

Blogowanie anonimowo

Byłeś kiedyś na blogu i miałeś trudności z ustaleniem, kto go pisze? Może to być celowe, zwłaszcza jeśli temat bloga jest drażliwy. Wielu blogerów, którzy chcą być wysłuchani na forum publicznym, woli to robić bez używania swoich prawdziwych nazwisk. Być może myślisz o blogowaniu o polityce, ale zajmujesz stanowisko, w którym Twoje poglądy polityczne nie powinny być powszechnie znane. Być może jesteś osobą, która przeżyła maltretowanie w dzieciństwie, która chce wziąć udział w bieżącej dyskusji i pomóc innym dorosłym, ale bez powszechnej wiedzy o Twojej tożsamości. Możesz pracować dla pracodawcy, który Twoim zdaniem angażuje się w niebezpieczne praktyki biznesowe i czujesz się etycznie zobowiązany do dzielenia się tymi informacjami; zwolnienie oznaczałoby, że nie masz już dostępu do informacji biurowych. A może masz osobisty dziennik, który szczegółowo opisuje twoje zasadniczo przyziemne życie, ale po prostu wolałbyś, aby inni nie wiedzieli, kim jesteś. Wielu blogerów polega na (postrzeganej) anonimowości, aby powstrzymać jeden aspekt swojego życia przed przywiązaniem do innych. Jednak natura Internetu i tożsamości cyfrowej sprawia, że połączenie kropek z jednej usługi internetowej z drugą może być zaskakująco łatwe. Gdy potencjalni pracodawcy, członkowie rodziny, potencjalni partnerzy w związku i inne osoby badają Cię, mogą znaleźć informacje, które chcesz, aby połączyły się z informacjami, które nie są odpowiednie. Wyszukiwanie w Internecie Twojego imienia może spowodować, że Twoje ponadprzeciętne zdjęcia z Instagrama pojawią się na tej samej liście wyników, co Twoje profesjonalne CV. Odpowiedzią wydaje się anonimowość.

Tak duża część naszego życia online jest obecnie połączona z powodu wykupów – takich jak Facebook i Instagram – oraz powszechnych logowań połączonych z mediami społecznościowymi i kontami Google. Jeśli Twoim celem jest anonimowość, upewnij się, że nic powiązanego z Twoim anonimowym blogiem nie jest również powiązane z Twoim mniej niż anonimowym życiem online!

Zanim wejdiesz na ścieżkę anonimowego blogowania, naprawdę warto zadać sobie pytanie, czy warto umieścić coś w Internecie, jeśli sprawiałoby to problem, gdyby było z Tobą powiązane. Jedynym najlepszym sposobem, aby uniemożliwić innym znalezienie informacji, które chcesz zachować w tajemnicy lub informacji, na których nie chcesz umieszczać swojego imienia i nazwiska, jest trzymanie ich poza zasięgiem opinii publicznej. Postawmy sprawę jasno: Internet jest tak publiczny, jak to tylko możliwe.

Potraktuj tę część jako źródło, wskazówkę i punkt wyjścia, a nie przepis na gwarantowaną anonimowość. Technologia i prawo się zmieniają i chociaż to, co tutaj mówię, może pomóc chronić twoją tożsamość, nie powinno to zastępować ciebie prowadzenia własnych badań i podejmowania własnych decyzji o tym, co publikować. Zasadniczo nie gwarantuję, że zastosowanie się do tej rady oznacza, że Twoja tożsamość pozostanie nieznaną. Ponadto nie ma to na celu ochrony przed przytąpaniem na robieniu czegokolwiek nielegalnego. Nie łam żadnych praw.

Decydowanie, ile anonimowości potrzebujesz

Powody decyzji o anonimowym blogowaniu mogą być bardzo różne, podobnie jak potencjalne konsekwencje bycia wykrytym. Oznacza to, że nie każdy bloger potrzebuje takiego samego poziomu ochrony tożsamości. Nastolatek opowiadający historie o nastoletnich wyczynach może nie chcieć zostać zidentyfikowany, ale jeśli tak jest, jest mało prawdopodobne, aby stanął przed ryzykiem postępowania karnego (lub gorzej), jak, powiedzmy, działacz polityczny w kraju, w którym wolność słowa nie jest chroniona. Wiele zmieniło się dla nastolatków żyjących w świecie online od czasu pojawienia się blogów i mediów społecznościowych. Pamiętaj o stanowym ustawodawstwie dotyczącym cyberprzemocy w swoim stanie rodzinnym. Treści postrzegane jako zastraszanie mogą wpędzić autora w prawdziwą gorącą wodę! Zastanów się, jaki poziom ochrony potrzebujesz, a także co może się stać, jeśli Twoja tożsamość zostanie ujawniona. Jeśli wypowiedanie się na swoim blogu

naraża Cię na karę więzienia, krzywdę fizyczną lub ściganie, wyraźnie musisz podjąć najwyższe środki ostrożności podczas konfigurowania i publikowania na swoim blogu. Możesz nawet poważnie przemyśleć dołączenie do świata blogów. Nie musisz blogować anonimowo, ale nie chcesz, aby czytelnicy mieli łatwy dostęp do informacji umożliwiających identyfikację, takich jak adres pocztowy, numer telefonu, a nawet tylko nazwisko? Zarejestruj swoją domenę za pomocą rejestracji prywatnej, aby informacje kontaktowe nie pojawią się w wyszukiwaniu bazy danych własności domeny WHOIS. Za kilka dolarów więcej w momencie zakupu adresu URL możesz również kupić trochę spokoju. Zobacz Część 3, aby uzyskać więcej informacji na temat rejestracji domeny. Ci, którzy zdecydują się na blogowanie na tematy, którym mogą sprzeciwiać się ich pracodawcy, a nawet blogowanie o swoich pracodawcach, również muszą być bardzo ostrożni, chociaż konsekwencje bycia tu zidentyfikowanym prawdopodobnie będą dotyczyć finansów, a nie bezpieczeństwa fizycznego lub karnego. Kolejne pytanie dotyczy tego, czy ktoś będzie dążył do odkrycia Twojej tożsamości. Są też tacy, którzy mogą po prostu woleć oddzielić niektóre aspekty swojego życia od innych. Mama futbolowa może woleć, żeby jej dzieci nie natrafiały na przykład na jej osobiste rozważania na temat seksualności, a raczej, żeby rodzice ich znajomych nie natknęli się na taki blog i połączyli kropki. W tej książce o marce osobistej zobaczysz wiele odniesień. Jeśli planujesz wykorzystać swoją platformę internetową do budowania wiarygodności w określonej dziedzinie, zdobycia okazji do napisania książki lub zamiany treści na gotówkę w jakikolwiek sposób, anonimowe blogowanie utrudni ustalenie Twojej osobistej marki. To powiedziawszy, pamiętaj, że za każdym razem, gdy ujawniasz się jako autor anonimowego bloga, nawet zaufanemu przyjacielowi, otwierasz drzwi nieco szerzej, aby te informacje stały się publiczne. Wielu anonimowych blogerów zostało zdemaskowanych nie w wyniku skomplikowanej technicznej pracy detektywistycznej, ale dlatego, że ktoś zdecydował się ujawnić tajemnicę. Czy planujesz blogować anonimowo, ale nadal wchodzić w interakcje ze społecznością blogerów podczas wydarzeń i konferencji? Utwórz konta w mediach społecznościowych pasujące do Twojego pseudonimu, aby Twoi znajomi blogujący przypadkowo nie oznaczyli Twojego konta osobistego podczas publikowania wspólnych zdjęć. Kiedy myślisz o ryzyku, konsekwencjach i kto może połączyć dwa do dwóch, zatrzymaj się i zastanów się nad innymi, którzy mogą ucierpieć, jeśli twoja tożsamość zostanie ujawniona. Jeśli możesz zostać zidentyfikowany i pisać na blogu o przyjacielach, rodzinie, byłych związkach, pracodawcach i innych osobach w niepoehlebnym sposób lub ujawniłeś poufne informacje na ich temat, stwarzasz możliwość konsekwencji wpływających również na ich życie. Ryzyko, które może być do zaakceptowania dla ciebie, może nie być takie dla innych, szczególnie jeśli nieświadomie naraża się na niebezpieczeństwo. Zalecam przeczytanie całego tego rozdziału przed podjęciem któregośkolwiek z tych kroków, ponieważ przechodzę od niskopoziomowych środków ostrożności; jeśli zdecydujesz, że musisz ustawić się na najwyższym poziomie, najpierw musisz wykonać kilka kroków opisanych później.

Anonimowość

Oczywiście nie powinieneś używać własnego imienia ani zdjęcia na swoim anonimowym blogu. Poza tym istnieją jeszcze inne podstawowe środki ostrożności, które należy podjąć podczas konfigurowania ochrony swojej tożsamości. Większość z nich opiera się na zdrowym rozsądku. Chociaż ten rozdział przedstawia kroki, które należy podjąć, aby blogować anonimowo, nie mogę wystarczająco podkreślić, że nie ma sposobu, aby zagwarantować anonimowość. Jeśli nie chcesz ryzykować odkrycia swojej tożsamości, nie kieruj się anonimowym blogowaniem.

Ustanowienie pseudonimu

To oczywiste, ale i tak to powiem: bez względu na to, kim jesteś, o czym jest Twój blog lub co może się wydarzyć, każdy anonimowy bloger potrzebuje pseudonimu. Pseudonim to fałszywe imię, najlepiej takie, które nie sugeruje sprytnie Twojego prawdziwego imienia ani nie dostarcza żadnych wskazówek, kim naprawdę jesteś. Na przykład „sekretarz generalny” nie jest dobrym pseudonimem dla tego bloga,

który piszesz o tym, jak bardzo twój pracodawca irytuje cię, ale „Fed Up Worker” wystarczy. Jeśli planujesz używać pseudonimu, ale planujesz również zarabiać na swoim blogu, będziesz musiał podać prawdziwe, identyfikujące informacje, aby otrzymać płatność i przesłać formularze podatkowe do dostawcy płatności. Dowiedz się więcej o blogowaniu anonimowo i dla zysku na stronie My Work From Home Money (<https://myworkfromhomemoney.com/anonymous-blogging>). Jeśli utworzyłeś konto w serwisie społecznościowym, a właściwie w jakiegokolwiek witrynie członkowskiej, być może zostałeś poproszony o utworzenie nazwy użytkownika do użycia w tej witrynie. Użycie tego pseudonimu na anonimowym blogu może być kuszące, ale nie rób tego. O wiele lepiej jest wybrać nowy pseudonim, którego nigdy wcześniej nie używałeś.

Konfigurowanie nowego adresu e-mail

Kolejnym krokiem w anonimowości jest utworzenie nowego adresu e-mail przy użyciu swojego pseudonimu. Niezależnie od usługi blogowania, z której zdecydujesz się korzystać, wszystkie wymagają posiadania adresu e-mail, aby rozpocząć, i nie możesz użyć adresu e-mail, który jest powiązany z jakkolwiek z Twoich prawdziwych informacji identyfikujących. Utwórz całkowicie nowe konto e-mail (i nie używaj żadnych informacji identyfikujących w ustawieniach konta). Nie importuj swoich kontaktów. Znajdziesz tam wiele bezpłatnych usług poczty internetowej. Najlepiej wybrać usługę, która oferuje bezpieczne połączenie, taką jak Gmail (www.gmail.com) lub RiseUp (www.riseup.net). Bezpieczne połączenie oznacza, że Twoja wizyta na stronie poczty e-mail nie może być szpiegowana przez technicznych szpiegów. Masz bezpieczne połączenie, jeśli możesz przejść do witryny poczty e-mail poprzedzonej przedrostkiem <https://> zamiast <http://>.

Wybór haseł

Ile razy używałeś tego samego hasła podczas rejestracji w nowej usłudze internetowej? Jeśli jesteś taki jak ja, to kupa! Większość osób, z którymi rozmawiam, przyznaje, że ma jedno lub dwa hasła, których używają na zmianę, jedno, które może być nieco bezpieczniejsze niż drugie, lub takie, którego używają, gdy w grę wchodzi karta kredytowa. Pozwól, że opowiem ci małą historię: Ravelry to bardzo popularna sieć społecznościowa zajmująca się robieniem na drutach (www.ravelry.com). Teraz Ravelry to świetna strona dla tkaczy - nie jest to cel o wysokiej wartości. Witryna nie prosi również o wiele danych osobowych i nie przechowuje danych finansowych ani innych ważnych zapisów. Jednak w czerwcu 2011 r. witryna była celem hakerów, którym udało się włamać na serwer i przechwycić wiele nazw użytkowników i haseł społeczności Ravelry. Chociaż hasła były zaszyfrowane, Ravelry obawiał się, że hakerzy mogą je złamać. Ravelry zalecił, aby wszyscy członkowie Ravelry zmienili swoje hasła na stronie i wzmocnili środki bezpieczeństwa. Ale są większe implikacje dla każdego członka społeczności Ravelry, który mógł użyć tej samej nazwy użytkownika i hasła na innej stronie. Gdyby haker wypróbował te nazwy użytkownika i hasła na innej, bardziej wrażliwej witrynie, takiej jak witryna banku lub witryna do udostępniania zdjęć, niektóre z tych nazw użytkownika i haseł prawdopodobnie zadziałałyby. Krótko mówiąc, wybierz unikalne nazwy użytkownika i hasła dla każdej usługi, którą naprawdę chcesz chronić – na przykład anonimowy blog. Najlepiej byłoby wybrać hasła zawierające różne małe i wielkie litery, a także cyfry i znaki specjalne, takie jak interpunkcja. Nie wybieraj hasła, które zawiera słowo, nawet jeśli zastąpisz niektóre litery znakami lub cyframi, i zdecydowanie nie używaj hasła, które jest imieniem lub datą urodzenia członka rodziny lub zwierzaka. Dobrym pomysłem jest częsta zmiana haseł. Dobrym pomysłem jest również nie zapisywanie haseł ani nie zapisywanie ich nigdzie (zwłaszcza na komputerze). Oczywiście nic z tego nie pomoże, jeśli w rezultacie nie pamiętasz swoich haseł, więc poeksperymentuj z zestawem dobrych praktyk dotyczących haseł, które nadal umożliwiają logowanie się do swoich usług.

Jestem fanem Norton Identity Safe Password Generator (<https://identitysafe.norton.com/password-generator>), który pozwala wygenerować losowy zestaw znaków, aby stworzyć naprawdę silne hasło.

Rozpoczęcie anonimowego bloga

Najbezpieczniejszym sposobem zachowania anonimowości jest wybór hostowanego oprogramowania do blogowania, które nie wymaga posiadania domeny, hostingu ani zakupu licencji. Dwie popularne i sprawdzone w czasie opcje to

»» WordPress.com (www.wordpress.com)

»» Blogger (www.blogger.com)

Witryna WPBeginner zapewnia samouczek specyficzny dla WordPressa dla tych, którzy chcą anonimowo blogować na WordPress: www.wpbeginner.com/wp-tutorials/how-to-blog-anonymously-using-wordpress. Pamiętaj, aby zarejestrować się przy użyciu swojego anonimowego adresu e-mail i pominąć wszelkie informacje identyfikujące w informacjach o koncie, nazwie bloga i tak dalej. Zachowaj ostrożność w przypadku linków wychodzących, które umieszczasz w postach na blogu lub blogach; linkowanie do któregoś ze znajomych lub linkowanie do własnego, nieanonimowego bloga to szybka wycieczka do samego siebie.

Świadomość czasu i lokalizacji

Jednym ze sposobów, w jaki możesz nieumyślnie udzielić wskazówek na temat tego, kim jesteś, jest zasugerowanie, w jakiej strefie czasowej się znajdujesz na podstawie tego, kiedy publikujesz posty na swoim blogu. Zastanów się nad zmianą godzin i dat swoich postów, aby były wyświetlane w czasie, gdy możesz spać lub w inny sposób być zajęty, ale nie posuwaj się tak daleko, aby nigdy nie publikować w czasie, który byłby odpowiedni dla Twojej strefy czasowej. Zmiana godziny i daty również rozwdzi się, gdy jesteś online i publikujesz od momentu opublikowania posta, co nieco utrudnia skorelowanie dostępu do Internetu z konkretną osobą. Może to pomóc, jeśli ktoś próbuje wyśledzić Twoją tożsamość, uzyskując dostęp do plików dziennika, kiedy komputer jest podłączony do Internetu lub gdy uzyskano dostęp do oprogramowania bloga.

Ostrożne podejście do treści

Bardziej prawdopodobne jest, że zostaniesz zidentyfikowany ze względu na to, co piszesz lub publikujesz, niż cokolwiek innego. Zachowaj szczególną ostrożność w odniesieniu do szczegółów, które dostarczają wskazówek dotyczących tego, kim jesteś, gdzie jesteś, co robisz i tak dalej. Bądź bardzo ostrożny w podawaniu konkretów. Oto sześć przykładów:

»» Liczba pracowników w Twoim miejscu pracy

»» Twoja lokalizacja geograficzna

"" Twoja profesja

»» Sklepy, w których często robisz zakupy

»» Imiona, numery, rasy i opisy Twoich pupili

»» Nazwiska przyjaciół i kolegów

Każdy pojedynczy szczegół prawdopodobnie nie wystarczy, aby Cię zidentyfikować, ale łącznie mogą namalować obraz dla doświadczonego czytelnika. Z czasem to staje się coraz większym problemem: im dłużej blogujesz, tym więcej informacji o sobie podajesz. Pamiętaj, że zdjęcia to zapisy z określonego

czasu i miejsca, więc jeśli umieścisz na swoim blogu zdjęcie, które zrobiłeś, mówisz światu, że byłeś w tym miejscu w tym czasie. Dobrym pomysłem jest usunięcie tego zdjęcia z komputera i karty aparatu, a na pewno nie powinieneś publikować go nigdzie indziej w Internecie. Chcesz także usunąć wszelkie metainformacje z samego obrazu. Jeśli chodzi o twój materiał tematyczny, powinieneś szczególnie uważać, aby zrozumieć, czy nie naruszasz jakichkolwiek praw w tym, co mówisz. Dla blogerów głównym problemem jest zniesławienie. Zniesławienie to każde pozornie oparte na faktach stwierdzenie, które jest zarówno fałszywe, jak i szkodliwe dla reputacji danej osoby. Publikowanie szkodliwych informacji o innej osobie jest dobrym sposobem na zainteresowanie jej ustaleniem, kim jesteś, aby mógł cię powstrzymać lub podjąć kroki prawne.

Zwiększenie bezpieczeństwa

Porozmawiajmy teraz o wielkich działach. Masz bloga i naprawdę musisz się upewnić, że nie jesteś zidentyfikowany jako autor. Na początek nie rób niczego, co wiąże się z dokonywaniem płatności kartą kredytową, takich jak rejestracja nazwy domeny, kupowanie licencji na oprogramowanie do blogów lub rejestracja w hostingu. Informacje o Twojej karcie kredytowej nie znajdują się na Twoim blogu, ale transakcja finansowa, która łączy Cię z domeną Twojego anonimowego bloga, to szybka droga do identyfikacji. Wiele innych środków ostrożności wymaga znacznej wiedzy technicznej. Pamiętaj, że podaję ci podstawy i wykorzystaj to jako punkt wyjścia do dalszych badań!

Zrozumienie adresów IP

Podstawowa kwestia techniczna związana z zachowaniem anonimowości w Internecie jest związana z Twoim adresem IP. Jak wspomniano, adres IP lub adres protokołu internetowego to numer identyfikacyjny przypisany do każdego urządzenia, które łączy się z Internetem, od komputera po smartfon. Adres IP jednoznacznie identyfikuje urządzenie i działa jak adres pocztowy, informując inne komputery, jak znaleźć to urządzenie. Za każdym razem, gdy korzystasz z Internetu, zostawiasz historię zawierającą ten adres IP, niezależnie od tego, czy wysyłasz e-maila, czy zamieszczasz komentarz na blogu. Oznacza to, że jeśli założysz anonimowego bloga, a adres IP urządzenia, z którego publikujesz na blogu, może być powiązany z Tobą, blog może być również przypisany do Ciebie. W rzeczywistości niektóre usługi poczty internetowej zawierają nawet adres IP jako część nagłówka wysyłanych wiadomości e-mail. Adres IP może być stały — serwer sieciowy zwykle znajduje się zawsze pod tym samym adresem IP — lub może być dynamiczny, co ma miejsce w przypadku większości domowych komputerów w Internecie. Jeśli uzyskujesz dostęp do Internetu za pośrednictwem dostawcy usług internetowych, czasami adres IP jest przydzielany w momencie faktycznego łączenia się z usługą. Oznacza to, że Twój adres IP się zmienia, ale nadal można go powiązać z dostawcą usług internetowych, a odpowiednia presja prawna może zmusić dostawcę usług internetowych do zrezygnowania z rejestrów, którzy klienci i kiedy używali jakich adresów IP. Chcesz wiedzieć, jaki jest Twój adres IP? Odwiedź www.whatismyip.com, a zobaczysz numer u góry strony. Oczywiście ukrywanie adresu IP jest niezbędne do zapewnienia najwyższego poziomu ochrony tożsamości. Nie jest to prosty proces, ale są na to sposoby. Możesz przyjrzeć się tym opcjom:

»»Anonimizator (www.anonymizer.com)

»»Tor (www.torproject.org)

Bezpieczne korzystanie z oprogramowania

Nawet po wdrożeniu dobrej strategii adresów IP istnieje kilka innych ważnych technicznych sposobów ochrony siebie. Być może nie będziesz musiał wykonywać wszystkich tych czynności, ale pamiętaj, że każdy dodatkowy środek ostrożności zmniejsza twoje szanse na zidentyfikowanie. Oto siedem zaleceń:

»» Korzystaj z aktualnej przeglądarki internetowej, która dobrze radzi sobie z lukami w zabezpieczeniach. Mozilla Firefox to dobry wybór; Internet Explorer nie jest.

»» Uruchom przeglądarkę w trybie prywatności (prywatne przeglądanie w Safari).

»» Zainstaluj i regularnie uruchamiaj oprogramowanie antywirusowe na swoim komputerze.

»» Jeśli piszesz swoje posty na swoim komputerze, usuń je ze swojego komputera i użyj oprogramowania przeznaczonego do trwałego usuwania plików z komputera. Mac ułatwia to - wystarczy wybrać opcję Bezpieczne opróżnianie kosza z menu Findera. Na komputerze sprawdź instalację oprogramowania, takiego jak Ccleaner (www.piriform.com/CCLEANER).

»» Gdy przejdziesz do trybu online, aby publikować na swoim blogu, wyczyść pliki cookie, hasła i historię przeglądarki. Technika wykonania tego będzie się różnić w zależności od używanej przeglądarki, więc zapoznaj się z dostarczoną dokumentacją, aby upewnić się, że wiesz, jak wykonać te zadania. Wyczyszczenie historii oznacza, że komputer jest czysty, jeśli inni go używają lub zostaje utracony. Powinieneś to również zrobić, jeśli korzystasz z komputera publicznego.

»» Zachowaj ostrożność podczas komentowania blogów, korzystania z forów lub rejestrowania się w usługach przy użyciu Twojej anonimowej tożsamości. Wiele z tych usług gromadzi adresy IP, gdy wysyłasz do nich posty lub rejestrujesz się.

»» Publiczne blogowanie to miecz obosieczny. Z jednej strony korzystanie z ogólnodostępnego komputera – w bibliotece czy kafejce internetowej – oznacza zamęt w kwestii tego, kto z tego komputera pisał na bloga. Z drugiej strony, jeśli jesteś publicznie, inni mogą prawdopodobnie zobaczyć Twój ekran, możesz być widoczny i nie wiesz, jakie oprogramowanie może znajdować się na komputerze, którego używasz.

Nadążać

Bądź na bieżąco z problemami technicznymi. Nie zakładaj, że ustawisz rzeczy, które będą Cię chronić na stałe. Internet jest bardzo płynnym miejscem: technologia i narzędzia zmieniają się nieustannie, a posiadanie wszystkich swoich podstaw dzisiaj nie gwarantuje, że jutro będziesz bezpieczny. Na przykład po prostu uaktualnienie przeglądarki do najnowszej wersji ma wpływ na bezpieczeństwo! Dotyczy to również kwestii prawnych związanych z anonimowością. Poznaj przepisy obowiązujące w Twoim kraju lub te, które mają do Ciebie zastosowanie, abyś mógł świadomie określić, jakie prawa naruszasz (jeśli w ogóle) lub jakie mogą być konsekwencje, gdy zostaniesz zidentyfikowany.