

JAK RABUJĘ BANKI

(i inne podobne miejsca)

FC AKA FREAKYCLOWN

WILEY

Tytuł oryginału: How I Rob Banks: And Other Such Places

Tłumaczenie: Zbigniew Waśko

ISBN: 978-83-289-0677-8

Copyright © 2023 by John Wiley & Sons, Inc.

All Rights Reserved. This translation published under license with the original publisher John Wiley & Sons, Inc.

Translation copyright © 2024 by Helion S.A.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise, without either the prior written permission of the Publisher.

WILEY and the Wiley logo are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates, in the United States and other countries, and may not be used without written permission. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc. is not associated with any product or vendor mentioned in this book.

Wszelkie prawa zastrzeżone. Nieautoryzowane rozpowszechnianie całości lub fragmentu niniejszej publikacji w jakiejkolwiek 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 wydawca 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 wydawca nie ponoszą również żadnej odpowiedzialności za ewentualne szkody wynikłe z wykorzystania informacji zawartych w książce.

Drogi Czytelniku!

Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres

<https://helion.pl/user/opinie/jakrab>

Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Helion S.A.

ul. Kościuszki 1c, 44-100 Gliwice

tel. 32 230 98 63

e-mail: helion@helion.pl

WWW: <https://helion.pl> (księgarnia internetowa, katalog książek)

Printed in Poland.

- Kup książkę
- Poleć książkę
- Oceń książkę

- Księgarnia internetowa
- Lubię to! » Nasza społeczność

Spis treści

O autorze	9
Podziękowania	11
Słowo wstępne	13
Wstęp	15
Rozdział 1. Czym jest socjotechnika?	19
Rozdział 2. 330 kamer	22
Rozdział 3. Drogo nie znaczy bezpiecznie	25
Rozdział 4. Problem z wózkiem	30
Rozdział 5. Najwyższy poziom bezpieczeństwa	34
Rozdział 6. Psychologia schodów	36
Rozdział 7. Sztuczka „na złamaną rękę”	38
Rozdział 8. Klejnoty koronne nie zawsze muszą błyszczeć	41
Rozdział 9. Teraz to jest moje biuro	44
Rozdział 10. Jak długopisem otworzyć każde drzwi?	48
Rozdział 11. Moje pierwsze porwanie	51
Rozdział 12. Potrzebowałem nowego komputera	57
Rozdział 13. Projektowanie własnego biura	60
Rozdział 14. Upoważnienie	64
Rozdział 15. Bystry menedżer	66
Rozdział 16. Nie umiem latać helikopterem	68
Rozdział 17. Doppelganger — sobowtóry istnieją	71

Rozdział 18. Kradzież kluczy	74
Rozdział 19. Niebezpiecznie jest iść samemu. Weź to!	77
Rozdział 20. Sztabka złota	81
Rozdział 21. Pluszowe dywany	86
Rozdział 22. Czyst(sz)y dostęp	89
Rozdział 23. Co my robimy w tych ciemnościach?	91
Rozdział 24. Co wiem o diamentach?	95
Rozdział 25. Jak otworzyć sejf?	98
Rozdział 26. Znaleźć bezpieczne miejsce	106
Rozdział 27. Tego się nie spodziewałem	110
Rozdział 28. Boczne drzwi do strefy chronionej	113
Rozdział 29. Jak wślizgnąć się za kimś przez nieprzezroczyste drzwi?	116
Rozdział 30. Strażnik, który był zbyt uprzejmy	118
Rozdział 31. Spokój pokerzysty	120
Rozdział 32. Co jest w tym pudle?	123
Rozdział 33. Jak ominąć system zabezpieczeń windy?	125
Rozdział 34. Rampa załadunkowa	127
Rozdział 35. Eskorta	130
Rozdział 36. Klatka schodowa	133
Rozdział 37. Omijanie czujników ruchu	135
Rozdział 38. Bankomaty	140
Rozdział 39. Otwarte okna	143
Rozdział 40. Bezpieczeństwo za marne pieniądze	146
Rozdział 41. Jak pokonać kłódkę?	150
Rozdział 42. Bramy zamknięte na kłódkę	153
Rozdział 43. Szklane bezpieczeństwo	157
Rozdział 44. Parkiety giełdowe	161

Rozdział 45. Jak radzić sobie z zamkami klawiszowymi?	164
Rozdział 46. Odpady elektroniczne	168
Rozdział 47. Czternaście komputerów stacjonarnych	171
Rozdział 48. Gadżety szpiegowskie	175
Rozdział 49. Jak zdobyć odciski palców?	178
Rozdział 50. Pięć banków na tydzień	183
Rozdział 51. Gdy dowiesz się zbyt wiele	187
Rozdział 52. Igła w stogu siana	190
Rozdział 53. Kradzież torebki i kluczy	194
Rozdział 54. Otwieranie zamków	197
Rozdział 55. Schowek z pornografią	202
Rozdział 56. Apartament po drugiej stronie ulicy	205
Rozdział 57. Zdjęcie do gazety	209
Rozdział 58. Przemoc rodzi przemoc	212
Rozdział 59. Fałszywy dokument tożsamości	215
Rozdział 60. Udawanie kogoś innego	219
Rozdział 61. Jak działają zamki elektromagnetyczne?	223
Rozdział 62. Eskortą osobistą	226
Rozdział 63. Moje ulubione drzwi	229
Rozdział 64. Bariery mikrofalowe	233
Rozdział 65. Porzucone przepustki	236
Rozdział 66. Przechodzenie przez bramki z kontrolą dostępu	239
Rozdział 67. Wściekły szef ochrony	242
Rozdział 68. Zabawa w lekarzy	245
Rozdział 69. To chodzi o mnie!	250
Rozdział 70. Jak posłużyć się batonikiem?	256
Rozdział 71. Dojeżdżanie autobusem do pracy	258

Rozdział 2.

330 kamer

Poznanie środowiska, które chcemy chronić, ma kluczowe znaczenie. Bez dogłębnego zrozumienia, w jaki sposób zabezpieczenia mają się wpasować w otoczenie, ryzykujemy, że będą nieskuteczne lub, co gorsza, będą działać przeciwko nam.

Poproszono mnie kiedyś o włamanie się do budynku rządowego. Obiekt nie znajdował się w Wielkiej Brytanii, ale ja niestety tak! W związku z tym nie byłem w stanie wykonać żadnych prac rozpoznawczych przed faktycznym włamaniem. Pojawił się jednak promyk nadziei: kolega z pracy był w owym miejscu kilka tygodni wcześniej. Pomimo tego, że nie miał doświadczenia w zakresie zabezpieczeń fizycznych, pomyślałem, że jeśli odpowiednio go podpytam, to może dowiem się czegoś, co pomoże mi się przygotować.

Oto informacje, które mi przekazał:

1. Jest tam mnóstwo drzwi, tak dużo, że nie policzyłem ich dokładnie. Może około 20. Bez strażników. Chyba nie są zamknięte na klucz.
2. Nie zauważyłem żadnych kamer. Może kilka, nie pamiętam.
3. Przy głównym wejściu był ochroniarz, ale samo wejście jest szeroko otwarte. Można wejść, dostać identyfikator i przejść poza barierki.
4. Dostęp jest raczej łatwy; mogłem chodzić, gdziekolwiek chciałem.

Pewnie już się domyślacie, że wszystko w tym raporcie było niezgodne z prawdą. Gdy tylko pojawiłem się na miejscu, sam wybrałem się na rekonesans i co się okazało? Budynek był istną fortecą.

Drzwi było rzeczywiście wiele, ale wszystkie były wyjściami awaryjnymi, których nie można było otworzyć z zewnątrz. Później dowiedziałem się, że w budynku zainstalowano 330 kamer. Główne wejście było strzeżone przez dwóch ochroniarzy uzbrojonych w pistolety. Nikt, kto nie był oczekiwany, nie mógł wejść do budynku; przepustkę na portierni wydawano tylko tym, którzy byli wcześniej umówieni.

Oczywiście mój kolega był oczekiwany i dlatego otrzymał przepustkę; nie był dokładnie obserwowany przez ochronę i tylko błąkał się po budynku. Przegapił również obecność uzbrojonych policjantów, nie zauważył licznych kamer i systemów uniemożliwiających przemieszczanie się między poszczególnymi częściami obiektu, a także nie zwrócił uwagi na wiele innych zabezpieczeń, o których nie wspomnę z oczywistych powodów.

Poczułem się bezradny w obliczu tej pozornie nieprzeniknionej fortecy z większą liczbą kamer, bardziej uzbrojoną ochroną i solidniejszym ogólnym zabezpieczeniem niż w jakimkolwiek obiekcie, który widziałem w całej swojej karierze.

Zrobiłem to, co zrobiłby każdy profesjonalista w mojej sytuacji: spanikowałem, zadzwoniłem do swojego kierownika ds. klientów i powiedziałem, że tego zlecenia nie wykonam.

Rzadko odczuwam tak zwany **syndrom oszusta**, czyli przekonanie, że nie jestem tak dobry, jak uważają inni. Poczułem się jednak trochę oszukany przez kolegę — po uzyskaniu od niego informacji obniżyłem własne standardy co do planowania, które powinienem był przeprowadzić.

Mój kierownik ds. kontaktów z klientami był jednak genialny; powiedział mi, żebym się nie wygłupiał, że nigdy nie widział, abym sobie z czymś nie poradził i że powinienem wziąć to zlecenie. Więc tak zrobiłem.

Następne 48 godzin spędziłem na oglądaniu, pomiarach czasu, planowaniu, szkicowaniu, robieniu notatek i przeglądaniu zasobów internetowych. Trzeciego dnia miałem już jedyny w moim mniemaniu plan infiltracji tego budynku i wywiązania się z zadania.

Wiele godzin później siedziałem z klientem i wyjaśniałem, jak udało mi się dostać do środka i wykonać zleczone zadania. Znajdowaliśmy się w pokoju ochrony, naprzeciwko szeregu monitorów i dużych ekranów. Kilku pracowników ochrony było zajętych sprawdzaniem śladów mojej obecności: udało mi się z łatwością ominąć większość kamer wewnątrz budynku — na nagraniach widać było jakieś dziwne mignięcia, ale nie uznano ich za podejrzane.

Tym, czego nie dało się wyjaśnić na podstawie nagrań, było moje nagłe pojawienie się w budynku. Zjawiłem się w pobliżu rampy załadunkowej i zostałem wpuszczony przez drzwi dla personelu przez uprzejmego przechodnia. Ale to, jak się znalazłem przed tymi drzwiami, pozostawało tajemnicą.

Gdy ochroniarze przewijali zarejestrowane filmy, pomogłem wskazać moment, w którym wszedłem do środka. Po zatrzymaniu nagrania na odpowiedniej klatce w samym rogu ekranu można było dostrzec kawałek buta.

Wyjaśniłem wtedy, że przestudiowałem plany budynku, a także rozmieszczenie i kierunki obserwacji kamer. Jeden punkt przykuł moją uwagę. Stacja załadunkowa, która znajdowała się pod ziemią, miała niezwykle budowę, a jej rampa wspaniale prezentowała się o świcie, oświetlona porannym światłem. Niski kąt padania promieni słonecznych i pozycja kamery oznaczały, że przez kilka minut rano słońce całkowicie ją oślepią. Wszystko, co musiałem zrobić, to zejść po rampie, prześlizgnąć się obok kamery w ciągu tych kilku minut i mieć nadzieję, że ochrona mnie nie zobaczy.

Mój sposób był bardzo sprytny. Uwierzcie mi jednak, że ochroniarze nie bardzo w to wierzyli i sądzili, że w jakiś sposób „oszukałem” kamerę.

Wspomniałem wtedy, że gdybym nie miał za zadanie jedynie przetestować zabezpieczenia, mógłbym skierować laser o dużej mocy w kamerę i całkowicie ją wyeliminować. Miałoby to trwałe skutki dla urządzenia i prawdopodobnie zostałoby zauważone przez pracowników ochrony, ale na pewno byłoby to możliwe.

Co ciekawe, po dotarciu do drzwi wewnętrznych okazało się, że są one zamknięte. Musiałem zapukać w szybę i przekonać kogoś, że zostawiłem przepustkę w środku. W ten sposób zostałem wpuszczony. Ponownie zawiodła kultura bezpieczeństwa, a nie technologia.

Gdy byłem już wewnątrz, podziękowałem uprzejmemu dżentelmanowi, poszedłem w lewo i skręciłem za rogiem. Pierwszymi osobami, na które niemal dosłownie wpadłem, byli dwaj uzbrojeni policjanci. Nie znałem ich języka, co zawsze jest niepokojące, gdy na horyzoncie pojawia się broń, ale od niechcenia skinąłem głową i przeszedłem obok. Nigdy nie wchodźcie w interakcje z ludźmi, jeśli możecie tego uniknąć!

PROGRAM PARTNERSKI

— GRUPY 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
Helion 

Przekonaj się, jak profesjonalista włamuje się do cyfrowej fortecy!

System zabezpieczeń powinien działać dobrze na wielu poziomach. Poza odpowiednio przygotowaną siecią konieczne jest zapewnienie bezpieczeństwa fizycznego. Podobnie jak bezpieczeństwo cyfrowe, tak i to fizyczne powinno być starannie testowane. A najlepszym testem jest... włamanie, w którego efekcie powstanie rzetelny raport pozwalający na wzmocnienie systemu zabezpieczeń. Jednak nawet najlepszy raport nie daje wiedzy, jaką można uzyskać, towarzysząc hakerowi podczas planowania i przeprowadzania włamania.

Dzięki tej świetnie napisanej i miejscami przezabawnej książce dowiesz się, na czym naprawdę polega testowanie granic bezpieczeństwa fizycznego. To fascynująca relacja o sposobach wynajdywania niedoskonałości zabezpieczeń, stosowania socjotechnik i wykorzystywania słabych stron ludzkiej natury. Wyjaśniono tu, jak działają systemy bezpieczeństwa banków i innych tego typu obiektów, zarówno na poziomie cyfrowym, jak i fizycznym, a także jak się wyszukuje podatności takich systemów. Pokazano też wiele narzędzi i technik, które ułatwiają uzyskanie dostępu do najlepiej zabezpieczonych obiektów na świecie. Dzięki tej książce przekonasz się, że przełamanie systemu bezpieczeństwa wymaga ogromnej cierpliwości, kreatywności i podejmowania szybkich decyzji, ale też że czasami można się do niego włamać z przerażającą łatwością.

FC AKA FREAKYCLOWN jest etycznym hakerem, a poza tym autorem książek i współzałożycielem firmy Cygenta. Od trzech dekad pomaga tysiącom banków, rządów i wielu innym instytucjom zwiększyć poziom bezpieczeństwa, włamując się legalnie do przeróżnych organizacji, zarówno fizycznie, jak i cyfrowo.

	KOD KORZYŚCI Sięgnij po więcej! ▶ 
 helion.pl	ISBN 978-83-289-0677-8
 HELION SA ul. Kościuszki 1c 44-100 Gliwice tel.: 32 230 98 63 helion@helion.pl	 9 788328 906778
Cena: 59,00 zł	

WILEY