

Inhaltsverzeichnis

1	Willkommen im Netz	11
1.1	Angriff und Verteidigung	12
1.2	Trau deinen Freunden nur bedingt	12
1.3	Facebook ist nicht gratis.....	13
1.3.1	Was verkauft Facebook an seine Werbekunden?	14
1.4	Gefällt mir – oder doch nicht?.....	16
1.4.1	Ein Klick mit Folgen	16
2	Angriffsvielfalt	19
2.1	Viele Freunde im digitalen Untergrund.....	19
2.2	Die Gefahr der falschen Freunde	21
2.2.1	Freundschaftsanfragen von Unbekannten	22
2.3	Der entführte Gefällt mir-Knopf.....	22
2.3.1	Getarnte Like-Buttons – Clickjacking.....	25
2.4	Die Selbstinfektion	27
2.4.1	Weit verbreitet: Angriffe per JavaScript	27
2.5	Wer war auf meinem Profil?	28
2.5.1	Aufschlussreicher Blick in den Facebook-Hilfereich.....	29
2.5.2	Wer hat mich von seiner Freundesliste verbannt?	32
2.6	Nicht verappln lassen	32
2.7	Befragt, getestet und betrogen.....	34
2.7.1	Wie wird mit den Tests Geld verdient?	36
2.8	Geklaute Log-in-Daten.....	38
3	Facebook wehrt sich	41
3.1	Infos über neue Angriffe und Sicherheitstipps	41
3.1.1	Ein Kampf gegen Windmühlen	42
3.2	Facebook jagt die Hintermänner	43
3.2.1	Vermeintlich leicht erreichbare Ziele – Honeypots.....	44
3.3	Neue Sicherheitsvorkehrungen und neue Angriffe	44
4	Angstware	49
4.1	Scareware-Kampagnen auch in Facebook.....	49
4.1.1	Gewaltige Umsätze	51
4.1.2	Man spricht Deutsch	52
4.2	Die Hintermänner	53
4.2.1	Kleinkriminelle als Handlanger.....	54

4.2.2	Geld zurück – so geht's.....	55
4.3	Bei Anruf Scareware	55
4.4	Ist Scareware legal?	57
4.5	Scareware im Anflug.....	58
4.6	Antivirenprogramme haben es schwer.....	60
4.7	Was tun, wenn der PC infiziert wurde?	61
5	Die Angel ausgeworfen	63
5.1	Vorspiegelung falscher Tatsachen	63
5.2	Facebook als Ziel.....	64
5.3	Facebook als Ausgangspunkt	67
5.3.1	Jede Menge Betrugsmuster	67
5.3.2	Immer wieder gern versucht: der Vorschussbetrug.....	67
5.3.3	Spam-Verbreitung per Nachricht und Pinnwand	68
5.4	Phishing-Nachrichten unter der Lupe.....	69
5.4.1	Erkennungsmerkmale einer Phishing-Mail	73
5.4.2	Hinter die Kulissen der Nachricht geblickt.....	74
5.4.3	E-Mail-Header-Analyse über einen Internetdienst.....	75
5.5	So schützen Sie sich und andere	76
5.5.1	Zweifelhafte Dateianhänge prüfen	77
6	Nächstes Ziel: Handys	79
6.1	Massiver Zuwachs an Schädlingen	79
6.2	Androiden in Gefahr	80
6.3	Trojaner hört auf Kreditkartennummern.....	83
6.4	Auch Rootkits im Angebot	84
6.5	Schadsoftware huckepack.....	85
6.6	Das Handy als Wanze	87
6.7	Wie schützt man sich und sein Smartphone?	88
7	Die Äpfel im Visier.....	91
7.1	Facebook als ein Verbreitungsweg.....	91
7.2	So kommt die Schadsoftware auf den Mac	92
7.3	Administratorrechte? Kein Problem!	94
7.4	Viren selbst gebaut	95
7.5	Gefälschte Schutzsoftware auch für den Mac	96
7.5.1	Durchaus professionell – MAC Defender	97
7.6	Der Mac wird ferngesteuert	99
7.7	Apple schwieg das Problem tot	100
7.8	... und schritt dann doch noch ein.....	102
8	Malware-Schleuder Google.....	107
8.1	Vergiftete Suchmaschinenergebnisse	107
8.1.1	So gehen die Cyber-Kriminellen vor.....	107

8.1.2	Vergiftete Bildsammlungen	111
8.2	Schutz vor dem Gift	112
9	Es geht nur ums Geld	115
9.1	Facebook, ein interessanter Ort	115
9.2	Cyber-Crime-Organisationen setzen auf Arbeitsteilung.....	116
9.2.1	Finder decken Schwachstellen auf	117
9.2.2	Exploiter bereiten den Angriff vor	117
9.2.3	Attacker reiten den Angriff.....	118
9.2.4	Kassierer kontrollieren die Bankkonten.....	119
9.2.5	Lastenmulis verteilen die Geldeingänge.....	119
9.2.6	Spezialisten für die Ideenfindung.....	120
9.3	Die Gefahr kommt von Osten	122
10	Facebook im Unternehmen	125
10.1	Verbannen oder lieben?.....	126
10.2	Ohne Facebook geht es nicht mehr.....	129
10.2.1	Ebenfalls spannend – die Rolle von Twitter	129
10.3	Die Angreifer nehmen, was sie kriegen können.....	129
10.4	Zweiter Sieger: der Virens Scanner	131
10.5	Verbieten oder reinlassen?	132
10.5.1	Geschickter als rigorose Sperren	133
11	Facebook, aber sicher	135
11.1	Grundlegende Facebook-Sicherheitstipps	135
11.2	Infos rund um Facebook-Betrügereien	137
11.3	Wurmkur für die Pinnwand	140
11.4	Sechs Sicherheitstipps auf die Schnelle	143
12	Computer und Daten schützen	145
12.1	Sinnvolle Verwendung von Benutzerkonten.....	145
12.1.1	Standardbenutzer versus Administrator.....	145
12.1.2	Was für ein Typ sind Sie?.....	146
12.1.3	Die Benutzerkontensteuerung	147
12.1.4	Deaktivierte Schutzfunktionen sind keine	149
12.1.5	Benutzerrechte und Kontotypen	149
12.2	Erstellen und Verwenden von Kennwörtern	150
12.3	Sicherer Umgang mit Updates	152
12.3.1	Wer schnell hilft, hilft doppelt	152
12.3.2	Wir lassen für uns arbeiten.....	154
12.3.3	Sämtliche Software aktuell halten.....	156
12.4	Antivirenprogramme: Der beste Schutz ist Aktivität und Aktualität	158
12.4.1	Hinweise zum Kauf, zur Installation und zur Aktualisierung.....	159

12.4.2	Empfehlenswerte Kombinationen	162
12.5	Firewall – die Brandschutzmauer eines Rechners	162
13	Sicherer Umgang mit Internetbrowsern.....	167
13.1	Internetbrowser up to date halten	168
13.1.1	Neue Browser-Versionen suchen und finden	168
13.2	Zeigen Sie bitte Ihren Ausweis	170
13.2.1	Ein amtlicher Ausweis fürs Web	171
13.3	Bunte Adressleisten: Farben für Ihre Sicherheit	172
13.3.1	Weiß: leer wie die nackte Wand	172
13.3.2	Teils weiß, teils blau: nicht zwingend vertrauenswürdig	172
13.3.3	Gelb: Überlegt handeln!	174
13.3.4	Rot: Finger weg!.....	174
13.3.5	Grün: Allseits gute Fahrt!	175
13.4	Filter und Referenzlisten.....	176
13.4.1	Blacklists und Whitelists.....	178
13.4.2	Cross-Site-Scripting-Filter.....	179
13.4.3	Jugendschutz und Kindersicherungen	180
13.5	Private Sitzungen – Anonymität wahren	180
13.5.1	Teil 1: Die interne Anonymität	181
13.5.2	Teil 2: Die externe Anonymität.....	182
	Stichwortverzeichnis	187