Hasła

Większość współczesnych ludzi zna pojęcie haseł i ich wykorzystanie w dziedzinie cyberbezpieczeństwa. A jednak jest ich tak wielu z błędnym przekonaniem na temat haseł i dezinformacja na ich temat rozprzestrzeniły się jak pożar, często prowadząc do podważania własnego bezpieczeństwa ze złymi praktykami dotyczącymi haseł. W tym rozdziale poznasz najlepsze praktyki dotyczące haseł. Te praktyki powinny pomóc zarówno zmaksymalizować własne bezpieczeństwo, jak i zachować rozsądną łatwość użytkowania.

Hasła: podstawowa forma uwierzytelniania

Uwierzytelnianie za pomocą hasła odnosi się do procesu weryfikacji tożsamości użytkownika (niezależnie od tego, czy jest to proces ludzki, czy komputerowy) poprzez poproszenie tego użytkownika o podanie hasła - to jest wcześniej uzgodnionej tajnej informacji - której rzekomo strona uwierzytelniająca wiedzieć, czy naprawdę był stroną, za którą się podaje. Chociaż termin hasło sugeruje, że informacja składa się z jednego słowa, dzisiejsze hasła mogą zawierać kombinacje znaków, które nie tworzą słów w żadnym języku mówionym ani pisanym. Pomimo dostępności od dziesięcioleci wielu innych podejść i technologii uwierzytelniania - z których wiele oferuje znaczną przewagę nad hasłami - hasła pozostają de facto światowym standardem uwierzytelniania osób online. Powtarzające się przepowiednie upadku haseł okazały się nieprawdziwe, a liczba używanych haseł rośnie każdego dnia. Ponieważ uwierzytelnianie haseł jest tak powszechne, a tak wiele naruszeń danych skutkowało włamaniem do baz danych haseł, temat wzbudził duże zainteresowanie mediów, a raporty często rozpowszechniały różne wprowadzające w błąd informacje. Uzyskanie właściwego zrozumienia sfery haseł jest ważne, jeśli chcesz być cyberbezpieczny.

Unikanie prostych haseł

Hasła zabezpieczają systemy tylko wtedy, gdy nieupoważnione osoby nie mogą ich łatwo odgadnąć. Przestępcy często odgadują hasła

* Odgadywanie typowych haseł: Nie jest tajemnicą, że 123456 i hasło to wspólne hasła - dane z niedawnych naruszeń ujawniają, że są one w rzeczywistości jednymi z najczęściej używanych haseł w wielu systemach (patrz: pasek boczny obok)! Przestępcy wykorzystują tę smutną rzeczywistość i często próbują włamać się do kont za pomocą zautomatyzowanych narzędzi, które pojedynczo wprowadzają hasła do systemów z list typowych haseł - i rejestrują, kiedy trafią. Niestety, takich hitów jest często sporo.

* Rozpoczynanie ataków słownikowych: ponieważ wiele osób decyduje się na używanie rzeczywistych angielskich słów jako haseł, niektóre zautomatyzowane narzędzia hakerskie po prostu przekazują wszystkie słowa ze słownika do systemu pojedynczo. Podobnie jak w przypadku list typowych haseł, takie ataki często prowadzą do wielu trafień.

* Wypychanie poświadczeń: Wypychanie poświadczeń odnosi się do sytuacji, gdy atakujący pobierają listy nazw użytkowników i haseł z jednej witryny - na przykład z witryny, która została naruszona i której baza danych z hasłami nazw użytkowników została następnie opublikowana online - i przekazują jej wpisy do innego systemu pojedynczo. w celu sprawdzenia, czy którekolwiek z poświadczeń logowania z pierwszego systemu działa z drugim. Ponieważ wiele osób ponownie używa kombinacji nazwy użytkownika i hasła między systemami, upychanie danych uwierzytelniających jest, ogólnie rzecz biorąc, dość skuteczne.

Uwagi dotyczące hasła

Podczas tworzenia haseł należy pamiętać, że bardziej złożone nie zawsze są lepsze, a wybrana siła hasła powinna zależeć od tego, jak wrażliwe są dane i system chroniony hasłem. W poniższych sekcjach omówiono hasła, które można łatwo odgadnąć, hasła skomplikowane, hasła wrażliwe i menedżery haseł.

Hasła osobiste, które łatwo odgadnąć

Przestępcy wiedzą, że wiele osób używa jako hasła imienia i nazwiska lub daty urodzenia ich bliskiej osoby lub zwierzaka, więc oszuści często przeglądają profile w mediach społecznościowych i wyszukują w Google, aby znaleźć prawdopodobne hasła. Używają również zautomatyzowanych narzędzi do przesyłania list nazw pospolitych do systemów docelowych jeden po drugim, jednocześnie obserwując, czy atakowany system akceptuje którekolwiek z nazw jako prawidłowe hasło. Przestępcy, którzy przeprowadzają ataki ukierunkowane, mogą wykorzystać lukę stworzoną przez takie spersonalizowane, ale łatwe do odgadnięcia hasła. Jednak problem jest znacznie większy: czasami rozpoznanie odbywa się za pomocą zautomatyzowanych środków - więc nawet oportunistyczni napastnicy mogą wykorzystać takie podejście. Co więcej, ponieważ z definicji znaczny procent ludzi ma pospolite imiona, często automatyczne podajniki nazw zwyczajowych aby osiągnąć znaczną liczbę trafień. Skomplikowane hasła nie zawsze są lepsze. Aby rozwiązać problemy związane ze słabymi hasłami, wielu ekspertów zaleca używanie długich, złożonych haseł - na przykład zawierających zarówno wielkie, jak i małe litery, a także cyfry i znaki specjalne.

Używanie takich haseł w teorii ma sens, a jeśli taki schemat jest używany do zabezpieczenia dostępu do niewielkiej liczby wrażliwych systemów, może działać całkiem dobrze. Jednak zastosowanie takiego modelu dla większej liczby haseł może prowadzić do problemów, które mogą zagrozić bezpieczeństwu:

* Niewłaściwe ponowne wykorzystanie haseł

* Zapisywanie haseł w niezabezpieczonych lokalizacjach

* Wybieranie haseł o słabej randomizacji i sformatowanych przy użyciu przewidywalnych wzorców, takich jak użycie wielkiej litery jako pierwszej litery skomplikowanego hasła, po której następują wszystkie małe litery, a następnie liczba. Dlatego w prawdziwym świecie, z praktycznego punktu widzenia, ponieważ ludzki umysł nie może zapamiętać wielu złożonych haseł, użycie dużej liczby złożonych haseł może spowodować poważne zagrożenie bezpieczeństwa. Według The Wall Street Journal, Bill Burr, autor specjalnej publikacji NIST 800-63 Dodatek A (która omawia wymagania dotyczące złożoności haseł), przyznał niedawno, że złożoność haseł zawiodła w praktyce. Obecnie zaleca używanie do uwierzytelniania haseł, a nie skomplikowanych haseł.

Hasła to hasła składające się z całych fraz lub ciągów znaków o długości frazy, a nie tylko z jednego słowa lub z grupy znaków o długości słowa. Czasami frazy hasła składają się nawet z całych zdań. Pomyśl o hasłach jako długich (zwykle przynajmniej 25 znaków), ale stosunkowo łatwych do zapamiętania.

Różne poziomy czułości

Nie wszystkie typy danych wymagają tego samego poziomu ochrony hasłem. Na przykład rząd nie chroni swoich niesklasyfikowanych systemów w ten sam sposób, w jaki zabezpiecza ściśle tajne informacje i infrastrukturę. Klasyfikuj w umyśle lub na papierze systemy, do których potrzebujesz bezpiecznego dostępu. Następnie nieformalnie sklasyfikuj systemy, do których uzyskujesz dostęp, i odpowiednio ustal własne nieformalne zasady dotyczące haseł. Na podstawie poziomów ryzyka możesz swobodnie stosować różne strategie dotyczące haseł. Hasła losowe, hasła złożone z wielu słów, które mogą być oddzielone cyframi, frazami, a nawet hasłami prostymi, mają odpowiednie zastosowania. Oczywiście uwierzytelnianie wieloskładnikowe może i powinno pomóc zwiększyć

bezpieczeństwo, gdy jest zarówno odpowiednie, jak i dostępne. Ustalenie silniejszego hasła do bankowości internetowej niż do komentowania bloga, na którym planujesz skomentować tylko raz w błękitnym księżycu, ma sens. Podobnie, Twoje hasło do bloga powinno być prawdopodobnie silniejsze niż to używane do uzyskania dostępu do bezpłatnej witryny z wiadomościami, która wymaga zalogowania się, ale na której nigdy niczego nie publikujesz i na którą, gdyby ktoś włamał się na Twoje konto, naruszenie nie miałoby żadnego wpływu na ciebie. Twoje najbardziej wrażliwe hasła mogą nie być tymi, które myślisz. Podczas klasyfikowania swoich haseł pamiętaj, że chociaż ludzie często uważają, że ich hasła do bankowości internetowej i innych systemów finansowych są najbardziej wrażliwymi hasłami, nie zawsze tak jest. Ponieważ wiele nowoczesnych systemów online umożliwia ludziom resetowanie haseł po zweryfikowaniu ich tożsamości za pomocą wiadomości e-mail wysłanych na ich wcześniej znane adresy e-mail, przestępca, który uzyska dostęp do czyjegoś konta e-mail, może być w stanie zrobić o wiele więcej niż tylko czytać wiadomości e-mail bez upoważnienia: Może on być w stanie zresetować hasła tego użytkownika do wielu systemów, w tym do niektórych instytucji finansowych. Podobnie wiele witryn korzysta z funkcji uwierzytelniania opartych na mediach społecznościowych - szczególnie tych dostarczanych przez Facebooka i Twittera - więc złamane hasło na platformie mediów społecznościowych może prowadzić do nieautoryzowanego dostępu do innych systemów, z których niektóre mogą być dość nieco bardziej wrażliwy z natury niż witryna, w której po prostu udostępniasz zdjęcia. Możesz ponownie używać haseł - czasami możesz być zaskoczony czytaniem tego oświadczenia w książce o bezpieczeństwie informacji: Nie musisz używać silnych haseł do kont, które tworzysz wyłącznie dlatego, że witryna wymaga logowania, ale z Twojej perspektywy nie jest to konieczne chroń wszystko, co ma wartość. Jeśli na przykład utworzysz konto w celu uzyskania dostępu do bezpłatnych zasobów i nie masz na nim nic wartościowego, a nie masz nic przeciwko założeniu nowego konta przy następnym logowaniu, możesz nawet użyć słabego hasło - i użyj go ponownie w innych podobnych witrynach.

Zasadniczo pomyśl o tym w ten sposób: jeśli wymóg rejestracji i logowania służy wyłącznie właścicielowi witryny - śledzenie użytkowników, reklamowanie ich itd. - i nie ma dla Ciebie znaczenia, czy przestępca uzyskał dane dostępu do Twojego konta i zmienił je, użyj prostego hasła. Pozwoli to zachować pamięć dla witryn, w których liczy się siła hasła. Oczywiście, jeśli korzystasz z menedżera haseł, możesz użyć silniejszego hasła do takich witryn.

Rozważ użycie menedżera haseł

Alternatywnie możesz użyć narzędzia do zarządzania hasłami, aby bezpiecznie przechowywać swoje hasła. Menedżery haseł to oprogramowanie, które pomaga ludziom zarządzać hasłami poprzez generowanie, przechowywanie i odzyskiwanie złożonych haseł. Menedżerowie haseł zwykle przechowują wszystkie swoje dane w zaszyfrowanych formatach i zapewniają dostęp użytkownikom dopiero po uwierzytelnieniu ich za pomocą silnego hasła lub uwierzytelniania wieloskładnikowego. Taka technologia jest odpowiednia dla haseł ogólnych, ale nie dla najbardziej wrażliwych. Różne menedżery haseł zostały zhakowane i jeśli coś pójdzie nie tak, gdy wszystkie jajka są w jednym koszyku, możesz mieć koszmar na rękach. Oczywiście pamiętaj, aby odpowiednio zabezpieczyć każde urządzenie, którego używasz do uzyskiwania dostępu do swojego menedżera haseł. Na rynku jest wielu menedżerów haseł. Podczas gdy wszyscy używają szyfrowania do ochrony przechowywanych w nich poufnych danych, niektórzy przechowują hasła lokalnie (na przykład w bazie danych w telefonie), a inni przechowują je w chmurze. Wiele nowoczesnych smartfonów jest wyposażonych w tak zwany bezpieczny obszar - prywatną, zaszyfrowaną przestrzeń, która jest podzielona na piaskownicę lub oddzielona od własnego środowiska roboczego. W idealnym przypadku wszelkie informacje o hasłach przechowywane na urządzeniu mobilnym są przechowywane w bezpiecznym obszarze. Do danych przechowywanych w bezpiecznym obszarze nie można uzyskać dostępu, chyba że użytkownik wejdzie

do bezpiecznego obszaru, zwykle po uruchomieniu aplikacji do bezpiecznego obszaru i wprowadzeniu specjalnego hasła. urządzenia zazwyczaj wyświetlają również jakiś specjalny symbol gdzieś na ekranie, gdy użytkownik pracuje z danymi lub aplikacją znajdującą się w bezpiecznym obszarze.

Tworzenie niezapomnianych, silnych haseł

Poniższa lista zawiera sugestie, które mogą pomóc w tworzeniu silnych haseł, które dla większości ludzi są o wiele łatwiejsze do zapamiętania niż pozornie przypadkowa, niezrozumiała mieszanka liter, cyfr i symboli:

* Połącz trzy lub więcej niepowiązanych ze sobą słów i nazw własnych, oddzielając je liczbami. Na przykład laptop2william7cows jest znacznie łatwiejszy do zapamiętania niż 6ytBgv% j8P. Ogólnie rzecz biorąc, im dłuższe słowa użyte w haśle, tym silniejsze będzie hasło wynikowe.

* Jeśli musisz użyć znaku specjalnego, dodaj znak specjalny przed każdą liczbą; możesz nawet użyć tego samego znaku we wszystkich swoich hasłach. (Jeśli używasz tych samych haseł co w poprzednim przykładzie i postępujesz zgodnie z tą radą, hasło to% 2william% 7cows do laptopa). Teoretycznie ponowne użycie tego samego znaku może nie być najlepszym sposobem robienia rzeczy z punktu widzenia bezpieczeństwa, ale czyni to znacznie łatwiejszym w zapamiętywaniu, a bezpieczeństwo powinno nadal być wystarczająco dobre do celów, do których hasło i tak jest odpowiednie samo w sobie.

* Najlepiej użyć przynajmniej jednego słowa innego niż angielski lub nazwy własnej. Wybierz słowo lub nazwę, które są Ci znane, ale inni raczej nie zgadną. Nie używaj imienia drugiej połówki, najlepszego przyjaciela ani zwierzaka.

* Jeśli musisz używać wielkich i małych liter (lub chcesz, aby hasło było jeszcze silniejsze), użyj wielkich liter, które zawsze pojawiają się w określonym miejscu we wszystkich silnych hasłach. Upewnij się jednak, że nie umieszczasz ich na początku słów, ponieważ większość ludzi je umieszcza w tym miejscu. Na przykład, jeśli wiesz, że zawsze zapisujesz drugą i trzecią literę ostatniego słowa wielką literą, to laptop2william7kALb nie jest trudniejszy do zapamiętania niż laptop2william7kalb.

Wiedząc, kiedy zmienić hasło

Konwencjonalna mądrość - jak zapewne słyszałeś wiele razy - jest taka, że idealnie jest dość często zmieniać hasło. Na przykład American Association of Retired Persons (AARP) zaleca na swojej stronie internetowej, aby ludzie (w tym nieproporcjonalnie starsi ludzie, którzy wchodzą w jego skład) „często zmieniali najważniejsze hasła, prawdopodobnie co drugi tydzień". Teoretycznie takie podejście jest poprawne - częste zmiany zmniejszają ryzyko na kilka sposobów - ale w rzeczywistości jest to zła rada, której nie należy stosować.

Jeśli masz konto bankowe, kredyt hipoteczny, kilka kart kredytowych, rachunek za telefon, rachunek za szybkie łącze internetowe, rachunki za media, konta w mediach społecznościowych, konta e-mail itp., Możesz łatwo mówić o kilkunastu krytycznych hasłach. Zmiana ich co dwa tygodnie oznaczałaby 312 nowych krytycznych haseł do zapamiętania w ciągu każdego roku - a oprócz tego prawdopodobnie masz o wiele więcej haseł. Dla wielu osób zmiana ważnych haseł co dwa tygodnie może oznaczać naukę stu nowych haseł każdego miesiąca. Jeśli nie masz fenomenalnej, fotograficznej pamięci, jakie jest prawdopodobieństwo, że zapamiętasz wszystkie takie hasła? A może po prostu osłabisz swoje hasła, aby ułatwić ich zapamiętanie po częstych zmianach? Najważniejsze jest to, że zmiana haseł często znacznie utrudnia ich zapamiętanie, zwiększając prawdopodobieństwo, że zapiszesz je i przechowujesz w niebezpieczny sposób, wybierzesz słabsze hasła i / lub ustawisz nowe hasła tak, aby były takie same jak stare hasła z minutą zmiany (na przykład hasło2, aby zastąpić hasło1). Oto rzeczywistość: jeśli na

początku wybierzesz silne, unikalne hasła, a witryny, w których ich używasz, nie zostały prawdopodobnie przejęte, wady częstej zmiany haseł przeważają nad zaletami. Dobrym pomysłem może być zmiana takich haseł co kilka lat. W rzeczywistości, jeśli system ostrzega Cię o wielu nieudanych próbach zalogowania się na Twoje konto, a Ty nie jesteś powiadamiany o takiej aktywności, prawdopodobnie możesz przetrwać wiele lat bez zmian bez narażania się na znaczne ryzyko. Oczywiście, jeśli używasz menedżera haseł, który może resetować hasła, możesz skonfigurować go tak, aby często je resetował. W rzeczywistości pracowałem z komercyjnym systemem zarządzania hasłami używanym do ochrony dostępu administratora do poufnych systemów finansowych, który automatycznie resetował hasła administratorów przy każdym logowaniu.

Zmiana haseł po naruszeniu

Jeśli otrzymasz powiadomienie od firmy, organizacji lub podmiotu rządowego, że doszło do naruszenia bezpieczeństwa i należy zmienić hasło, postępuj zgodnie z poniższymi wskazówkami:

* Nie klikaj żadnych linków w wiadomości, ponieważ większość takich wiadomości to oszustwa.

* Odwiedź witrynę internetową organizacji i oficjalne konta w mediach społecznościowych, aby sprawdzić, czy takie ogłoszenie rzeczywiście zostało wydane.

* Zwróć uwagę na wiadomości, aby zobaczyć, czy wiarygodne media głównego nurtu donoszą o takim naruszeniu.

* Jeśli historia się sprawdzi, przejdź do witryny internetowej organizacji i wprowadź zmianę.

Nie zmieniaj wszystkich swoich haseł po każdym naruszeniu. Zignoruj ekspertów, którzy płaczą wilkiem i każą ci to robić po każdym naruszeniu, aby zachować dodatkową ostrożność. Nie jest to konieczne, pochłania Twój mózg, czas i energię oraz zniechęca Cię do zmiany haseł, gdy jest to rzeczywiście konieczne. W końcu, jeśli dokonasz takich zmian hasła, a następnie dowiesz się, że Twoi znajomi, którzy nie wypadli gorzej od Ciebie po włamaniu, możesz się zmęczyć i zignorować przyszłe ostrzeżenia, aby zmienić hasło, gdy to zrobisz.

Jeśli ponownie używasz haseł w witrynach, w których hasła mają znaczenie - czego nie powinieneś robić - a hasło, które zostało gdzieś przejęte, jest również używane w innych witrynach, pamiętaj, aby zmienić je również w innych witrynach. W takim przypadku skorzystaj z okazji podczas resetowania haseł, aby przełączyć się na unikalne hasła dla każdej z witryn.

Dostarczanie haseł ludziom

Na swojej stronie internetowej Federalna Komisja Handlu Stanów Zjednoczonych (FTC) zaleca:

Nie udostępniaj haseł przez telefon, SMS-y ani e-maile. Legalne firmy nie będą wysyłać Ci wiadomości z prośbą o podanie hasła.

Brzmi to jak dobra rada i byłaby, gdyby nie jeden ważny fakt: legalne firmy proszą Cię o hasło przez telefon! Skąd więc wiesz, kiedy podanie hasła jest bezpieczne, a kiedy nie?

Czy powinieneś po prostu sprawdzić swój identyfikator dzwoniącego? Nie. Smutna rzeczywistość jest taka, że oszuści regularnie fałszują identyfikatory rozmówców.

Nigdy nie należy podawać żadnych poufnych informacji - w tym hasła, oczywiście przez telefon, chyba że zainicjowałeś połączenie ze stroną żądającą hasła i jesteś pewien, że zadzwoniłeś do uprawnionej strony. Na przykład podanie hasła dostępu do konta telefonicznego przedstawicielowi obsługi klienta, który prosi o nie podczas rozmowy zainicjowanej przez dzwoniącego do banku za pomocą numeru

wydrukowanego na karcie bankomatowej, jest znacznie mniej ryzykowne, niż gdyby ktoś dzwonił do Ciebie z roszczeniem pochodzić z banku i prosi o podanie tych samych prywatnych informacji w celu „zweryfikowania Twojej tożsamości".

Przechowywanie haseł

Najlepiej nie zapisuj swoich haseł do wrażliwych systemów ani nie przechowuj ich w żadnym innym miejscu niż mózg. W przypadku mniej wrażliwych haseł użyj menedżera haseł lub przechowuj je w postaci zaszyfrowanej na silnie zabezpieczonym komputerze lub urządzeniu. Jeśli przechowujesz hasła w telefonie, korzystaj z bezpiecznego obszaru.

Przesyłanie haseł

Teoretycznie nigdy nie powinieneś wysyłać e-maili ani SMS-ów z hasłem. Co więc powinieneś zrobić, jeśli Twoje dziecko pisze do Ciebie ze szkoły, mówiąc, że zapomniało hasła do swojego adresu e-mail lub w podobny sposób? Najlepiej, jeśli musisz podać komuś hasło, zadzwoń do niego i nie podawaj hasła, dopóki nie zidentyfikujesz drugiej strony za pomocą głosu. Jeśli z jakiegoś powodu musisz wysłać hasło na piśmie, wybierz szyfrowane połączenie, które jest oferowane przez różne narzędzia do czatu. Jeśli takie narzędzie nie jest dostępne, rozważ podzielenie hasła i wysłanie niektórych e-mailem, a innych SMS-em. Oczywiście żadna z tych metod nie jest idealnym sposobem przesyłania haseł, ale z pewnością są one lepszymi opcjami niż to, co robi tak wiele osób, czyli zwykłe wysyłanie haseł tekstem lub e-mailem w postaci zwykłego tekstu.

Odkrywanie alternatyw dla haseł

W niektórych przypadkach powinieneś skorzystać z alternatyw dla uwierzytelniania hasłem. Chociaż istnieje wiele sposobów uwierzytelniania ludzi, współczesny użytkownik może napotkać pewne typy:

* Uwierzytelnianie biometryczne

* Uwierzytelnianie za pomocą wiadomości SMS

* Hasła jednorazowe oparte na aplikacji

* Uwierzytelnianie za pomocą tokena sprzętowego

* Uwierzytelnianie oparte na USB

Uwierzytelnianie biometryczne

Uwierzytelnianie biometryczne odnosi się do uwierzytelniania przy użyciu unikalnego identyfikatora osoby fizycznej - na przykład odcisku palca. Korzystanie z biometrii - zwłaszcza w połączeniu z hasłem - może być silną metodą uwierzytelniania i na pewno ma swoje miejsce. Dwie popularne formy stosowane na rynku konsumenckim to odciski palców i uwierzytelnianie na podstawie tęczówki. Jednak w wielu przypadkach lepiej będzie, jeśli użyjesz silnego hasła. Przed użyciem uwierzytelniania biometrycznego weź pod uwagę następujące kwestie:

* Twoje odciski palców są prawdopodobnie na całym telefonie. Trzymasz telefon palcami. Jak trudne byłoby dla przestępców, którzy kradną telefon, podniesienie Twoich odcisków i odblokowanie telefonu, jeśli włączysz uwierzytelnianie oparte na odciskach palców za pomocą wbudowanego czytnika linii papilarnych (patrz Rysunek 7-3)? Jeśli na urządzeniu znajduje się czuły przedmiot, może to być zagrożone. Nie, przeciętny oszust, który chce szybko zarobić na sprzedaży twojego telefonu, raczej nie poświęci czasu na jego odblokowanie - najprawdopodobniej po prostu go wyczyści - ale jeśli

ktoś chce mieć dane z twojego telefonu z jakiegokolwiek powodu, a ty używane odciski palców do zabezpieczenia urządzenia, możesz mieć poważny problem z rękami.

* Jeśli przechwycono Twoje dane biometryczne, nie możesz ich zresetować, tak jak hasła. Czy w pełni ufasz stronom, którym przekazujesz te informacje, że będą je odpowiednio chronić?

* Jeśli Twoje dane biometryczne znajdują się w telefonie lub komputerze, co się stanie, jeśli złośliwe oprogramowanie w jakiś sposób zainfekuje Twoje urządzenie? Co się stanie, jeśli serwer, na którym przechowujesz te same informacje, zostanie naruszony? Czy jesteś pewien, że wszystkie dane są prawidłowo zaszyfrowane, a oprogramowanie na Twoim urządzeniu w pełni chroni dane biometryczne przed przechwyceniem?

* Zimna pogoda stwarza problemy. Odcisków palców nie można odczytać nawet przez rękawiczki zgodne ze smartfonem.

* Okulary noszone przez miliony ludzi stanowią wyzwanie dla skanerów tęczówki. Niektóre czytniki tęczówki wymagają od użytkownika zdjęcia okularów w celu uwierzytelnienia. Jeśli używasz takiego uwierzytelniania do zabezpieczenia telefonu, możesz mieć trudności z odblokowaniem telefonu, gdy przebywasz na zewnątrz w słoneczny dzień.

* Biometria może podważyć Twoje prawa. Jeśli z jakiegoś powodu organy ścigania chcą uzyskać dostęp do danych w telefonie chronionym biometrycznie lub innym systemie komputerowym, może być w stanie zmusić Cię do podania uwierzytelnienia biometrycznego, nawet w krajach takich jak Stany Zjednoczone, w których masz prawo. milczeć i nie podawać hasła. Podobnie rząd może być w stanie uzyskać nakaz zebrania danych biometrycznych, których nie można zresetować w przeciwieństwie do hasła. Nawet jeśli dane udowodnią, że jesteś niewinny wobec tego, co rząd podejrzewa, że zrobiłeś źle, czy ufasz, że rząd odpowiednio zabezpieczy dane w perspektywie długoterminowej?

* Podszywanie się jest możliwe. Niektóre quasi-biometryczne uwierzytelnianie, takie jak rozpoznawanie twarzy na niektórych urządzeniach, można oszukać, aby uwierzyć, że dana osoba jest obecna, odtwarzając jej wideo w wysokiej rozdzielczości z tą osobą.

* Uwierzytelnianie głosowe jest przydatne w przypadku połączeń głosowych. Ten typ uwierzytelniania jest szczególnie przydatny w połączeniu z innymi formami uwierzytelniania, takimi jak hasło. Wiele organizacji używa go do uwierzytelniania klientów, którzy czasami dzwonią, nawet o tym nie informując. Mimo to uwierzytelnianie głosowe nie może być używane w sesjach online bez przeszkadzania użytkownikom.

Jako takie biometria ma swoje miejsce. Używanie odcisku palca do odblokowywania funkcji w telefonie jest z pewnością wygodne, ale zastanów się, zanim przejdziesz dalej. Upewnij się, że w Twoim przypadku korzyści przeważają nad wadami.

Uwierzytelnianie za pomocą wiadomości SMS

W przypadku uwierzytelniania opartego na wiadomościach SMS kod jest wysyłany na Twój telefon komórkowy. Następnie wpisujesz ten kod w witrynie lub aplikacji, aby potwierdzić swoją tożsamość. Ten typ uwierzytelniania sam w sobie nie jest uważany za wystarczająco bezpieczny do uwierzytelnienia, gdy wymagane jest prawdziwe uwierzytelnianie wieloskładnikowe. Wyrafinowani przestępcy potrafią przechwytywać takie hasła, a socjotechnika firm telekomunikacyjnych w celu przejmowania numerów telefonów pozostaje problemem. To powiedziawszy, jednorazowe hasła SMS używane w połączeniu z silnym hasłem są krokiem powyżej samego użycia hasła. Pamiętaj jednak, że w większości przypadków jednorazowe hasła są bezwartościowe jako środek bezpieczeństwa, jeśli

wysyłasz je do witryny wyłudzającej informacje, a nie do legalnej witryny. Przestępca może odtworzyć je na prawdziwej stronie w czasie rzeczywistym.

Hasła jednorazowe oparte na aplikacji

Hasła jednorazowe generowane za pomocą aplikacji uruchomionej na telefonie lub komputerze są dobrym dodatkiem do silnych haseł, ale nie powinny być używane samodzielnie. Hasła jednorazowe oparte na aplikacji są prawdopodobnie bezpieczniejszym sposobem uwierzytelniania niż hasła jednorazowe oparte na wiadomościach SMS (patrz poprzednia sekcja), ale mogą być niewygodne; Jeśli na przykład otrzymasz nowy telefon, może być konieczne ponowne skonfigurowanie informacji we wszystkich witrynach, w których używasz haseł jednorazowych utworzonych przez aplikację generatora uruchomioną na smartfonie. Podobnie jak w przypadku haseł jednorazowych opartych na wiadomościach SMS, jeśli wyślesz wygenerowane przez aplikację jednorazowe hasło do witryny phishingowej przestępcy zamiast do legalnej witryny, przestępca może odtworzyć je na odpowiedniej prawdziwej stronie w czasie rzeczywistym, co zmniejsza korzyści w zakresie bezpieczeństwa hasła jednorazowego w całości.

Uwierzytelnianie za pomocą tokena sprzętowego

Tokeny sprzętowe, które generują nowe hasła jednorazowe co x sekund, są podobne do aplikacji opisanych w poprzedniej sekcji z główną różnicą jest to, że musisz mieć przy sobie specjalistyczne urządzenie, które generuje kody jednorazowe. Niektóre tokeny mogą również działać w innych trybach - na przykład zezwalając na typy uwierzytelniania typu wyzwanie-odpowiedź, w których logowana witryna wyświetla numer wezwania, który użytkownik wprowadza do tokena w celu pobrania odpowiedniego numeru odpowiedzi, który wprowadza użytkownik do witryny w celu uwierzytelnienia.

Chociaż urządzenia z tokenami sprzętowymi są zwykle bezpieczniejsze niż jednorazowe aplikacje generujące, ponieważ te pierwsze nie działają na urządzeniach, które mogą zostać zainfekowane przez złośliwe oprogramowanie lub zdalnie przejęte przez przestępców, mogą być niewygodne. Są również podatne na zgubienie i nie zawsze są wodoodporne - i czasami ulegają zniszczeniu, gdy ludzie robią pranie po pozostawieniu urządzeń w kieszeniach spodni.

Uwierzytelnianie oparte na USB

Urządzenia USB zawierające informacje uwierzytelniające - na przykład certyfikaty cyfrowe - mogą wzmocnić uwierzytelnianie. Należy jednak zachować ostrożność, aby korzystać z takich urządzeń tylko w połączeniu z zaufanymi maszynami - nie chcesz, aby urządzenie zostało zainfekowane lub zniszczone przez jakieś urządzenie i chcesz mieć pewność, że na przykład maszyna otrzymująca certyfikat nie t przesłać go nieuprawnionemu podmiotowi. Wiele nowoczesnych urządzeń USB oferuje różnego rodzaju zabezpieczenia przed takimi atakami. Wiele nowoczesnych urządzeń USB oferuje różnego rodzaju zabezpieczenia przed takimi atakami. Oczywiście urządzenia USB można podłączać tylko do urządzeń i aplikacji obsługujących uwierzytelnianie oparte na USB. Musisz także nosić urządzenie przy sobie i upewnić się, że nie zostanie zgubione ani uszkodzone.