Dziesięć sposobów na poprawę bezpieczeństwa cybernetycznego bez wydawania fortuny

Nie wszystkie ulepszenia bezpieczeństwa wymagają dużych nakładów pieniężnych. W tym rozdziale poznasz dziesięć sposobów na szybkie zwiększenie bezpieczeństwa cybernetycznego bez wydawania dużych pieniędzy.

Zrozum, że jesteś celem

Ludzie, którzy uważają, że hakerzy chcą włamać się do ich komputerów i telefonów, a przestępcy chcą ukraść ich dane, zachowują się inaczej niż ludzie, którzy nie rozumieją prawdziwej natury zagrożenia. Zinternalizowanie dzisiejszej rzeczywistości pomoże wprowadzić do ciebie zdrowy sceptycyzm, a także wpłynie na twoje nastawienie i zachowanie na wiele innych sposobów - z których wiele możesz nawet nie zdawać sobie sprawy, że to wpływa. Na przykład, jeśli uważasz, że jesteś celem cyberataków, jest mniej prawdopodobne, że ślepo ufasz, że wiadomości e-mail, które otrzymujesz z banku, zostały faktycznie wysłane przez bank, a zatem prawdopodobieństwo upadku jest mniejsze. są ofiarami oszustw phishingowych niż ludzie, którzy uważają, że nie są celem. Ludzie, którzy uważają, że przestępcy szukają haseł i numerów PIN, są również bardziej skłonni do lepszej ochrony tych wrażliwych danych niż ludzie, którzy uważają, że oszuści „nie mają powodu, by chcieć" ich danych.

Użyj oprogramowania zabezpieczającego

Wszystkie urządzenia komputerowe (laptopy, telefony, tablety itp.) w domu mają informacje wrażliwe lub które zostaną połączone z innymi sieciami urządzenia wymagają oprogramowania zabezpieczającego. Kilka popularnych, niedrogich pakietów obejmuje program antywirusowy, zaporę ogniową, antyspam i inne przydatne technologie. Urządzenia przenośne powinny mieć możliwość zdalnego czyszczenia i oprogramowanie zoptymalizowane pod kątem systemów mobilnych; pamiętaj, aby włączyć te funkcje, gdy tylko otrzymasz urządzenie. Wiele telefonów ma fabrycznie zainstalowane oprogramowanie zabezpieczające - upewnij się, że je włączyłeś i korzystasz z niego.

Szyfruj poufne informacje

Przechowuj wszystkie poufne dane w zaszyfrowanym formacie. Jeśli masz wątpliwości, czy coś jest wystarczająco czułe, aby zaszyfrować, prawdopodobnie tak jest, więc zachowaj ostrożność i zaszyfruj. Szyfrowanie jest wbudowane w wiele wersji systemu Windows, a także dostępnych jest wiele bezpłatnych narzędzi do szyfrowania. To zdumiewające, jak wiele wrażliwych danych, które zostały naruszone, mogłoby pozostać bezpiecznych, gdyby strony z którego został skradziony, użył bezpłatnych narzędzi szyfrujących. Ponadto nigdy nie przesyłaj poufnych informacji, chyba że są one zaszyfrowane. Nigdy nie wprowadzaj poufnych informacji do żadnej witryny internetowej, jeśli nie korzysta ona z SSL / TLS szyfrowanie, o czym świadczy ładowanie strony za pomocą HTTPS, a nie HTTP, różnicę łatwo zauważyć, patrząc na wiersz adresu URL przeglądarki internetowej. Szyfrowanie obejmuje złożone algorytmy matematyczne, ale nie musisz znać żadnych szczegółów, aby korzystać z szyfrowania i czerpać z niego korzyści. Należy jednak pamiętać, że obecnie używane są dwie główne rodziny algorytmów szyfrowania:

* Symetryczny: używasz tego samego tajnego klucza do szyfrowania i odszyfrowywania.

* Asymetryczny: używasz jednego tajnego klucza do szyfrowania, a drugiego do odszyfrowania

Większość prostych narzędzi do szyfrowania wykorzystuje szyfrowanie symetryczne, a wszystko, co musisz pamiętać, to hasło do odszyfrowania danych. Jednak w trakcie swojej kariery zawodowej możesz napotkać różne asymetryczne systemy, które wymagają ustanowienia zarówno klucza

publicznego, jak i prywatnego. Klucz publiczny jest udostępniany światu, a klucz prywatny jest utrzymywany w tajemnicy. Szyfrowanie asymetryczne pomaga w przesyłaniu danych:

* Jeśli chcesz wysłać informacje do Jana, aby tylko Jan mógł je odczytać, zaszyfruj dane kluczem publicznym Jana, aby tylko Jan mógł je odczytać, ponieważ jest jedyną stroną, która ma prywatny klucz Jana.

* Jeśli chcesz wysłać informacje do Jana i chcesz, aby John wiedział, że je wysłałeś, zaszyfruj dane własnym kluczem prywatnym, a zatem Jan odszyfruje je za pomocą Twojego klucza publicznego i będzie wiedział, że je wysłałeś, ponieważ tylko Ty masz prywatny klucz, który pasuje do Twojego klucza publicznego.

* Jeśli chcesz wysłać informacje do Jana w formacie, który tylko Jan może odczytać, oraz w formacie, który Jan będzie wiedział, że je wysłałeś, zaszyfruj zarówno swoim własnym kluczem prywatnym, jak i publicznymi kluczami Jana.

W rzeczywistości, ponieważ asymetria wymaga dużej mocy obliczeniowej, rzadko jest używana do szyfrowania całych rozmów, ale raczej jest wykorzystywana do szyfrowania specjalnych kluczy sesyjnych, czyli do przekazywania stronom konwersacji kluczy potrzebnych do szyfrowania symetrycznego. Dodatkowe dyskusje dotyczące szyfrowania asymetrycznego wykraczają poza zakres tej książki.

Częsta kopia zapasowa

Twórz kopie zapasowe na tyle często, że jeśli coś pójdzie nie tak, nie będziesz panikować, ile danych utraciłeś, ponieważ ostatnia kopia zapasowa została utworzona kilka dni temu. Oto ogólna zasada: jeśli nie masz pewności, czy tworzysz kopie zapasowe wystarczająco często, prawdopodobnie tak nie jest. Bez względu na to, jak wygodne może się to wydawać, nie trzymaj kopii zapasowych podłączonych do komputera, a nawet do sieci komputerowej (patrz Rozdział 13). Jeśli zachowasz kopie zapasowe dołączone w taki sposób, istnieje poważne ryzyko, że jeśli ransomware lub inne złośliwe oprogramowanie w jakiś sposób zdoła zainfekować twoją sieć, może również uszkodzić kopie zapasowe, co podważyłoby powód tworzenia kopii zapasowych w pierwszej kolejności! Idealnie byłoby, gdyby obie kopie zapasowe były przechowywane zarówno w siedzibie firmy, jak i poza nią. Przechowywanie w siedzibie umożliwia szybkie przywracanie. Przechowywanie poza siedzibą firmy pomaga zapewnić, że kopie zapasowe są dostępne nawet wtedy, gdy witryna stanie się niedostępna lub coś innego zniszczy cały sprzęt komputerowy i dane cyfrowe w określonej witrynie. Jeszcze jedno: upewnij się, że regularnie sprawdzasz, czy Twoje kopie zapasowe faktycznie działają. Tworzenie kopii zapasowych jest bezwartościowe, jeśli faktycznie nie możesz ich przywrócić.

Nie udostępniaj haseł ani innych danych logowania

Każda osoba uzyskująca dostęp do ważnego systemu powinna mieć własne dane logowania. Nie udostępniaj swoim dzieciom ani innym bliskim haseł do bankowości internetowej, poczty e-mail, mediów społecznościowych itp. - zapewnij każdemu własny login. Wdrożenie takiego schematu nie tylko poprawia możliwość wyśledzenia źródła problemów w przypadku ich wystąpienia, ale, co może ważniejsze w przypadku rodzin, stwarza dużo większe poczucie odpowiedzialności i zachęca ludzi do lepszej ochrony swoich haseł.

Użyj właściwego uwierzytelniania

Prawdopodobnie słyszałeś konwencjonalną mądrość dotyczącą używania złożonych haseł do wszystkich systemów, ale nie przesadzaj. Jeśli używanie zbyt wielu złożonych haseł powoduje ponowne

użycie haseł w wielu wrażliwych systemach lub zapisywanie haseł w niezabezpieczonych lokalizacjach, rozważ inne strategie tworzenia haseł, takie jak łączenie słów, liczb i nazw własnych, takich jak custard4tennis6Steinberg. Więcej szczegółów w rozdziale 7. W przypadku wyjątkowo wrażliwych systemów, w przypadku silniejszych form uwierzytelnienia, np. jako uwierzytelnianie wieloskładnikowe są dostępne, skorzystaj z ofert i korzystaj z nich. W przypadku systemów, dla których hasła tak naprawdę nie mają znaczenia, rozważ użycie słabych, łatwych do zapamiętania haseł. Nie marnuj siły roboczej tam, gdzie nie trzeba jej używać. Możesz też użyć menedżera haseł - ale nie w przypadku najbardziej wrażliwych haseł, ponieważ nie chcesz umieszczać wszystkich swoich jajek w jednym koszyku.

Mądrze korzystaj z mediów społecznościowych

Nadmierne udostępnianie postów w mediach społecznościowych powodowało i nadal powoduje wiele problemów, takich jak wyciek poufnych informacji, naruszenie zasad zgodności i pomoc przestępcom w przeprowadzaniu zarówno cyber, jak i fizycznych ataków. Upewnij się, że Twój telefon nie koryguje automatycznie żadnych wrażliwych materiałów podczas publikowania i nie wycinaj i nie wklejaj przypadkowo żadnych wrażliwych treści w oknie mediów społecznościowych.

Oddziel dostęp do Internetu

Prawie wszystkie nowoczesne routery Wi-Fi pozwalają na uruchomienie dwóch lub więcej sieci - skorzystaj z tej funkcji. Jeśli pracujesz na przykład w domu, rozważ podłączenie laptopa do Internetu za pośrednictwem innej sieci Wi-Fi niż ta, której dzieci używają do przeglądania Internetu i grania w gry wideo. Jak omówiono w rozdziale 4, poszukaj funkcji gościa na stronach konfiguracji routera - to tam zazwyczaj znajdziesz możliwość skonfigurowania drugiej sieci (często nazywanej siecią gościa).

Bezpiecznie korzystaj z publicznego Wi-Fi

Chociaż publiczne Wi-Fi to duże udogodnienie, z którego większość ludzi korzysta regularnie, stwarza również poważne zagrożenia dla cyberbezpieczeństwa. Z powodu korzyści, jakie zapewnia publiczne Wi-Fi, jednak praktycy cyberbezpieczeństwa, którzy głoszą, że ludzie powinni powstrzymywać się od korzystania z publicznych sieci Wi-Fi, są mniej więcej tak samo skuteczni w swoich wysiłkach, jak gdyby poinstruowali ludzi, aby porzucili niezabezpieczone komputery i powrócili do używania maszyny do pisania. W związku z tym ważne jest, aby nauczyć się bezpiecznie korzystać z publicznej sieci Wi-Fi i zrozumieć wiele technik zwiększania szans na obronę przed psotami.

Zatrudnij profesjonalistę

Zwłaszcza jeśli zaczynasz lub prowadzisz małą firmę, zasięgnięcie porady eksperta może być mądrą inwestycją. Specjalista ds. Bezpieczeństwa informacji może pomóc w zaprojektowaniu i wdrożeniu podejścia do cyberbezpieczeństwa. Minimalny koszt niewielkiej ilości profesjonalnej pomocy może się zwrócić wielokrotnie w postaci zaoszczędzonego czasu, pieniędzy i problemów. Osoby, które Cię zaatakują - cyberprzestępcy i inni hakerzy - mają wiedzę techniczną i ją wykorzystują. Jeśli zatrudniasz prawnika, jeśli zostałeś oskarżony o popełnienie przestępstwa, idź do lekarza, jeśli poczujesz, że nadchodzi wirus, lub zatrudnij księgowego, jeśli byłeś audytowany przez IRS, zatrudnij cyberprofesjonalistę

Dziesięć sposobów bezpiecznego korzystania z publicznej sieci Wi-Fi

Użyj swojego telefonu komórkowego jako mobilnego punktu dostępowego

Jeśli masz nieograniczony pakiet danych komórkowych, możesz uniknąć ryzyka związanego z publicznym Wi-Fi, przekształcając swój telefon komórkowy w mobilny punkt dostępu i podłączając

laptopa i inne urządzenia, które nie mają komórkowej usługi transmisji danych, do telefonu komórkowego zamiast do publicznej sieci Wi-Fi. Fi.

Wyłącz łączność Wi-Fi, gdy nie korzystasz z Wi-Fi

Wyłączenie łączności Wi-Fi uniemożliwi urządzeniu (bez powiadamiania) łączenie się z siecią o tej samej nazwie, z którą łączyłeś się wcześniej. Przestępcy mogą i mają konfigurować punkty dostępu Wi-Fi o nazwach podobnych do popularnych publicznych sieci Wi-Fi, aby skłonić ludzi do łączenia się z zatrutymi sieciami, które kierują ich ofiary do fałszywych witryn lub rozpowszechniają złośliwe oprogramowanie na podłączonych urządzeniach. Jako dodatkowy bonus, wyłączenie Wi-Fi oszczędza również energię baterii.

Nie wykonuj wrażliwych zadań przez publiczne Wi-Fi

Nie korzystaj z bankowości internetowej, nie rób zakupów online ani nie uzyskuj dostępu do dokumentacji medycznej online podczas korzystania z publicznego połączenia Wi-Fi.

Nie resetuj haseł podczas korzystania z publicznych sieci Wi-Fi

Należy unikać resetowania haseł przez publiczne Wi-Fi. W rzeczywistości nie należy resetować żadnych haseł w miejscu publicznym, niezależnie od tego, czy korzystasz z publicznej sieci Wi-Fi.

Użyj usługi VPN

Jeśli nie możesz korzystać z połączenia komórkowego i musisz korzystać z publicznego połączenia Wi-Fi do wrażliwych zadań pomimo zalecenia, aby tego nie robić, rozważ przynajmniej skorzystanie z usługi VPN, która zapewnia wiele korzyści w zakresie bezpieczeństwa. Obecnie dostępnych jest wiele popularnych usług VPN. Korzystanie z usługi VPN wiąże się jednak z pewnym kompromisem. Możesz zauważyć, że komunikacja jest nieco wolniejsza lub ma większe opóźnienia niż bez uruchomionej sieci VPN.

Użyj Tora

Jeśli nie chcesz, aby ktokolwiek śledził Twoją historię przeglądania, rozważ przeglądanie za pomocą Tora, który odbija Twoją komunikację przez wiele serwerów i sprawia, że śledzenie jest niezwykle trudne. Istnieją nawet przeglądarki Tor dla smartfonów. Podobnie jak VPN, Tor może spowolnić Twoją komunikację.

Użyj szyfrowania

Używaj protokołu HTTPS zamiast HTTP dla wszystkich stron internetowych, które go oferują, aby uniemożliwić innym użytkownikom sieci zobaczenie treści Twojej komunikacji.

Wyłącz udostępnianie

Jeśli używasz komputera lub urządzenia, które udostępnia dowolne z jego zasobów, wyłącz wszelkie udostępnienia przed połączeniem się z publiczną siecią Wi-Fi. Jeśli nie masz pewności, czy Twoje urządzenie udostępnia zasoby, sprawdź to. Nie zakładaj, że tak nie jest.

Mieć oprogramowanie zabezpieczające informacje na wszystkich urządzeniach podłączonych do publicznych sieci Wi-Fi

W przypadku komputerów pakiety bezpieczeństwa muszą zawierać co najmniej funkcje antywirusowe i osobiste zapory ogniowe. W przypadku smartfonów i tabletów użyj aplikacji zaprojektowanej

specjalnie do zabezpieczania takich urządzeń. I oczywiście upewnij się, że oprogramowanie zabezpieczające jest aktualne przed połączeniem się z publiczną siecią Wi-Fi.

Poznaj różnicę między True Public Wi-Fi a Shared Wi-Fi

Nie wszystkie publiczne Wi-Fi są równie ryzykowne. Zwykle istnieje znacznie mniejsze ryzyko przekierowania do fałszywych witryn lub dostarczenia złośliwego oprogramowania do urządzenia, na przykład w przypadku korzystania z chronionej hasłem sieci gościa w siedzibie klienta, niż w przypadku korzystania z niezabezpieczonego bezpłatnego Wi-Fi oferowanego przez Biblioteka Publiczna. Nie oznacza to, że powinieneś w pełni ufać sieci; inni goście na miejscu nadal stanowią zagrożenie.