcą, do którego praktyk bezpieczeństwa informacji masz zaufanie, wirtualne numery kart kredytowych oferują korzyści w zakresie ochrony przed potencjalnymi oszustwami i mogą być odpowiednio używane, gdy radzenie sobie z mniej znanymi stronami. Oprócz minimalizowania ryzyka dla siebie, jeśli dostawca okaże się skorumpowany, wirtualne numery kart kredytowych oferują inne korzyści w zakresie bezpieczeństwa. Jeśli przestępcy włamują się do dostawcy i ukradną Twój numer wirtualnej karty kredytowej, który był wcześniej używany, nie tylko nie mogą za jego pomocą pobierać opłat, ale ich próby mogą nawet pomóc organom ścigania w ich wyśledzeniu, a także pomóc zespołom śledczym zidentyfikować źródło wycieku danych o numerze karty kredytowej.

Monitoruj swoje konta

Regularne sprawdzanie nierozpoznanych działań na kontach płatniczych, bankowych i zakupowych to dobry pomysł. Najlepiej byłoby, gdybyś sprawdził to nie tylko w dziennikach transakcji online, ale także sprawdzając odpowiednie miesięczne wyciągi (bez względu na metodę dostawy) pod kątem wszystkiego, co nie należy.

Zgłoś podejrzaną aktywność jak najszybciej

Im szybciej potencjalne oszustwo jest zgłaszane odpowiedzialnym stronom za zajęcie się nim, tym większa szansa na jego odwrócenie i zapobieżenie dalsze nadużywanie materiałów, które zostały wykorzystane w celu popełnienia przestępstwa pierwszy akt oszustwa. Im szybciej zostanie zgłoszone oszustwo, tym większe szansa na złapanie popełniających ją stron.

Zastosuj odpowiednią strategię dotyczącą haseł

Chociaż konwencjonalna mądrość może wymagać skomplikowanych haseł dla wszystkich systemów, taka strategia haseł zawodzi w praktyce. Pamiętaj, aby wdrożyć odpowiednią strategię dotyczącą haseł.

Wykorzystaj uwierzytelnianie wieloskładnikowe

Uwierzytelnianie wieloskładnikowe oznacza uwierzytelnianie, które wymaga od użytkownika uwierzytelnienia przy użyciu co najmniej dwóch z następujących metod:

* Coś, co wie użytkownik, na przykład hasło

* Coś, czym jest użytkownik, na przykład odcisk palca

* Coś, co ma użytkownik, na przykład token sprzętowy

W przypadku bardzo wrażliwych systemów należy używać form uwierzytelniania, które są silniejsze niż same hasła. Wszystkie następujące formy uwierzytelnienia mają swoje miejsce:

* Biometria, czyli wykorzystywanie pomiarów różnych cech człowieka do identyfikacji ludzi. Odciski palców, odciski głosu, skany tęczówki, szybkość, z jaką ludzie wpisują różne znaki na klawiaturze i tym podobne, to przykłady biometrii.

* Certyfikaty cyfrowe, które skutecznie udowadniają systemowi, że dany klucz publiczny reprezentuje osobę prezentującą certyfikat. Jeśli osoba prezentująca certyfikat jest w stanie odszyfrować wiadomości zaszyfrowane kluczem publicznym w certyfikacie, oznacza to, że osoba prezentująca certyfikat posiada odpowiedni klucz prywatny, który powinien posiadać tylko prawowity właściciel.

* Hasła jednorazowe lub jednorazowe tokeny wygenerowane przez aplikacje lub wysłane SMS-em na swój telefon komórkowy.

* Tokeny sprzętowe, które są zazwyczaj małymi urządzeniami elektronicznymi podłączanymi do portu USB, wyświetlającymi numer zmieniający się co minutę lub umożliwiającymi użytkownikom wprowadzenie numeru wyzwania i otrzymanie odpowiedniego numeru odpowiedzi z powrotem. Dzisiaj aplikacje na smartfony pełnią takie funkcje, pozwalając, przynajmniej teoretycznie, smartfonowi przejąć rolę tokena sprzętowego. (Należy pamiętać, że smartfony mogą cierpieć na różnego rodzaju luki w zabezpieczeniach, na które nie mogą wpływać tokeny sprzętowe, więc tokeny sprzętowe są nadal prawdopodobnie bardziej odpowiednie w niektórych sytuacjach wysokiego ryzyka).

* Uwierzytelnianie oparte na wiedzy, które opiera się na prawdziwej wiedzy, a nie zwykłym odpowiadaniu na pytania z niewielką liczbą możliwych odpowiedzi, które często można odgadnąć, np. „Jaki kolor miał Twój pierwszy samochód?” Zwróć uwagę, że technicznie rzecz biorąc, dodanie pytań uwierzytelniających opartych na wiedzy do uwierzytelniania hasła nie tworzy uwierzytelniania wieloskładnikowego, ponieważ zarówno hasło, jak i odpowiedź oparta na wiedzy są przykładami rzeczy, o których wie użytkownik. Jednak takie postępowanie z pewnością poprawia bezpieczeństwo, gdy pytania są odpowiednio wybrane.

Większość instytucji finansowych, firm zajmujących się mediami społecznościowymi i dużych internetowych, sprzedawcy oferują uwierzytelnianie wieloskładnikowe - używaj go. Należy również pamiętać, że wysyłając jednorazowe hasła do smartfonów użytkowników za pośrednictwem wiadomości tekstowych, teoretycznie weryfikuje, czy osoba logująca się posiada smartfon, który ma posiadać użytkownik (coś, co ma użytkownik), różne luki podważają to przypuszczenie. Na przykład przestępca może przechwytywać wiadomości tekstowe, nawet bez, na przykład, przestępca może przechwytywać wiadomości tekstowe, nawet bez posiadania telefonu.

Wyloguj się, gdy skończysz

Nie polegaj na automatycznym przekroczeniu limitu czasu, zamykaniu przeglądarki ani wyłączaniu komputera w celu wylogowania z kont. Wyloguj się za każdym razem, gdy skończysz. Nie zostawiaj siebie zalogowanego między sesjami, chyba że korzystasz z urządzenia, które znasz - tak blisko jak to możliwe - pewność pozostanie bezpieczna.

Użyj własnego komputera lub telefonu

Nie wiesz, jak dobrze ktoś inny zabezpieczył swoje urządzenie - może mieć na nim złośliwe oprogramowanie, które przechwytuje Twoje hasła i inne poufne informacje lub przechwytywanie sesji i wykonywanie wszelkiego rodzaju nikczemnych czynności. Co więcej, pomimo faktu, że jest to bardzo problematyczne, niektóre aplikacje i strony internetowe - do dziś - przechowują dane w punktach końcowych, które są używane do uzyskiwania do nich dostępu. Nie chcesz zostawiać innym ludziom pamiątek ze swoich wrażliwych sesji.

Zablokuj komputer

Zablokuj komputer, którego używasz do uzyskiwania dostępu do poufnych kont, i zabezpiecz go fizycznie.

Używaj oddzielnego, dedykowanego komputera do wrażliwych zadań

Rozważ zakup specjalnego komputera używanego do bankowości internetowej i innych poufnych zadań. Dla wielu ludzi drugi komputer nie jest praktyczny, ale jeśli tak jest, posiadanie takiego komputera - na którym nigdy nie czytasz e-maili, nie uzyskujesz dostępu do mediów społecznościowych, nie przeglądasz internetu itd. - zapewnia korzyści w zakresie bezpieczeństwa.

Używaj oddzielnej, dedykowanej przeglądarki do wrażliwych zadań internetowych

Jeśli nie możesz uzyskać oddzielnego komputera, użyj przynajmniej oddzielnej przeglądarki do ważnych zadań. Nie używaj tej samej przeglądarki, której używasz do czytania wiadomości, sprawdzania postów na blogu i większości innych czynności.

Zabezpiecz swoje urządzenia dostępowe

Każdy telefon, laptop, tablet i komputer stacjonarny używany do uzyskiwania dostępu do bezpiecznych systemów powinien mieć zainstalowane oprogramowanie zabezpieczające, które należy skonfigurować tak, aby regularnie skanowało aplikacje po ich dodaniu, a także uruchamiało okresowe skanowanie ogólne. Upewnij się też, że oprogramowanie jest aktualne - większość produktów z technologią antywirusową działa znacznie lepiej w przypadku nowszych odmian złośliwego oprogramowania, gdy jest na bieżąco, niż gdy nie.

Dbaj o aktualność swoich urządzeń

Oprócz utrzymywania aktualności oprogramowania zabezpieczającego należy zainstalować aktualizacje systemu operacyjnego i programu, aby zmniejszyć ryzyko wystąpienia luk w zabezpieczeniach. Funkcja Windows AutoUpdate i jej odpowiednik na innych platformach mogą uprościć to zadanie.

Nie wykonuj wrażliwych zadań przez publiczne Wi-Fi.

Jeśli musisz wykonać wrażliwe zadanie, gdy jesteś w miejscu, w którym nie masz dostępu do bezpiecznej, prywatnej sieci, rób to, co musisz, przez system komórkowy, a nie przez publiczne Wi-Fi. Publiczne Wi-Fi stwarza po prostu zbyt wiele zagrożeń.

Nigdy nie używaj publicznej sieci Wi-Fi do jakichkolwiek celów w miejscach o wysokim ryzyku

Nie podłączaj żadnego urządzenia, z którego planujesz wykonywać wrażliwe zadania, do sieci Wi-Fi na obszarach, które są podatne na zatrucia cyfrowe - to znaczy do hakowania lub dystrybucji złośliwego oprogramowania do urządzeń łączących się z siecią. Konferencje hakerów i niektóre kraje, takie jak Chiny, które są znane z przeprowadzania cyberszpiegostwa, to przykłady obszarów, w których może wystąpić zatrucie cyfrowe. Wielu specjalistów od cyberbezpieczeństwa zaleca wyłączanie głównego

komputera i telefonu oraz używanie oddzielnego komputera i telefonu podczas pracy w takich środowiskach.

Uzyskuj dostęp do swoich kont tylko wtedy, gdy jesteś w bezpiecznej lokalizacji

Nawet jeśli korzystasz z sieci prywatnej, nie wpisuj haseł do wrażliwych systemów ani nie wykonuj innych poufnych zadań w miejscu, w którym ludzie mogą łatwo oglądać to, co piszesz i zobaczyć Twój ekran.

Ustaw odpowiednie limity

Różne miejsca online pozwalają na ustalenie limitów - na przykład, ile pieniędzy można przelać z konta bankowego, największego obciążenia, jakie można obciążyć kartą kredytową, gdy karta nie jest fizycznie obecna (jak w przypadku zakupów online), czyli maksymalna ilość towarów, które możesz kupić w ciągu jednego dnia. Ustaw te ograniczenia. Nie tylko ograniczą szkody, jeśli przestępca naruszy Twoje konto, ale w niektórych przypadkach mogą wywołać alerty o oszustwach i całkowicie zapobiec kradzieży.

Użyj alertów

Jeśli Twój bank, dostawca kart kredytowych lub często odwiedzany sklep oferuje możliwość ustawiania alertów tekstowych lub e-mailowych, powinieneś poważnie rozważyć skorzystanie z tych usług. Teoretycznie idealnie byłoby, gdyby wystawca wysyłał Ci alert za każdym razem, gdy na Twoim koncie występuje aktywność. Jednak z praktycznego punktu widzenia, jeśli mogłoby to Cię przytłoczyć i spowodować zignorowanie wszystkich wiadomości (jak w przypadku większości ludzi), rozważ poproszenie o powiadomienie o transakcjach przekraczających określoną kwotę w dolarach (co może być być ustawione na różne progi dla różnych sklepów lub rachunków) lub w inny sposób wydawać się emitentowi potencjalnie oszukańczy.

Okresowo sprawdzaj listy urządzeń dostępu

Niektóre witryny i aplikacje - zwłaszcza te instytucji finansowych - pozwalają sprawdzić listę urządzeń, które uzyskały dostęp do Twojego konta. Sprawdzanie tej listy przy każdym logowaniu może pomóc w szybkim zidentyfikowaniu potencjalnych problemów związanych z bezpieczeństwem.

Sprawdź dane ostatniego logowania

Po zalogowaniu się na niektórych stronach internetowych i za pośrednictwem niektórych aplikacji - szczególnie tych instytucji finansowych - możesz zobaczyć informacje o tym, kiedy i skąd ostatnio pomyślnie się zalogowałeś przed bieżącą sesją. Ilekroć jakikolwiek podmiot pokaże Ci takie informacje, rzuć okiem. Jeśli coś jest nie tak, a przestępca niedawno się zalogował, udając Ciebie, może to wyglądać jak obolały kciuk.

Odpowiednio reaguj na wszelkie ostrzeżenia o oszustwach

Jeśli otrzymasz telefon od banku, wystawcy karty kredytowej lub sklepu w sprawie potencjalnego oszustwa na Twoim koncie, odpowiedz szybko. Ale nie rób tego, rozmawiając ze stroną, która do ciebie dzwoniła. Zamiast tego skontaktuj się z punktem sprzedaży pod znanym prawidłowym numerem, który jest reklamowany na jego stronie internetowej.

Nigdy nie wysyłaj żadnych poufnych informacji przez niezaszyfrowane połączenie.

Gdy uzyskujesz dostęp do witryn internetowych, poszukaj ikony kłódki, która wskazuje, że używany jest szyfrowany protokół HTTPS. Dzisiaj HTTPS jest wszechobecny; Wykorzystuje je nawet wiele stron

internetowych, które nie proszą użytkowników o podanie wrażliwych danych. Jeśli nie widzisz ikony, używany jest niezaszyfrowany protokół HTTP. W takim przypadku nie podawaj poufnych informacji ani nie loguj się. Brak kłódki w witrynie, która wyświetla monit o podanie loginu i hasła lub obsługuje transakcje finansowe, jest ogromną czerwoną flagą, że coś jest nie tak. Jednak w przeciwieństwie do tego, co prawdopodobnie słyszałeś w przeszłości, obecność blokady niekoniecznie oznacza, że witryna jest bezpieczna.

Uważaj na ataki socjotechniczne

W kontekście cyberbezpieczeństwa socjotechnika odnosi się do psychologicznej manipulacji dokonywanej przez cyberataków na ich zamierzonych ofiarach w celu wykonania działań, których bez takiej manipulacji cele nie wykonałyby, lub do ujawnienia poufnych informacji, których w innym przypadku by nie ujawnili. Aby uchronić się przed atakami socjotechnicznymi, wszystkie e-maile, SMS-y, rozmowy telefoniczne lub komunikaty w mediach społecznościowych od wszystkich banków, firm obsługujących karty kredytowe, dostawców opieki zdrowotnej, sklepów itp. Należy traktować jako potencjalnie fałszywe. Nigdy nie klikaj linków w takiej korespondencji. Zawsze łącz się z takimi podmiotami wpisując adres URL w pasku adresu przeglądarki internetowej. Więcej informacji na temat zapobiegania atakom z użyciem inżynierii społecznej można znaleźć w rozdziale 8.

Ustal hasła logowania głosowego

Dostęp online to nie jedyna ścieżka, którą przestępca może wykorzystać do włamania się na Twoje konta. Wielu oszustów dokonuje rekonesansu online, a następnie wykorzystuje inżynierię społeczną, aby dostać się na konta ludzi, korzystając ze staroświeckich połączeń telefonicznych z odpowiednimi działami obsługi klienta w organizacjach docelowych. Aby chronić siebie i swoje konta, ustanawiaj hasła logowania głosowego do swoich kont, gdy tylko jest to możliwe - to znaczy, ustawiaj hasła, które należy podać personelowi obsługi klienta, aby mogli oni przekazywać wszelkie informacje z kont lub wprowadzać zmiany w im. Wiele firm oferuje taką możliwość, ale stosunkowo niewiele osób z niej korzysta.

Chroń swój numer telefonu komórkowego

Jeśli korzystasz z silnego uwierzytelniania za pomocą wiadomości tekstowych, najlepiej skonfiguruj numer telefonu do przekazywania połączeń na swój telefon komórkowy i użyj tego numeru podczas podawania numeru telefonu komórkowego. Takie postępowanie zmniejsza prawdopodobieństwo, że przestępcy będą w stanie przechwycić jednorazowe hasła wysyłane na Twój telefon, a także zmniejsza szanse powodzenia różnych innych ataków. Na przykład Google Voice umożliwia ustanowienie nowego numeru telefonu, który przekierowuje na Twój telefon komórkowy, dzięki czemu możesz podać numer inny niż prawdziwy numer telefonu komórkowego i zarezerwować ten numer do wykorzystania w procesie uwierzytelniania.

Nie klikaj linków w e-mailach ani SMS-ach

Klikanie linków to jeden z głównych sposobów przekierowywania ludzi na fałszywe strony internetowe. Na przykład niedawno otrzymałem wiadomość e-mail zawierającą łącze. Gdybym kliknął łącze w wiadomości, zostałbym przeniesiony na fałszywą stronę logowania LinkedIn, która gromadzi kombinacje nazw użytkownika i hasła LinkedIn i udostępnia je przestępcom.

Nie przesadzaj w mediach społecznościowych

Nie chcesz dać przestępcom odpowiedzi na pytania, które są używane do ochrony Twojego konta lub oferowania im informacji, których mogą użyć, aby uzyskać dostęp do Twoich kont za pomocą inżynierii społecznej.

Zwróć uwagę na politykę prywatności

Zrozum, co oznacza witryna, jeśli mówi, że zamierza udostępniać Twoje dane stronom trzecim lub sprzedawać je innym.

Zabezpieczanie danych stronami, z którymi miałeś do czynienia

Kiedy wchodzisz w interakcję ze stroną internetową, nie wszystkie dane są pod Twoją kontrolą. Jeśli przeglądasz witrynę internetową przy typowych ustawieniach przeglądarki internetowej, witryna ta może śledzić Twoją aktywność. Ponieważ wiele witryn dystrybuuje treści od stron trzecich - na przykład z sieci reklamowych - witryny mogą nawet być w stanie śledzić Twoje zachowanie w innych witrynach. Jeśli masz konto na jakichkolwiek witrynach, które wykonują takie śledzenie i logują się, wszystkie witryny wykorzystujące treści dystrybuowane mogą znać Twoją prawdziwą tożsamość i mnóstwo informacji o Tobie - nawet jeśli nigdy nie powiedziałeś im nic o sobie. Nawet jeśli nie masz takiego konta lub nie logujesz się, profile Twojego zachowania mogą być tworzone i wykorzystywane do celów marketingowych, nawet bez wiedzy, kim jesteś. (Oczywiście, jeśli kiedykolwiek zalogujesz się w przyszłości do dowolnej witryny korzystającej z sieci, wszystkie witryny z profilami mogą powiązać je z Twoją prawdziwą tożsamością. O wiele trudniej jest chronić dane o Tobie, które są w posiadaniu osób trzecich. stron, ale to nie jest pod twoją kontrolą niż ochrona danych na twoich kontach. Nie oznacza to jednak, że jesteś bezsilny. (Jak na ironię i niestety, większość właścicieli takich danych prawdopodobnie lepiej chroni dane ludzie niż sami ludzie. Oprócz stosowania strategii z poprzedniej sekcji możesz chcieć przeglądać w sesjach prywatnych. Na przykład za pomocą przeglądarki Tor - która automatycznie kieruje cały ruch internetowy przez komputery na całym świecie przed wysłaniem do miejsca docelowego - utrudniasz osobom trzecim śledzenie Cię. Pakiet przeglądarki Tor jest bezpłatny i zawiera wszystkie rodzaje funkcji związanych z prywatnością, w tym blokowanie plików cookie i odcisków palców na płótnie, zaawansowana forma tra urządzenia ckingowe. Jeśli Tor wydaje się skomplikowany, możesz również skorzystać z renomowanej usługi VPN do podobnych celów. Korzystając z technologii przeglądania, która utrudnia witrynom śledzenie Cię, jest mniej prawdopodobne, że utworzą szczegółowe profile o Tobie - a im mniej danych o Tobie mają, tym mniej danych o Tobie można ukraść. Poza tym możesz nie chcieć, aby te strony tworzyły profile o tobie na pierwszym miejscu. Jedną z technologii, która pomimo swojej nazwy nie uniemożliwia śledzenia na poziomie zbliżonym do Tora lub VPN, jest tryb prywatny oferowany przez większość przeglądarek internetowych. Niestety, pomimo swojej nazwy, tryb prywatny ma pod tym względem wiele poważnych słabości i nie zbliża się do zapewnienia prywatności.

Zabezpieczanie danych na stronach, z którymi nie miałeś interakcji

Wiele podmiotów prawdopodobnie przechowuje znaczne ilości danych o Tobie, mimo że nigdy świadomie nie wchodziłeś z nimi w interakcje ani w inny sposób nie upoważniłeś ich do przechowywania takich informacji. Na przykład co najmniej jedna duża usługa mediów społecznościowych tworzy de facto profile dla osób, które nie mają kont w tej usłudze, ale zostały wspomniane przez inne osoby lub które weszły w interakcję z witrynami wykorzystującymi różne widżety społecznościowe lub inne powiązane technologie. Usługa może następnie używać tych profili do celów marketingowych - nawet w niektórych przypadkach bez znajomości prawdziwej tożsamości osoby. Ponadto różne serwisy informacyjne, które zbierają informacje z wielu publicznych baz danych, tworzą profile w oparciu o takie dane zawierające szczegóły, o których możesz nawet nie zdawać sobie sprawy, że są publicznie dostępne. Niektóre strony genealogiczne wykorzystują wszelkiego rodzaju

publiczne rejestry, a także pozwalają ludziom aktualizować informacje o innych osobach. Ta możliwość może prowadzić do sytuacji, w których wszelkiego rodzaju niepubliczne informacje o Tobie mogą być dostępne dla subskrybentów witryny (lub osób z bezpłatnymi subskrypcjami próbnymi) bez Twojej wiedzy lub zgody. Takie witryny ułatwiają znajdowanie nazwisk panieńskich matek, co podważa schemat uwierzytelniania używany przez wiele organizacji. Oprócz witryn z drzewami genealogicznymi, różne profesjonalne witryny przechowują informacje o zawodowych historiach, publikacjach i tak dalej. I oczywiście biura informacji kredytowej przechowują wszelkiego rodzaju informacje o Twoim postępowaniu z kredytem - takie informacje są im przekazywane przez instytucje finansowe, agencje windykacyjne i tak dalej. Chociaż ustawa Fair Credit Reporting Act może pomóc w zarządzaniu informacjami o tobie, które mają biura, nie może pomóc w usunięciu negatywnych informacji, które pojawiają się w innych miejscach, na przykład w starych artykułach prasowych, które są online. Oprócz konsekwencji takich dla prywatności, jeśli jakiekolwiek informacje w tych artykułach dostarczą odpowiedzi na pytania kwestionujące używane do uwierzytelniania, może to spowodować zagrożenie bezpieczeństwa. W takich przypadkach warto skontaktować się z dostawcą danych, wyjaśnić sytuację i poprosić o usunięcie danych. W niektórych przypadkach będą współpracować. Ponadto niektóre firmy, takie jak firmy ubezpieczeniowe i apteki, przechowują informacje medyczne o ludziach. Zwykle osoby fizyczne mają niewielką kontrolę nad takimi danymi. Oczywiście tego typu dane, które nie są pod Twoją pełną kontrolą, mogą mieć na Ciebie wpływ. Najważniejsze jest to, że wiele podmiotów prawdopodobnie przechowuje znaczne ilości danych o tobie, nawet jeśli nigdy nie wchodziłeś z nimi w bezpośrednią interakcję. Obowiązkiem takich organizacji jest ochrona swoich magazynów danych, ale nie zawsze robią to w odpowiedni sposób. Jak zauważa Federalna Komisja Handlu na swojej stronie internetowej, naruszenie danych w biurze kredytowym Equifax, odkryte w 2017 roku, ujawniło wrażliwe dane osobowe 143 milionów Amerykanów. Rzeczywistość jest taka, że poza przypadkami, w których można ręcznie aktualizować rekordy lub żądać ich aktualizacji, niewiele można zrobić, aby chronić dane w takich scenariuszach