

Radosław Sokół



Jak pozostać anonimowym w sieci

**Omijaj natrętów w sieci
— chroń swoje dane osobowe!**

Helion 

Wszelkie prawa zastrzeżone. Nieautoryzowane rozpowszechnianie całości lub fragmentu niniejszej publikacji w jakiegokolwiek postaci jest zabronione. Wykonywanie kopii metodą kserograficzną, fotograficzną, a także kopiowanie książki na nośniku filmowym, magnetycznym lub innym powoduje naruszenie praw autorskich niniejszej publikacji.

Wszystkie znaki występujące w tekście są zastrzeżonymi znakami firmowymi bądź towarowymi ich właścicieli.

Autor oraz Wydawnictwo HELION dołożyli wszelkich starań, by zawarte w tej książce informacje były kompletne i rzetelne. Nie biorą jednak żadnej odpowiedzialności ani za ich wykorzystanie, ani za związane z tym ewentualne naruszenie praw patentowych lub autorskich. Autor oraz Wydawnictwo HELION nie ponoszą również żadnej odpowiedzialności za ewentualne szkody wynikłe z wykorzystania informacji zawartych w książce.

Redaktor prowadzący: Michał Mrowiec

Projekt okładki: Studio Gravite / Olsztyn
Obarek, Pokoński, Pazdrijowski, Zaprucki

Wydawnictwo HELION
ul. Kościuszki 1c, 44-100 GLIWICE
tel. 32 231 22 19, 32 230 98 63
e-mail: helion@helion.pl
WWW: <http://helion.pl> (księgarnia internetowa, katalog książek)

Drogi Czytelniku!

Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres

<http://helion.pl/user/opinie/jakpoz>

Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

ISBN: 978-83-246-9847-9

Copyright © Helion 2015

Printed in Poland.

- [Kup książkę](#)
- [Poleć książkę](#)
- [Oceń książkę](#)

- [Księgarnia internetowa](#)
- [Lubię to! » Nasza społeczność](#)

Spis treści

Rozdział 1. Wstęp	7
Co to znaczy być „anonimowym” w Sieci	8
Jak działa Internet	9
Identyfikowanie użytkowników po adresie	10
Inne sposoby identyfikowania użytkowników	11
Czy można być anonimowym w Sieci	12
Szyfrowanie połączeń sieciowych	12
Korzystanie z serwerów pośredniczących	13
Korzystanie z szyfrowanej sieci anonimizującej	14
Korzystanie z obcych połączeń sieciowych	14
Na jakich etapach można być śledzonym	15
Komputer osobisty	15
Łącze internetowe	16
Infrastruktura internetowa	16
Serwery docelowe	17
Komu zależy na śledzeniu użytkownika	17
Ciekawscy	17
Reklamodawcy	18
Instytucje rządowe	19
Organizacje przestępcze	19
Anonimowość, prywatność, bezpieczeństwo	20
Bezpieczeństwo informatyczne	20
Prywatność	21
Anonimowość	22
Podsumowanie	22
Rozdział 2. Bezpieczeństwo i prywatność	23
Hasła	23
Zapisywanie haseł w systemach informatycznych	24
Łamanie haseł	26
Zdobywanie haseł	29
Bezpieczeństwo hasła	30

Bezpieczny system operacyjny	33
Serwisy społecznościowe	47
Niebezpieczeństwa	47
Czego unikać	48
Konfiguracja: Facebook	50
Konfiguracja: Nk.pl	52
Inne serwisy społecznościowe	54
Ostateczny krok ku pełnej prywatności	54
Wirtualizacja	60
Co daje wirtualizacja	60
Problemy z wirtualizacją	61
Instalacja Oracle VirtualBox	62
Tworzenie maszyny wirtualnej	67
Uruchamianie maszyny wirtualnej	72
Ćwiczenia	74
Podsumowanie	74
Rozdział 3. World Wide Web	77
Jak można śledzić użytkownika WWW	78
Informacje uzyskiwane od przeglądarki WWW	78
Ciasteczka	81
Superciasteczka	82
Bezpieczna przeglądarka WWW	83
Do-Not-Track	84
JavaScript	86
Szyfrowanie transmisji	88
Blokowanie wyskakujących okien	91
Ciasteczka	94
Usuwanie zapisanych danych	99
Moduły dodatkowe	100
Przeglądanie w trybie prywatnym	108
Serwery pośredniczące	109
Identyfikator User-Agent	115
Ćwiczenia	117
Podsumowanie	118
Rozdział 4. Poczta elektroniczna	119
Jak działa poczta elektroniczna	120
Postać wiadomości pocztowej	120
Obieg wiadomości pocztowych	122
Fałszywe wiadomości	128
Spam	131
Dostawcy usługi poczty elektronicznej	134
Szyfrowanie transmisji	135
Prywatność wiadomości	136
Anonimowość	137
Własny serwer poczty elektronicznej	137
Bezpieczna poczta elektroniczna	138
Szyfrowanie komunikacji z serwerem	138
Szyfrowanie treści wiadomości	143
Potwierdzanie autentyczności wiadomości	163
Komunikatory internetowe	164
Ćwiczenia	166
Podsumowanie	167

Rozdział 5. Pełna anonimowość 169

 Połączenia VPN 170

 Usługodawcy 171

 Konfigurowanie połączenia 171

 Nawiązywanie połączenia 173

 Weryfikowanie funkcjonowania połączenia 175

 Dezaktywacja połączenia 175

 Sieć Tor 175

 Instalowanie oprogramowania 176

 Wstępna konfiguracja pakietu 179

 Uruchomienie bezpiecznej przeglądarki 183

 Weryfikowanie funkcjonowania połączenia 184

 SecureDrop 184

 Ćwiczenia 185

 Podsumowanie 185

Dodatek A Wersje systemu Windows 187

Skorowidz 189

Rozdział 2.

Bezpieczeństwo i prywatność

Niezależnie od tego, czy chce się zapewnić sobie pewien poziom prywatności, czy też wędrować po Internecie całkowicie anonimowo, koniecznie należy zadbać o bezpieczeństwo tych podróży. Dopiero bezpieczne środowisko internetowe — takie, w którym konta usług wykorzystywanych przez użytkownika nie są narażone na włamanie i kradzież danych — pozwala zapewnić jakikolwiek poziom prywatności i anonimowości.

W tym rozdziale przedstawione zostaną już bardziej praktyczne zagadnienia związane z dbaniem o bezpieczeństwo komputera i systemu operacyjnego, zabezpieczaniem usług sieciowych oraz rozsądnym i uważnym korzystaniem z zasobów Internetu.

Hasła

Hasła towarzyszą użytkownikom komputerów prawie od samego początku. Gdy tylko pojawiły się dane, do których dostęp nie powinien być powszechny, starano się unieemożliwić ich odczytanie i modyfikowanie przez stosowanie tajnych haseł. Z kolei gdy coraz szersze możliwości komputerów pozwoliły na korzystanie z nich przez więcej niż jednego użytkownika, a nawet kilku użytkowników jednocześnie, pojawiła się konieczność rozróżniania tożsamości użytkownika. W ten sposób powstały konta użytkowników, do których dowiązано stosowane już wcześniej hasła.

Hasło jest jednym z gorszych sposobów utrudnienia nieautoryzowanego dostępu do komputera, konta użytkownika lub zasobu. Przez lata eksperymentowano ze stosowaniem między innymi kluczy kryptograficznych oraz identyfikacji biometrycznej. Ta ostatnia metoda jest dość kontrowersyjna:

- ◆ Techniki rozpoznawania odcisków palców są mało skuteczne w przypadku silnego zabrudzenia, zatłuszczenia lub uszkodzenia opuszków palców (na przykład na skutek oparzenia lub otarcia). Czytniki linii papilarnych są co prawda czasem stosowane jako alternatywne metody uwierzytelniania,

jednak zazwyczaj towarzyszy im bardziej tradycyjne rozwiązanie (na przykład kody cyfrowe lub hasła).

- ◆ Rozpoznawanie głosu z jednej strony może uniemożliwić prawidłową identyfikację użytkownika w przypadku choroby lub niedyspozycji, z drugiej zaś fałszywie zaakceptować dostęp niepowołanych osób o podobnym głosie. Urządzenia rozpoznające głos wymagają ponadto idealnych warunków pracy, bez hałasu tła.
- ◆ Identyfikację twarzy łatwo uniemożliwić diametralną zmianą fryzury, zarostem lub opatrunkiem. Niektóre systemy rozpoznające użytkowników po twarzy można też było śmiesznie łatwo oszukać, umieszczając przed kamerą odpowiednio ucharakteryzowanego manekina lub wręcz... zdjęcie danego użytkownika.
- ◆ Rozpoznawanie tęczy jest podatne na zafałszowania wynikające ze stosowania okularów, soczewek kontaktowych oraz poddawania oka operacjom chirurgicznym.

Nieco lepszym rozwiązaniem są urządzenia, których obecność jest niezbędna do uzyskania dostępu¹. Zawierają one generator kluczy kryptograficznych — jego idealna kopia znajduje się w systemie, do którego dostęp jest chroniony. Wprowadzenie (bezpośrednio lub pośrednio) właściwego w danej chwili klucza jest warunkiem uwierzytelnienia użytkownika. Utrudnia to znacznie włamanie osobom, które nie dysponują tym urządzeniem. Mimo to odkryte niedawno w całej rodzinie tokenów luki bezpieczeństwa umożliwiały włamywaczom przewidywanie sekwencji kluczy kryptograficznych i w efekcie unieruchamiały zabezpieczenia.

Wbrew pozorom zatem hasła, choć słabe pod względem bezpieczeństwa i bardzo podatne na ich utratę lub podsłuchanie, mają swoje zalety. Są tworem abstrakcyjnym, więc osoba pamiętająca hasło może go użyć w dowolnym miejscu i czasie. Nawet jeżeli ktoś nie ma fizycznej możliwości wprowadzenia hasła, może poprosić o to w krytycznej chwili zaufaną osobę. Hasła łatwo też przekazywać, na przykład w przypadku przenoszenia odpowiedzialności za serwery lub usługi sieciowe na inną osobę.

Istotne jest jednak, by tworzone hasła były jak najbardziej bezpieczne i jednocześnie jak najłatwiejsze do zapamiętania. Zapisanie hasła likwiduje bowiem jego podstawową zaletę: obecność wyłącznie w pamięci jednej osoby.

Zapisywanie haseł w systemach informatycznych

Wbrew pozorom bardzo niewiele systemów informatycznych zapisuje hasła wprost, to znaczy w formie czytelnej dla człowieka. Taki sposób zapisywania umożliwiałby wykradanie haseł i ich bezpośrednie odczytywanie. W przypadku usług sieciowych dostępnych dla setek tysięcy użytkowników stanowiłoby to katastrofalne naruszenie ich bezpieczeństwa².

¹ Tak zwane tokeny.

² Nie oznacza to, że takie systemy nie istnieją. W historii bezpieczeństwa sieciowego występowały przypadki wycieku baz danych z hasłami użytkowników zapisanymi czystym tekstem, to znaczy w formie czytelnej bezpośrednio dla człowieka.

Typowo baza danych zawierająca informacje o kontach użytkowników przechowuje tak zwane **skrót** **hasła**³. Skrót jest wartością liczbową o szerokim zakresie⁴, uzyskiwaną za pomocą określonego algorytmu⁵. Cechą funkcji skrótu jest to, że jest nieodwracalna. Z jednej strony nie istnieją dwa różne hasła dające tę samą wartość skrótu⁶, jednak z drugiej nie jest technicznie możliwe odtworzenie hasła na podstawie samego skrótu, poza czasochłonnym zgadywaniem go⁷.

Stosowanie skrótów chroni nie tylko przed wykradzeniem oryginalnej postaci hasła z bazy danych serwisu sieciowego, ale też zapobiega przesyłaniu go przez sieć. Podczas uwierzytelniania się w serwisie, wprowadzone przez użytkownika hasło jest przekształcane na skrót i dopiero w takiej formie przesyłane do serwerów obsługujących usługę. Jeżeli nawet przesyłane informacje zostaną podsłuchane i przechwycone, sam skrót — choć ułatwi nieuprawnione zalogowanie się do serwisu — nie zdradzi postaci hasła.

To samo hasło przekształcone tą samą funkcją skrótu w dwóch różnych serwisach sieciowych skutkowałoby pojawieniem się tego samego skrótu. W takim przypadku wykradnięcie skrótu z jednego serwisu ułatwiałoby włamywaczowi zalogowanie się w drugim serwisie. Z tego powodu skrót wylicza się nie na podstawie samego hasła, lecz hasła połączonego z tak zwaną **solą**⁸, czyli dowolnym fragmentem tekstu charakterystycznym dla danego serwisu. Sól, oprócz uniemożliwienia tak prostego włamania się na konta o tym samym hasle, może utrudniać odgadywanie najprostszych haseł użytkowników.

W Internecie znajduje się wiele serwisów umożliwiających eksperymentowanie z przekształcaniem dowolnych zbiorów lub fragmentów tekstu do postaci skrótów⁹. Na przykład hasło `alamakota123` po przekształceniu na skrót MD5 i SHA-1 przyjmuje następujące postaci:

Hasło:	<code>alamakota1234</code>
MD5:	<code>9ED4ED328CE4568BCB2D5F6F96B177CA</code>
SHA-1:	<code>D954006C1D1F9D4FE74D396426142B673B671B54</code>

³ Ang. *password hash*.

⁴ Od kilkudziesięciu do kilkuset bitów. Na przykład algorytm MD5 generuje skrót o długości 128 b, a SHA-1 — o długości 160 b.

⁵ Dawniej wykorzystywany był algorytm MD5 (ang. *Message Digest, version 5*). Ze względu na znane niedoskonałości tego algorytmu znacząco pogarszające jego bezpieczeństwo, obecnie najczęściej stosowany jest algorytm SHA-1 (ang. *Secure Hash Algorithm, version 1*). Coraz częściej mówi się też o stosowaniu innych algorytmów generowania skrótów haseł, na przykład SHA-2.

⁶ W teorii. W praktyce możliwe jest wygenerowanie tak zwanej **wiadomości kolizyjnej**, to znaczy innego fragmentu tekstu (na przykład hasła), którego skrót jest taki sam jak tekstu oryginalnego. Jedną ze wspomnianych wcześniej niedoskonałości algorytmu MD5 jest właśnie względna łatwość generowania wiadomości kolizyjnych.

⁷ Patrz niżej, podpunkt dotyczący łamania haseł.

⁸ Ang. *salt*.

⁹ Przykładowo: <http://onlinemd5.com/>, jednak Autor nie może gwarantować, że po opublikowaniu książki wspomniana strona będzie nadal funkcjonowała i udostępniała tę funkcjonalność.

Łamanie haseł

W filmach hasła łamie się albo przez zgadywanie (przy czym bohater odgaduje właściwe hasło po kilku próbach), albo za pomocą programu, który przegląda kombinacje znaków, a na ekranie pojawiają się na zielono trafienia układające się w kompletne hasło. W praktyce żadna z tych metod nie ma szans zadziałać. Po pierwsze, hasło albo jest całkowicie poprawne, albo całkowicie niepoprawne i na pewno nie ma możliwości dowiedzenia się, że kilka pierwszych liter zostało już odgadniętych. Po drugie, każdy sensowny system po kilku pierwszych nieudanych próbach uwierzytelnienia się w systemie blokuje konto i powiadamia administratora.

Każda poważna próba łamania haseł odbywa się w trybie offline, to znaczy na podstawie wykradzionej bazy danych kont użytkowników zawierającej skróty haseł¹⁰. W takim przypadku włamywacz nie musi przejmować się mechanizmami monitorującymi błędy uwierzytelnienia ani systemami opóźniającymi kolejne próby załogowania się do serwisu¹¹. Może dokonać tylu prób, ile tylko chce, z maksymalną wydajnością oferowaną przez stosowane komputery¹².

Ogólnie rozpoznaje się trzy podstawowe techniki łamania haseł.

Metoda brutalnej siły

Ta metoda polega na wypróbowywaniu wszystkich kombinacji znaków o coraz to większej długości. Gwarantuje to odgadnięcie hasła, jednak — na szczęście — jest bardzo czasochłonne. Przykładowe czasy odgadnięcia haseł o różnej długości z wykorzystaniem metody brutalnej siły przedstawia tabela 2.1. Należy jednak pamiętać, że czas łamania hasła maleje wraz ze wzrostem mocy obliczeniowej komputerów i z roku na rok ta technika pozwala skutecznie łamać coraz dłuższe hasła.

Szybkość weryfikacji kolejnych kombinacji zależy też od nakładów finansowych poniesionych na łamanie hasła. Można przyjąć, że w przypadku skoordynowanego, dobrze finansowanego projektu tego typu czas łamania hasła skraca się tysiąckrotnie.

W związku z powyższym sensowny poziom bezpieczeństwa w aspekcie możliwości techniki brutalnej siły zapewniają hasła zbudowane co najmniej z małych i wielkich liter, o długości co najmniej 12 znaków. Niestety, łatwe do zapamiętania hasła spełniające te założenia mogą być podatne na atak metodą słownikową.

¹⁰ Niestety, takie bazy danych nagminnie krążą w Internecie. Część z nich jest dostępnych bez problemu w sieciach *peer-to-peer*, inne zaś są udostępniane przez grupy przestępcze za — względnie niewielką w sumie — opłatą.

¹¹ Większość serwisów internetowych celowo opóźnia kolejne próby uwierzytelnienia w przypadku podania błędnego hasła, by utrudnić i spowolnić włamanie.

¹² Masowego łamania haseł dokonuje się często w sposób rozproszony, korzystając albo z setek lub tysięcy komputerów, albo z silnych serwerów wyposażonych w uniwersalne moduły obliczeniowe GPGPU.

Tabela 2.1. Szacunkowe czasy łamania hasel metodą brutalnej siły

Długość hasła:	4	5	6	7	8	9	10
Same cyfry	< 1 s	< 1 s	< 10 s	< 90 s	< 17 min	kilka godzin	kilka dni
Same małe litery ¹³	kilka sekund	kilka minut	godzina	jeden dzień	kilkanaście dni	kilkanaście miesięcy	kilkanaście lat
Małe i wielkie litery	kilka minut	godzina	kilka dni	kilkadziesiąt dni	kilkanaście lat	kilkaset lat	—
Małe i wielkie litery plus cyfry	kilka minut	kilka godzin	kilkanaście dni	kilka miesięcy	kilkaset lat	—	—
Małe i wielkie litery, cyfry i znaki specjalne	kilkanaście minut	kilkanaście godzin	kilkadziesiąt dni	kilkanaście lat	kilkaset lat	—	—

Metoda słownikowa

Ta metoda polega na sprawdzaniu poprawności hasel pobieranych z przygotowanej wcześniej bazy, tak zwanego **słownika**¹⁴. Taki słownik zawiera przede wszystkim wszystkie dotychczas odgadnięte hasła, ponieważ istnieje duże prawdopodobieństwo, że inni użytkownicy zastosowali takie same, łatwe do zapamiętania lub wprowadzenia z klawiatury kombinacje znaków. Ponadto tego typu słowniki często uzupełnia się wyrazami ojczystego języka użytkownika, w szczególności imionami, nazwami miast, a nawet przekleństwami.

Korzystanie ze słownika znacząco zmniejsza nakład pracy potrzebnej do złamania hasła. Na przykład złamanie metodą brutalnej siły hasła o długości 10 znaków, składającego się wyłącznie z małych liter alfabetu łacińskiego, wymaga ponad 100 bilionów kolejno przeprowadzanych prób. W przypadku metody słownikowej hasło to może zostać odgadnięte po kilkudziesięciu tysiącach prób, oczywiście jeśli występowało ono w słowniku.

Tabela 2.2 przedstawia 25 hasel najczęściej stosowanych w 2013 roku. Powstała ona na bazie wykradzionych baz danych użytkowników anglojęzycznych i polskojęzycznych serwisów internetowych. Jak widać, wszystkie zamieszczone w tabeli hasła to albo łatwe do wprowadzenia sekwencje sąsiadujących na klawiaturze znaków, lub proste wyrazy (w szczególności imiona). Można być pewnym, że wszystkie one znajdują się wśród pierwszych pozycji wszystkich słowników hasel stosowanych w czasie włamań. Z tego powodu absolutnie należy unikać stosowania hasel choćby podobnych do wymienionych.

¹³ Lub same wielkie litery.

¹⁴ Ang. *dictionary*.

Tabela 2.2. 25 haseł najczęściej stosowanych w 2013 roku¹⁵

Pozycja	Hasła użytkowników anglojęzycznych	Hasła użytkowników polskojęzycznych
1	123456	123456
2	password	qwerty
3	12345678	12345
4	qwerty	pol ska
5	abc123	zaq12wsx
6	123456789	456
7	111111	111111
8	1234567	dupa
9	iloveyou	aaaaaa
10	adobe123	podrywacz
11	123123	123123
12	admin	legia
13	1234567890	qwerty1
14	letmein	marcin
15	photoshop	1234
16	1234	qazwsx
17	monkey	mateusz
18	shadow	123qwe
19	sunshine	maciek
20	12345	mic hał
21	password1	widzew
22	princess	matrix
23	azerty	hasło
24	trustno1	master
25	000000	misiek

Bardziej rozbudowane pakiety oprogramowania służące do łamania haseł metodą słownikową pozwalają dodatkowo określić reguły modyfikacji zawartości słownika. Włamywacz może ustalić, że niektóre litery mają być zamieniane na konkretne symbole, wielkość znaków ma się zmieniać, a na początku lub końcu hasła mają być dodawane dodatkowe symbole lub cyfry. W ten sposób element słownika katastrofa może pozwolić włamywaczowi pokonać ustawione przez „sprytnego” użytkownika hasło K4t4str0f41: wystarczy, by przewidział reguły zamieniające literę a na cyfrę 4 i literę o na cyfrę 0, zmianę pierwszej litery wyrazu na wielką i dodawanie cyfry 1 na końcu wyrazu. Takie modyfikacje znacząco wydłużają czas łamania hasła, jednak wciąż jest on tysiące razy krótszy niż w przypadku metody brutalnej siły.

¹⁵ Źródła: hasła anglojęzyczne: <http://www.cbsnews.com/news/the-25-most-common-passwords-of-2013/>,
hasła polskojęzyczne: <http://bs.net.pl/artykuly-nie-tylko-dla-informatykw/najpopularniejsze-hasla-polakow>.

Metoda tęczowych tablic

W przypadku haseł przechowywanych w postaci skrótów, które są dostępne bezpośrednio dla włamywacza, skuteczniejsza z punktu widzenia czasu przeszukiwania może być **metoda tęczowych tablic**¹⁶. W dużym skrócie: polega ona na wygenerowaniu tablicy, w której dla każdej możliwej wartości skrótu można znaleźć tekst, który doprowadził do powstania tej wartości.

Ponieważ jednak taka tablica miałaby wielki rozmiar, stosuje się pewną sztuczkę. Definiuje się dowolną funkcję (tak zwaną **funkcję redukującą**), która jest w stanie przekształcić wartość skrótu na nowe hasło¹⁷ i wielokrotnie poddaje kolejne hasła na zmianę operacji wyznaczania wartości skrótu oraz redukowania skrótu. W tablicy wyników (nazywanej właśnie **tęczową tablicą**) zapisuje się źródłowe hasło, ostateczną wartość skrótu oraz liczbę operacji, które doprowadziły do powstania tej wartości.

W czasie łamania hasła skróty poddaje się z kolei kolejnym operacjom redukcji, licząc na to, że w pewnym momencie uzyska się wartość zapamiętaną w tęczowej tablicy. Możliwe jest wtedy łatwe skojarzenie wartości skrótu z hasłem.

Metoda tęczowych tablic działa poprawnie jedynie przy przestrzeganiu dwóch ograniczeń:

- a) Budowa hasła musi być z góry znana. Tęczowa tablica musi być przygotowana dla haseł spełniających konkretne założenia, na przykład: wszystkie hasła o długości do sześciu znaków, zbudowane wyłącznie z małych liter alfabetu łacińskiego.
- b) Wartość skrótu nie może być wygenerowana z uwzględnieniem soli. Jeżeli serwis internetowy zapisuje hasła użytkowników z indywidualną solą, inną dla każdego konta, stosowanie metody tęczowych tablic będzie po prostu nieopłacalne.

Zdobywanie haseł

Nie zawsze hasło musi zostać złamane, by włamywacz mógł skorzystać z obcego konta użytkownika. Istnieją dwie podstawowe techniki pozwalające na uzyskanie hasła obcej osoby, bez konieczności poświęcania na to wielu godzin lub dni.

Metoda psychologiczna

Metoda psychologiczna polega na przekonaniu użytkownika, że powinien przekazać wszystkie swoje dane identyfikacyjne osobie trzeciej. Najczęstszym wytłumaczeniem potrzeby uzyskania czyjegoś hasła są problemy techniczne związane z kontem. Hasło uzyskuje się albo telefonicznie, podając się za pracownika działu obsługi klienta,

¹⁶ Ang. *rainbow tables*.

¹⁷ Nie oznacza to, że tak wygenerowane hasło odpowiada konkretnej wartości skrótu z punktu widzenia algorytmu funkcji skrótu.

działu IT lub działu pomocy technicznej, albo za pośrednictwem poczty elektronicznej lub strony WWW udających oficjalne środki komunikacji danej instytucji. Obecnie tego typu ataki są często przeprowadzane w stosunku do klientów bankowości elektronicznej, a uzasadnieniem potrzeby wprowadzenia hasła na żądanie jest na przykład rzekome zablokowanie konta na skutek wcześniej przeprowadzonych prób włamania.

Najlepszym zabezpieczeniem przed tego typu atakami jest edukacja użytkowników. Jest to szczególnie istotne w przypadku podróbek stron WWW instytucji (na przykład banków), które dla mało doświadczonego użytkownika mogą być trudne lub niemożliwe do odróżnienia od oryginałów. Generalnie jednak poważnym sygnałem ostrzegawczym powinno być samo pytanie o hasło w sytuacji innej niż świadoma próba skorzystania z danej usługi podejmowana przez użytkownika.

Podśluch hasła

Za pomocą narzędzi służących rejestrowaniu naciskanych klawiszy (programy typu *key-logger*) możliwe jest przechwycenie (podśluchanie) hasła wprowadzanego przez użytkownika¹⁸. Podśluchane sekwencje klawiszy są następnie przesyłane przez sieć do włamywacza lub odczytywane przez niego bezpośrednio w późniejszym terminie.

Użytkownik nie jest w żaden sposób powiadamiany o podśluchu, a fakt istnienia programu szpiegującego na komputerze może umknąć uwadze nawet doświadczonych administratorów. Programy tego typu najczęściej też nie są wykrywane przez pakiety antywirusowe, są bowiem pisane na zamówienie i używane na ograniczonej liczbie komputerów.

Najlepszym sposobem zabezpieczenia się przed tego typu atakiem jest stosowanie bezpiecznego środowiska programowego¹⁹. Bezwzględnie należy unikać wprowadzania jakichkolwiek danych wrażliwych (a szczególnie haseł) na komputerach, których bezpieczeństwa nie jesteśmy pewni: komputerach służbowych, należących do znajomych, znajdujących się w miejscach publicznych.

Bezpieczeństwo hasła

Aby zapewnić sensowny poziom bezpieczeństwa hasła, należy:

a) Stosować hasło:

- ◆ dłuższe niż 10 znaków;
- ◆ składające się co najmniej z małych i wielkich liter, a najlepiej również z cyfr i znaków specjalnych;
- ◆ niebędące prostą sekwencją liter leżących blisko siebie na klawiaturze;

¹⁸ I przy okazji wielu innych informacji, które nie są zapisywane lub przesyłane w postaci jawnej.

¹⁹ Techniki umożliwiające zwiększenie poziomu bezpieczeństwa środowiska programowego są opisane w dalszej części tego rozdziału.

- ♦ niebędące wyrazem jakiegokolwiek języka (również z uwzględnieniem prostych, mechanicznych przekształceń wyrazów).
- b) Nigdy nie przekazywać nikomu hasła, nawet w sytuacjach, które wydają nam się uzasadnione.
- c) Nigdy nie narażać hasła na podsłuchanie, czy to za pomocą oprogramowania typu *key-logger*, czy też podczas przesyłania siecią teleinformatyczną.

Tworzenie bezpiecznych haseł

Istnieje wiele technik tworzenia bezpiecznych haseł. Należy przy tym podkreślić, że sformułowanie „bezpieczne hasło” jest nieco mylące, gdyż nie istnieją całkowicie bezpieczne hasła. Opisanie poniżej wybrane techniki pozwalają wymyślić hasła, które są znacznie trudniejsze, jednak nie niemożliwe do złamania.

Technika haseł losowych

Najdoskonalsza z technik, jednak najtrudniejsza w użyciu. Tworzone hasło składa się z całkowicie losowo dobranych liter, cyfr i symboli specjalnych. Najlepiej jest, gdy losowania dokonuje komputer, gdyż ludzie — mimo najlepszych chęci — słabo radzą sobie z generowaniem ciągów losowych i często starają się je przesadnie zróżnicować.

Złamanie hasła losowego jest możliwe przede wszystkim za pomocą metody brutalnej siły. Przy założeniu, że hasło takie będzie miało co najmniej 15 znaków długości, jego odтворzenie — przy obecnym stanie techniki — będzie niemożliwe w skończonym czasie.

Oczywistą wadą haseł losowych jest praktyczny brak możliwości ich zapamiętania. Z kolei zapisanie hasła w wielu przypadkach całkowicie przeczy idei zabezpieczenia dostępu do pewnych zasobów. Ta technika jest jednak stosowana czasem w połączeniu z **bankami haseł** — programami, które przechowują w zaszyfrowanej postaci dane uwierzytelniające w serwisach internetowych i automatycznie wpisują je w odpowiednie pola formularzy logowania się użytkownika. Łączy to wysoki poziom bezpieczeństwa haseł losowych z brakiem konsekwencji wycieku hasła do jednego z używanych serwisów (ponieważ w każdym z nich stosowane jest unikatowe hasło), nie zmniejszając komfortu użytkownika²⁰.

Przykładowe hasło losowe: kD7,aUzgfh2_1+A

Technika pierwszych znaków

Sposobem uzyskania łatwego do zapamiętania, a zarazem względnie losowego ciągu znaków, jest użycie pierwszej litery każdego kolejnego wyrazu długiego zdania lub całego fragmentu tekstu. Na przykład na podstawie fragmentu:

Z matki obcej, krew jego dawne bohaterzy,

A imię jego czterdzieści i cztery.

²⁰ Oczywiście wymaga to stosowania bezpiecznego, wiarygodnego programu banku haseł. Źle zaimplementowany bank haseł sam w sobie może zagrozić bezpieczeństwu, ułatwiając wyciek wszystkich danych uwierzytelniających danego użytkownika.

można utworzyć hasło:

Zmo,kjdb,Aij40i4.

mające długość 17 znaków i zawierające małe i wielkie litery oraz cyfry i znaki specjalne. Takie hasło jest bardzo trudne do złamania, lecz można je zapamiętać.

Można stosować odmiany tej techniki lepiej przystosowane do pamiętanego fragmentu tekstu, używając na przykład dwóch pierwszych znaków każdego wyrazu lub ostatniego znaku każdego wyrazu.

Technika całych zdań

Rozwinięciem poprzedniej techniki jest stosowanie jako hasła całego, łatwego do zapamiętania zdania. Na przykład, poprawnym hasłem będzie SzlaDziweczkaDoLaseczkaDoZielonego. Co prawda zawiera ono tylko małe i wielkie litery alfabetu łacińskiego, jednak jego długość (35 znaków) w zasadzie wyklucza ataki metodą brutalnej siły. To hasło jest też bardzo trudne do złamania metodą słownikową, gdyż zawiera sześć połączonych elementów słownika. Ze względu na długość trudno również oczekiwać, by poddało się ono atakowi metodą tęczyowych tablic.

Ten sposób tworzenia haseł ma jednak dwie podstawowe wady:

- a) Niektóre systemy informatyczne nie dopuszczają bardzo długich haseł²¹. Stosowanie opisanej techniki ma sens jedynie w przypadku, gdy hasło składa się co najmniej z czterech lub pięciu wyrazów i 20 znaków.
- b) Wpisanie tak długiego hasła zajmuje dużo czasu, zmniejszając produktywność i zwiększając prawdopodobieństwo, że ktoś podglądnie hasło w czasie jego wprowadzania.

Bezpieczne stosowanie haseł

Nawet jeżeli hasło jest trudne do złamania, jego stopień skomplikowania staje się bezwartościowy, jeżeli dobrowolnie lub na skutek pomyłki przekazemy je innej osobie. Należy zatem stosować następujące zasady bezpieczeństwa:

- ◆ nie wolno zapisywać haseł w postaci jawnej²²;
- ◆ nie wolno przekazywać haseł nikomu, nawet osobom teoretycznie do tego uprawnionym (dział techniczny, szefostwo²³);

²¹ Niechlubnym przykładem są tutaj niektóre usługi internetowe firmy Microsoft, narzucające limit długości hasła wynoszący 16 znaków.

²² W zasadzie jedynym odstępstwem od reguły niezapisywania haseł jest ich przechowywanie w programach typu bank haseł.

²³ W każdym systemie informatycznym istnieje możliwość utworzenia hierarchii praw dostępu, dającej szefostwu wgląd w używane zasoby bez konieczności znajomości hasła pracownika. Nawet w przypadku kończenia stosunku pracy dział IT ma możliwość skasowania haseł i ustawienia ich od nowa, bez znajomości dotychczasowych. Jedynie w przypadku kont funkcyjnych (a nie indywidualnych) przyjęło się — choć jedynie z wygody — przekazywać hasła administracyjne do urzędzeń i serwerów nowym pracownikom na danym stanowisku.

Skorowidz

A

adres
 IP, 10
 komputera, 11
 niepubliczny, 11
 prywatny, 10
 publiczny stały, 10
 publiczny zmienny, 11
 routera, 11
 MAC, 14
 pocztowy, 127
algorytm
 MD5, 25
 SHA-1, 25
analiza adresu pocztowego, 127
anonimowość, 8, 12, 22, 169
anonimowe
 wiadomości pocztowe, 129, 130
 wysyłanie poczty, 137
atak zero-day, 34
autentyczność
 strony WWW, 90
 wiadomości, 163
automatyczne aktualizacje, 35

B

banki haseł, 31
bezpieczeństwo, 23, 74
 hasła, 30
 informatyczne, 20
 komputera, 16
 poczty elektronicznej, 138
 przeglądarki WWW, 83, 183
 systemu operacyjnego, 33
bezpieczne stosowanie haseł, 32
biblioteka TLS, 89
big data, 18
blokowanie
 ruchu sieciowego, 41
 wyskakujących okienek, 91–94
błąd Heartbleed, 13

C

cechy
 komunikacji internetowej, 165
 poczty elektronicznej, 165
certyfikat
 strony, 90
 unieważniający, 157, 158
ciasteczko, cookie, 81, 94
cyber-bullying, 119
czasy łamania haseł, 27

D

dane
 formularzy, 100
 konta użytkownika, 57
 ochrony przed śledzeniem, 100
 osobowe, 7
 uwierzytelniające, 174
 witryn, 100
darmowe serwery pośredniczące, 113
dezaktywacja połączenia VPN, 175
DNS, Domain Name System, 111, 120
dodatek, 100
Do-Not-Track, 84
dostawa
 bezpośrednia, 124
 typowa, 125
 wieloetapowa, 126
dostawcy usługi poczty elektronicznej, 134
dostęp
 do sieci bezprzewodowych, 14
 przez klienta poczty, 139
dynamiczne tworzenie obrazów, 80
działanie
 Internetu, 9
 poczty elektronicznej, 120
 serwera pośredniczącego, 13, 112
zapyory, 41

E

Enigmail, 150
certyfikat unieważniający, 157
klucze, 156
konfiguracja zaawansowana, 155
odczytywanie zaszyfrowanej wiadomości, 161
wybór kont, 153
wybór trybu pracy, 152, 154
wybór trybu uzupełniania wiadomości, 154
wysyłanie zaszyfrowanej wiadomości, 159
zakończenie konfiguracji, 159
etapy
 przesyłania wiadomości, 136
 śledzenia, 15

F

falszywe wiadomości, 128
firewall, 37
FTP, File Transfer Protocol, 12

G

generator kluczy
 kryptograficznych, 24
GPG, 144

H

hasło, 23, 100
 bezpieczeństwo, 30
 bezpieczne stosowanie, 32
 klucza prywatnego, 156
 łamanie, 26
 zapisywanie, 24
 zdobywanie, 29
historia pobierania, 100

Host Drive, 73
 HTTP, Hypertext Transfer Protocol, 12
 hypervisor, 60

I

identyfikator User-Agent, 115
 identyfikowanie
 przeglądarki, 116
 użytkowników, 10, 11, 80
 IMAP, Internet Message Access Protocol, 12, 123
 importowanie klucza publicznego, 163
 informacje
 identyfikujące stronę, 89
 o adresie sieciowym, 113
 o module dodatkowym, 104
 o przeglądaniu, 99
 o użytkowniku, 47
 od przeglądarki, 78, 80
 przechowywane przez strony, 98
 infrastruktura internetowa, 16
 instalacja
 Enigmail, 150
 GPG, 144–150
 Oracle VirtualBox, 62
 komunikat systemu UAC, 66
 opcje, 64, 65
 pakiety dystrybucyjne, 62
 plansza powitalna, 63
 połączenie sieciowe, 65
 potwierdzenie, 67
 zakończenie, 67
 Tor, 176–179
 instytucja uwierzytelniająca
 certyfikat, 139
 instytucje rządowe, 19
 interfejs sieciowy, 37
 intranet, 10
 IP, Internet Protocol, 10

J

język
 HTML5, 80
 JavaScript, 86

K

kategorie bezpieczeństwa stron, 87
 klient, 78
 klient poczty elektronicznej, 139
 klucz
 prywatny, 143
 publiczny, 143, 163
 klucze kryptograficzne, 24
 komputer osobisty, 15
 komunikacja SecureDrop, 184

komunikat systemu UAC, 66
 komunikatory internetowe, 164
 konfiguracja
 Facebook, 50
 bezpieczeństwa strefy, 88
 interfejsu sieciowego, 38
 konta pocztowego, 134, 141, 142
 maszyny wirtualnej, 72
 modułu Enigmail, 152, 155, 159
 Nk.pl, 52
 połączeń internetowych, 111
 prywatności, 53, 95
 serwera IMAP, 141
 serwera SMTP, 142
 Tor, 179
 instalowania aktualizacji, 36
 połączenia VPN, 171

L

LAN, 10
 likwidacja konta, 54
 lista
 darmowych serwerów
 pośredniczących, 114
 modułów, 105
 ochrony przed śledzeniem, 107
 usług, 44
 luki zero-day, 34

Ł

łamanie haseł, 26
 metoda brutalnej siły, 26
 metoda słownikowa, 27
 metoda tęczyowych tablic, 29
 łącze internetowe, 16

M

maskarada, 10
 maszyna wirtualna, 16, 60, 67
 dysk twardy, 69
 format zapisu, 70
 napęd optyczny, 73
 pamięć operacyjna, 69
 pojemność dysku, 71
 sposób przyrastania zbioru, 70
 uruchamianie, 72
 ustawienia, 72
 mechanizm Do-Not-Track, 84
 metainformacje, 120
 metoda
 brutalnej siły, 26
 psychologiczna, 29
 słownikowa, 27
 tęczyowych tablic, 29
 uwierzytelnienia, 142
 moduł

Enigmail, 150
 zarządzania usługami, 44
 moduły dodatkowe przeglądarki, 100
 Mozilla Thunderbird, 139, 150

N

nagłówek
 Accept-Language, 78
 User-Agent, 79
 narzędzie, *Patrz* program
 NAT, Network Address Translation, 10
 nawiązywanie połączenia
 z Tor, 180
 VPN, 173

O

obce prywatne sieci
 bezprzewodowe, 14
 obieg wiadomości pocztowych, 122
 odbieranie klucza publicznego, 163
 odcięcie od usługi, 37
 odciski palców, 23
 odczytywanie zaszyfrowanej
 wiadomości, 161
 odłączanie usług sieciowych, 37
 ograniczenia łącza sieciowego, 14
 okna wyskakujące, 91–94
 okno
 panelu sterowania, 40
 przeglądarki Tor, 183
 tekstowej konsoli systemu, 127
 trybu prywatnego, 110
 Usługi, 44
 zarządzania dodatkami, 101, 102
 opcje
 internetowe, 97
 konta pocztowego, 133
 prywatności, 92
 organizacje przestępcze, 19
 ostrzeżenie systemu UAC, 145
 otwarty tekst, 135

P

pakiety, 9
 panel
 narzędzi programistycznych, 115
 sterowania, 40
 sterowania oprogramowania, 43
 ustawień emulacji, 115
 parametry serwera
 pośredniczącego, 181
 password hash, 25
 PGP, 144
 pliki cookie, 100, *Patrz także*
 ciasteczko

pobieranie danych konta, 57
poczta elektroniczna, 119
 anonimowość, 137
 bezpieczeństwo, 138
 dostawcy usługi, 134
 dostęp przez WWW, 138
 potwierdzanie autentyczności, 163
 prywatność wiadomości, 136
 przychodząca, 141
 szyfrowanie komunikacji, 138
 szyfrowanie transmisji, 135
 szyfrowanie treści, 143
 własny serwer, 137
 wychodząca, 142
podpis elektroniczny, 154
podsluchiwanie
 hasła, 30
 transmisji sieciowej, 15
pojemność dysku wirtualnego, 71
połączenia
 nieszyfrowane, 140
 VPN, 170, 173
POP3, Post Office Protocol v.3, 12, 123
pop-under, 191
pop-up, 91
port
 110, 140
 143, 140
 993, 140
 995, 140
potwierdzanie autentyczności
 wiadomości, 163
powiadomienie o gromadzeniu
 danych, 56
poziom
 anonimowości, 16
 likwidacji konta, 55
profilowanie oferty reklamowej, 7
program
 GnuPG, 144
 GPG, 144
 Mozilla Thunderbird, 139, 150
 PGP, 12
 VirtualBox, 62
 VMware Workstation, 60
programy typu key-logger, 30
protokoły sieciowe, 12
protokół
 FTP, 12
 HTTP, 12, 81
 HTTPS, 94
 IMAP, 12
 POP3, 12
 SMTP, 12
 SOCKS5, 13
prywatność, 21, 23, 54, 74
prywatność wiadomości, 136
przeglądanie InPrivate, 109
przeglądarka Tor, 183

przeglądarka WWW, 78, 83
 bezpieczeństwo, 83
 blokowanie wyskakujących
 okien, 91–94
 ciasteczka, 94
 Do-Not-Track, 84
 identyfikator User-Agent, 115
 JavaScript, 86
 moduły dodatkowe, 100
 opcje internetowe, 97
 opcje prywatności, 92
 szyfrowanie transmisji, 88
 tryb prywatny, 108
 ustawienia połączeń
 internetowych, 111
 ustawienia prywatności, 95
 usuwanie danych, 99
 usuwanie historii, 99
pule adresów IP, 10
punkty hot-spot, 14

R

reguły tymczasowego
 przechowywania danych, 98
reklama, 77
reklamodawcy, 18
rodzaje ataków, 15
routery, 10
routing cebulowy, 175
rozpoznawanie
 głosu, 24
 odcisków palców, 23
 tęczówki, 24
 twarzy, 24

S

SecureDrop, 184
Sender Policy Framework, 126
serwer, 78
 DNS, 111
 docelowy, 17
 dostępowy VPN, 169
 HTTP, 81
 nadawcy, 125
 odbiorcy, 125
 pośredniczący, proxy, 13, 109, 169
 SMTP, 128
 typu botnet, 41
serwisy społecznościowe, 47
 Facebook, 50
 Google+, 119
 likwidacja konta, 54
 niebezpieczeństwa, 47
 Nk.pl, 52
 wyciek informacji, 48, 54

sieci
 anonimizujące, 14, 170
 bezwzrostowe
 prywatne, 14
 publiczne, 14
 komutowane, 9
 pakietowe, 9
 peer-to-peer, 26
 prywatne, 39
 publiczne, 39
 wewnętrzne, 10
sieć
 LAN, 10
 Tor, 175
skrótów hasel, 25
skrypty JavaScript, 79
skrzynka pocztowa, 125
słownik, dictionary, 27
SMTP, Simple Mail Transfer
 Protocol, 12, 120–123
sól, salt, 25
spam, 131
SSL, Secure Sockets Layer, 89
stalkerzy, 17
stan zapory sieciowej, 39, 40
STARTTLS, 140
superciasteczka, 82
system
 operacyjny
 automatyczne aktualizacje, 35
 bezpieczeństwo, 33
 usuwanie oprogramowania, 42
 wyłączanie usług, 43
 zabezpieczanie połączenia, 37
 pocztowy WWW, 139
 SecureDrop, 185
 Sender Policy Framework, 123
 UAC, 145
szyfrowana sieć anonimizująca, 14
szyfrowanie, 135
 danych, 144
 komunikacji, 138
 połączenia, 12, 139
 transmisji, 88, 135
 wiadomości pocztowych, 143, 150
 złączników, 161

Ś

śledzenie użytkownika
 administratorzy serwera, 17
 analiza ruchu sieciowego, 16
 bezpieczeństwo komputera, 16
 ciekawscy, 17
 instytucje rządowe, 17, 19
 łącznie internetowe, 16
 monitorowanie komputera, 15
 organizacje przestępcze, 17, 19
 reklamodawcy, 18
 WWW, 78

T

technika
 całych zdań, 32
 hasel losowych, 31
 pierwszych znaków, 31
 tęczowa tablica, 29
 tłumaczenie nazwy serwera
 na adres IP, 128
 tokeny, 24
 Tor
 bezpieczna przeglądarka, 183
 cenzurowanie, 182
 instalacja, 176
 nawiązywanie połączenia, 180
 obejście blokady, 182
 SecureDrop, 184
 serwer pośredniczący, 181
 weryfikowanie adresu
 sieciowego, 184
 wstępna konfiguracja, 179
 zaporą sieciową, 181
 trasowanie cebulowe, 175
 tryb prywatny, 108
 tworzenie
 bezpiecznych hasel, 31
 certyfikatu unieważniającego, 159
 maszyny wirtualnej, 67
 pary kluczy, 156
 połączenia VPN, 172
 tymczasowe pliki internetowe, 99

U

uruchamianie
 bezpiecznej przeglądarki, 183
 maszyny wirtualnej, 72
 usługa, 43
 SPF, 138
 WWW, 77
 usługi sieciowe, 37
 ustawienia, *Patrz* konfiguracja
 usuwanie
 danych z przeglądarki, 99
 historii przeglądania, 99
 konta Facebook, 57
 konta Nk.pl, 59
 oprogramowania, 42
 uwierzytelnienie użytkownika, 81

V

VirtualBox, 62
 VirtualBox Host-Only Networking,
 63
 VirtualBox Python 2.x Support, 63
 VirtualBox USB Support, 63
 VPN, Virtual Private Network, 169
 dane uwierzytelniające, 174
 dezaktywacja połączenia, 175
 konfigurowanie połączenia, 171
 nawiązywanie połączenia, 173
 weryfikowanie połączenia, 175

W

wady wirtualizacji, 61
 wdzwanianie, 170
 wersje systemu Windows, 187
 weryfikowanie adresu sieciowego,
 175, 184
 węzły wyjściowe, 176
 whistleblower, 9
 whistleblowing, 119
 wiadomości pocztowe, 121
 anonimowe, 130
 dostawa bezpośrednia, 124
 dostawa typowa, 125
 dostawa wieloetapowa, 126
 fałszywe, 128
 obszar nagłówków, 120
 obszar treści, 121
 protokoły, 122
 pusty wiersz, 121
 spam, 131
 załącznik, 132
 wiadomość kolizyjna, 25
 Windows, 187
 wirtualizacja, 60
 guest, 61
 host, 61
 Oracle VirtualBox, 62
 wady, 61
 zalety, 61
 wirtualny
 dysk twardy, 69
 napęd optyczny, 73
 wirus, 15
 własny serwer poczty elektronicznej,
 137

właściwości usługi, 46
 włączanie
 szyfrowania wiadomości, 160
 trybu prywatnego, 109
 wtyczka, 100
 WWW, World Wide Web, 77
 wybór
 identyfikatora przeglądarki, 116
 przeglądarki internetowej, 16
 systemu operacyjnego, 16
 wyciek informacji, 48, 54
 wyłączenie
 usług, 37, 43–46
 zapory systemu, 41
 wysyłanie zaszyfrowanej
 wiadomości, 159

Z

zabezpieczanie
 połączenia sieciowego, 37
 systemu operacyjnego, 34
 zadania związane z kontem, 59
 zalety wirtualizacji, 61
 załącznik, 132
 załącznik z kluczem publicznym, 163
 zapisywanie hasel, 24
 zaporą sieciową, 37, 39, 40
 zarządzanie
 akceleratorami, 106
 dostawcami wyszukiwania, 105
 listami ochrony przed
 śledzeniem, 107
 modułami, 103
 usługami, 44
 zasady szyfrowania załączników,
 161
 zbędne
 oprogramowanie, 42
 usługi, 43
 zdobywanie hasel, 29

Ż

żądanie serwera HTTP, 81

PROGRAM PARTNERSKI

GRUPY WYDAWNICZEJ HELION



1. ZAREJESTRUJ SIĘ
2. PREZENTUJ KSIĄŻKI
3. ZBIERAJ PROWIZJĘ

Zmień swoją stronę WWW
w działający bankomat!

Dowiedz się więcej i dołącz już dzisiaj!

<http://program-partnerski.helion.pl>

GRUPA WYDAWNICZA

 **Helion SA**

Problem ochrony danych osobowych we współczesnym świecie staje się coraz bardziej palący. Dotyczy to także — a może przede wszystkim — Internetu. Zawodne systemy weryfikacji danych w połączeniu z olbrzymimi możliwościami nielegalnego ich gromadzenia i wykorzystywania sprawiają, że każdy z nas może paść ofiarą cyberprzestępców, a przynajmniej codziennie irytować się z powodu nachalnych spersonalizowanych reklam, zalewu sprofilowanego spamu czy innych sygnałów świadczących o tym, że ktoś zbiera nasze dane i próbuje manipulować nami za ich pomocą.

Jeśli chcesz uwolnić się od oglądania czegoś, co atakuje Cię przy każdym otwarciu przeglądarki internetowej, marzysz o tym, by uniknąć natrętnych e-maili od obcych nadawców, które w dodatku wyglądają jak wiadomości od kumpla, i potrzebujesz odrobiny luzu w wirtualnym świecie — ta książka Ci pomoże. Dowiesz się z niej, jak skonfigurować przeglądarkę, by nie zbierała wiadomości o Tobie, i jak korzystać z zaawansowanych systemów ochrony prywatności, takich jak Tor. Zrozumiesz, jak działają internetowi szpiecy, i nauczysz się ich unikać. Odkryjesz, jak dbać o zawartość swojej poczty i zabezpieczać się przed spamerami. Dla własnego bezpieczeństwa — sprawdź, jak to działa!

- Co to znaczy być anonimowym w sieci?
- Komu może zależeć na śledzeniu użytkownika?
- Techniki zapewnienia bezpieczeństwa wpływającego na anonimowość
- Jak można śledzić i analizować ruch osoby oglądającej strony WWW?
- Co to są ciasteczka i superciasteczka?
- Likwidacja reklam na stronach WWW
- Konfigurowanie przeglądarki WWW pod kątem anonimowości
- Czy można nadać fałszywą wiadomość e-mail?
- Jakie informacje są zawarte w wiadomości e-mail?
- Jak spam pocztowy może naruszać anonimowość i prywatność
- Serwery proxy i VPN: sposób działania, konfiguracja, poziom anonimowości i bezpieczeństwa
- System Tor: sposób działania, sprawdzanie poziomu anonimowości

Zabezpiecz się przed nieproszonymi gośćmi z Internetu!

Helion

25120 numer katalogowy

księgarnia internetowa



<http://helion.pl>

zamówienia telefoniczne



0 801 339900



0 601 339900

Sprawdź najnowsze promocje:

Ⓞ <http://helion.pl/promocje>

Ⓞ Książki najchętniej czytane:

Ⓞ <http://helion.pl/bestsellery>

Zamów informacje o nowościach:

Ⓞ <http://helion.pl/nowosci>

Helion SA
ul. Kościuszki 1c, 44-100 Gliwice
tel.: 32 230 98 63
e-mail: helion@helion.pl
<http://helion.pl>

sięgnij po **WIĘCEJ**



KOD KORZYŚCI

ISBN 978-83-246-9847-9



9 788324 698479

Informatyka w najlepszym wydaniu

cena: 34,90 zł