

## SPIS TREŚCI

<b>1</b>	<b>WSTĘP .....</b>	<b>9</b>
1.1	DLA KOGO JEST ADRESOWANA KSIĄŻKA.....	9
1.2	KORZYŚCI Z PRZECYTANIA.....	9
1.3	W JAKIM CELU STOSOWAĆ CYBERBEZPIECZEŃSTWO? .....	9
<b>2</b>	<b>PODSTAWOWE POJĘCIA.....</b>	<b>13</b>
2.1	ADRES FIZYCZNY MAC .....	13
2.2	ADRES IP–NUMER IDENTYFIKACYJNY KOMPUTERA .....	15
2.3	ROUTER .....	20
2.4	SERWER DHCP .....	21
2.5	DNS.....	21
2.6	PROGRAM ANTYWIRUSOWY .....	23
2.7	ZAPORA SIECIOWA - FIREWALL .....	24
2.8	NETYKIETA.....	25
2.9	PRAWA AUTORSKIE.....	26
2.10	KRYPTOWALUTA .....	28
2.11	WIRUS KOMPUTEROWY .....	29
2.12	ROBAK .....	30
2.13	KOŃ TROJAŃSKI .....	31
2.14	SPAM – CZYLI MASOWE KORESPONDENCJE.....	34
2.15	SNIFFING – CZYLI PODSŁUCH ELEKTRONICZNY .....	35
2.16	SPOOFING –NACIĄGANIE, CZYLI PODSZYWANIE SIĘ .....	36
2.17	PHISHING .....	37
2.18	FAŁSZYWA REKLAMA LUB KOMUNIKAT .....	39
2.19	STEALWARE–CZYLI OKRADANIE UŻYTKOWNIKÓW Z PIENIĘDZY.....	41
2.20	CROSS SITE SCRIPTING .....	41
2.21	RANSOMWARE– CZYLI OPROGRAMOWANIE SZANTAŻUJĄCE .....	42
2.22	BOTNET.....	43
2.23	ATAK DDOS.....	45
2.24	ZATRUWANIE DNS.....	46
2.25	GROOMING .....	47
2.26	SEXTING .....	49
2.27	HEJT.....	50
2.28	STALKING – CZYLI NĘKANIE RÓWNIEŻ W INTERNECIE .....	51
2.29	DEEP I DARK WEB .....	52

2.30	INTERNET RZECZY .....	54
<b>3</b>	<b>KTO CHCE NAM ZAGROZIĆ?.....</b>	<b>59</b>
3.1	HACKER, CRACKER I UGRUPOWANIA .....	59
3.2	FIRMA SZUKAJĄCA LUB OFERUJĄCA TANIĄ I NIEUCZCIWĄ REKLAMĘ .....	62
3.3	ZŁODZIEJ, CZYLI FAŁSZYWY PROFIL W INTERNECIE .....	63
3.4	ATAKI UKIERUNKOWANE.....	64
<b>4</b>	<b>BEZPIECZNY SYSTEM OPERACYJNY .....</b>	<b>69</b>
4.1	JA JAKO UŻYTKOWNIK KOMPUTERA .....	69
4.2	PIERWSZE KROKI Z SYSTEMEM .....	70
4.3	KOMPUTER BEZ HASŁA .....	75
4.4	BEZPIECZNE HASŁO .....	77
4.5	BEZPIECZNE KONTO .....	78
4.6	SYSTEM OPERACYJNY I AKTUALIZACJE.....	83
4.7	PROGRAM ANTYWIRUSOWY .....	86
4.8	ZAPORA I OCHRONA SIECI.....	89
4.9	POZOSTAŁE ZABEZPIECZENIA SYSTEMU WINDOWS .....	93
4.10	ALTERNATYWNE SYSTEMY ZABEZPIECZEŃ.....	94
<b>5</b>	<b>BEZPIECZNE POŁĄCZENIE Z SIECIĄ .....</b>	<b>103</b>
5.1	SIEĆ DOMOWA LUB W MAŁYM BIURZE .....	103
5.2	KONFIGURACJA ROUTERA.....	110
5.3	INDYWIDUALNE HASŁO DOSTĘPU .....	114
5.4	SIEĆ BEZPRZEWODOWA WI-FI I JEJ BEZPIECZEŃSTWO .....	117
5.5	FILTROWANIE UŻYTKOWNIKÓW SIECI.....	120
5.6	KONFIGURACJA SIECI DLA GOŚCI. ....	127
5.7	KONFIGURACJA USŁUGI DHCP.....	132
5.8	DOSTĘP DO SIECI W MIEJSCU PUBLICZNYM.....	135
5.9	WIRTUALNA SIEĆ PRYWATNA VPN .....	139
5.10	MÓJ WŁASNY HOTSPOT.....	144
<b>6</b>	<b>PRZEGLĄDARKA INTERNETOWA.....</b>	<b>153</b>
6.1	KORZYSTANIE NA CO DZIEŃ Z PRZEGLĄDARKI INTERNETOWEJ .....	153
6.2	BEZPIECZNE I NIEBEZPIECZNE STRONY .....	156
6.3	SZYFROWANIE A BEZPIECZEŃSTWO.....	165
6.4	GOŚCINNE KORZYSTANIE Z PRZEGLĄDARKI .....	170
6.5	PRZYWRACANIE PRZEGLĄDARKI DO USTAWIEŃ POCZĄTKOWYCH.....	173
6.6	CIEKAWE NARZĘDZIE DO USUWANIA SZKODLIWYCH DODATKÓW I ADWARE. ....	179

<b>7</b>	<b>PRACA W CHMURZE.....</b>	<b>185</b>
7.1	CO TO JEST „CHMURA” .....	185
7.2	CHMURA GOOGLE-A.....	186
7.2.1	<i>Dysk Google.....</i>	<i>188</i>
7.2.2	<i>Bezpieczeństwo chmury Google.....</i>	<i>193</i>
7.3	KONTO MICROSOFT.....	199
7.3.1	<i>OneDrive.....</i>	<i>200</i>
7.3.2	<i>Bezpieczeństwo chmury Microsoft.....</i>	<i>206</i>
<b>8</b>	<b>BEZPIECZNE ZAKUPY W INTERECIE .....</b>	<b>213</b>
8.1	WERYFIKACJA SKLEPU .....	213
8.2	SZYFROWANA TRANSMISJA DANYCH .....	216
8.3	METODY PŁATNOŚCI .....	217
8.3.1	<i>Przesyłka za pobraniem.....</i>	<i>217</i>
8.3.2	<i>Przedpłata przelewem.....</i>	<i>218</i>
8.3.3	<i>Przedpłata na pomoc pośrednika.....</i>	<i>219</i>
8.3.4	<i>Płatności błyskawiczne Blik .....</i>	<i>220</i>
<b>9</b>	<b>DZIECKO W SIECI .....</b>	<b>227</b>
9.1	ZAGROŻENIA DZIECKA W SIECI .....	227
9.2	KONTROLA RODZICIELSKA.....	228
9.3	SYSTEMOWA KONTROLA RODZICIELSKA .....	229
9.4	ANTYWIRUS Z OCHRONĄ RODZICIELSKĄ.....	237
9.5	SPECJALISTYCZNE PROGRAMY OCHRONY RODZICIELSKIEJ .....	239