

Spis treści

Rozdział 1. Wstęp	7
Co to znaczy być „anonymowym” 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