

Spis treści

Bezpieczeństwo IT. Po co sobie zawracać głowę, przecież wszystko działa — czyli dla kogo jest ta książka	7
Rozdział 1. Hasło to fundament bezpieczeństwa. Oby był solidny	9
1.1. Dlaczego hasła są ważne?	9
1.2. Zarządzaj hasłami za darmo — KeePass	11
Rozdział 2. Uwierzytelnianie dwuskładnikowe. Bezpieczeństwo na wyższym poziomie	23
2.1. Hasła to nie wszystko	23
2.2. Uwierzytelniaj dwuetapowo	24
2.3. Konfiguracja uwierzytelniania dwuskładnikowego — poczta, dyski i inne usługi	26
2.3.1. Aplikacje Google	26
2.3.2. Aplikacje Microsoft	28
2.4. Konfiguracja uwierzytelniania dwuskładnikowego kont w mediach społecznościowych	31
Rozdział 3. Korzystanie z poczty elektronicznej bez niespodzianek, czyli może nie każdy list jest do Ciebie... ..	35
3.1. Firmy kurierskie	36
3.2. Faktury i rachunki od dostawców usług telekomunikacyjnych, energii elektrycznej itp.	38
3.3. Pismo z urzędu	42

Rozdział 4. Chroń swój komputer i surfuj bezpiecznie 49

4.1. Sprawdzaj reputację stron WWW przed ich otwarciem. Pakiety „Internet Security”	49
4.2. Dodatkowa ochrona przeciwko złośliwemu oprogramowaniu	53
4.3. Aktualizacja oprogramowania	56
4.4. Dodatkowe możliwości ochrony komputera	59

Rozdział 5. Przegląd certyfikatów bezpieczeństwa oraz ich weryfikacja 63

5.1. Weryfikuj certyfikaty na stronach WWW	63
5.2. Krótki przegląd certyfikatów SSL	67
5.3. Przygotowanie certyfikatu do instalacji w serwisie WWW	70
5.3. Certyfikaty do podpisu poczty elektronicznej	73

Rozdział 6. Chroń swoje dane, aby uniknąć emocji i... strat finansowych 79

6.1. Kopia zapasowa (backup), archiwum	79
6.2. Ochrona danych na komputerach mobilnych (szyfrowanie)	86
6.3. Ochrona danych poprzez wykonywanie kopii w tle	91

Rozdział 7. Korzystaj z bankowości internetowej i płać bezpiecznie 95

7.1. Bezpieczna bankowość internetowa	95
7.2. Bezpiecznie z kartą bankową	102

Rozdział 8. Smartfon to też komputer. Ochrona urządzeń mobilnych 109

8.1. Program antywirusowy i instalowanie aplikacji	109
8.2. Ataki z wykorzystaniem wiadomości SMS oraz połączeń telefonicznych	113
8.3. Kopie zapasowe. Zabezpieczenie pamięci urządzenia	116
8.4. Bezpieczne korzystanie z internetu	119

Rozdział 9. Bezpieczeństwo poza domem, biurem i na wakacjach 125

9.1. Korzystanie z internetu	125
9.2. niesprawdzone oferty i oszustwa	129
9.3. Chroń swoje dane osobowe	131

Rozdział 10. Zagrożenia w mediach społecznościowych i komunikatorach 135

10.1. Chroń swoje konto i swoją prywatność	135
10.2. Uważaj na oszustów	141
10.3. Komunikator jako źródło szkodliwego oprogramowania	143

Rozdział 11. Dziecko w sieci	147
11.1. Zasady bezpiecznego korzystania z internetu przez dzieci	147
11.2. Kontrola rodzicielska (programy i urządzenia)	152
 Rozdział 12. Firmowy i prywatny serwis WWW	 157
12.1. Aktualizacje serwisu	157
12.2. Zabezpieczanie panelu administracyjnego	158
12.3. Kopie zapasowe strony	160
12.4. Komentarze bez spamu	161
12.5. Przeciwdziałanie atakom na stronę	164
 Zamiast podsumowania. Jak to wszystko opanować, również w świetle RODO?	 169
 Skorowidz	 173