

Digitale Sicherheit für Senioren

für Dummies

DAS INHALTS- VERZEICHNIS

» Hier geht's
direkt
zum Buch

Auf einen Blick

Über den Autor	9
Einleitung	21
Teil I: Das Beste zuerst: Ihr Computer ist eine Burg	27
Kapitel 1: Eine unbekannte Welt namens Internet	29
Kapitel 2: Die Einlasskontrolle in die Burg – Router, Firewall und Virenschanner	37
Kapitel 3: Der Burgherr bestimmt die Regeln	45
Teil II: Die Welt vor der Burg und ihre Fallen	57
Kapitel 4: Der Browser – das Internet sichtbar machen	59
Kapitel 5: Suchmaschinen im Internet	77
Kapitel 6: Cookies – harmlos oder gefährlich?	87
Teil III: Die bösen Gegner	95
Kapitel 7: Ihre Rüstung und Ihre Schwachpunkte	97
Kapitel 8: Die bösen Ritter	119
Kapitel 9: Wo ist der blöde Zettel mit dem Passwort?	139
Teil IV: Die Schmuggelwege der bösen Ritter	147
Kapitel 10: Die E-Mail, der digitale Briefkasten	149
Kapitel 11: Online-Shopping – Einkaufen im Internet	163
Kapitel 12: eBay – der digitale Flohmarkt	177
Kapitel 13: Online-Banking	187
Kapitel 14: Bezahlen im Internet	201
Kapitel 15: Digitale Produkte – was man nicht im Laden kaufen kann	215
Kapitel 16: Die »künstliche Intelligenz«	227
Kapitel 17: Soziale Medien – Die Plauderecke in der Burg	237
Kapitel 18: Einfallstor USB-Stick	249
Teil V: Der Top-Ten-Teil	259
Kapitel 19: Die zehn besten Websites für Senioren	261
Kapitel 20: Zehn Tipps für mehr Komfort bei körperlichen Einschränkungen	267
Abbildungsverzeichnis	271
Stichwortverzeichnis	281

Inhaltsverzeichnis

Über den Autor	9
Einleitung	21
Über dieses Buch	22
Was Sie nicht lesen müssen	22
Törichte Annahmen über die Leser	22
Wie dieses Buch aufgebaut ist	23
Konventionen in diesem Buch	25
Symbole, die in diesem Buch verwendet werden	25
Wie es weitergeht	26
TEIL I	
DAS BESTE ZUERST: IHR COMPUTER IST EINE BURG	27
Kapitel 1	
Eine unbekannte Welt namens Internet	29
Die Angst vor etwas Neuem	30
Das Internet – ein schwarzer Himmel voller Plakate	32
Den Nutzen erkennen und die Hemmschwelle überwinden	34
Ihr Computer ist eine Burg	36
Kapitel 2	
Die Einlasskontrolle in die Burg – Router, Firewall und Virenschanner	37
Anweisungen für den Router	40
Eine weitere Sicherheitsschleuse – die Firewall	40
Die letzte Sicherheitsschleuse – der Virenschanner	42
Ein guter Virenschanner ist schon in der Burg	42
Bei Alarm ab in die Quarantäne	43
Betrügerische Falschmeldung	44
Kapitel 3	
Der Burgherr bestimmt die Regeln	45
Der Burgherr besitzt alle Rechte	45
Keine Rechte für das Fußvolk	45
Zugriffsrechte für Programme	46
Zugriffsrechte für Webcams	49
Benutzerkonten für verschiedene Benutzer	51
Benutzerwechsel im laufenden Betrieb	54

TEIL II

DIE WELT VOR DER BURG UND IHRE FALLEN 57

Kapitel 4

Der Browser – das Internet sichtbar machen 59

Die Qual der Wahl – verschiedene Browser	60
Microsoft Edge	61
Google Chrome	62
Mozilla Firefox.....	62
Opera.....	63
DuckDuckGo	64
Brave, ein heimlicher Testsieger	64
Der persönliche Fingerabdruck	65
Der private Modus	67
Der Tor-Browser, ein ganz spezielles Pferd	69
Öffentliches WLAN	70
Gefahr rechtzeitig erkennen.....	71
Tipp 1: Statusleiste im Browser im Blick behalten	71
Tipp 2: Auf Verschlüsselung der Übertragung achten	72
Tipp 3: Verdächtige Internetadresse googeln	73
Tipp 4: VirusTotal	75

Kapitel 5

Suchmaschinen im Internet..... 77

Auch Suchmaschinen surfen.....	77
Neugierig war des Schneiders Weib	78
Browser oder Suchmaschine, wer speichert mehr?	79
Wer die Wahl hat, hat die Qual.....	80
Welche Suchmaschinen sind empfehlenswert?	80
MetaGer.....	81
Wenn Sie sich entschieden haben.....	81
Bildersuche – was ist zu beachten?	83
Geschicktes Tab-Management	84

Kapitel 6

Cookies – harmlos oder gefährlich? 87

Cookies verstehen – ein Einkaufsbummel mit stiller Begleitung.....	88
Gesammelte Informationen für Werbung und Statistik.....	90
Welche Daten werden durch Cookies gesammelt?.....	91
Die nervigen Cookie-Hinweise – welche Auswahlmöglichkeiten gibt es?	91
Wie gehen Sie nun am besten mit Cookies um?	93

TEIL III	
DIE BÖSEN GEGNER	95
Kapitel 7	
Ihre Rüstung und Ihre Schwachpunkte	97
Die »guten« Datensammler.....	98
Datenschutz	98
Der gläserne Internetbesucher	100
Geheimhalten durch Verschlüsselung	100
Das SSL/TLS-Zertifikat	102
Was können Sie tun, wenn es zu einer Datenpanne kommt?.....	104
Die heimlichen Helfer der bösen Ritter	105
Angriffspunkte der bösen Ritter	110
Angebot von Geld, Gewinn und Reichtum	110
Angebot von Bequemlichkeit und Komfort	111
Angebot von Zuneigung und Partnerschaft.....	111
Gefälschte E-Mails, Webseiten oder Nachrichten	111
Das Spiel mit Angst und Zeitdruck.....	112
Neugier wecken	113
Das Spiel mit Ihrer Scham.....	113
Bitte um Fernzugriff.....	115
Im Namen von Microsoft	115
Nichts überstürzen – lassen Sie sich Zeit	118
Kapitel 8	
Die bösen Ritter	119
Mit List und Tücke statt mit Gewalt	120
Der persönliche Weg in Ihre Burg	121
Der Angriff durch programmierte Werkzeuge – Viren, Würmer und Trojaner	122
Virens Scanner – die Antwort der guten Ritter	126
Die verschiedenen Methoden der bösen Ritter.....	127
Phishing	127
Identitätsdiebstahl.....	129
Gefälschte Zahlungsaufforderung.....	129
Quishing	131
Ransomware – Erpressung durch verschlüsselte Daten	133
Gefälschte Paketverfolgung	134
Keylogger.....	135
Man-in-the-Middle-Angriff	135
Und immer wieder: Schwachstelle Mensch	137

Kapitel 9

Wo ist der blöde Zettel mit dem Passwort?..... 139

Welche Programme und Anwendungen benötigen ein Passwort?.....	142
Was macht ein gutes Passwort aus?	142
Wie leicht ist ein Passwort zu knacken?.....	143
So erstellen Sie ein Passwort mit System	144
Ein digitaler Schlüsselbund	144
Der Passwortmanager	146

TEIL IV

DIE SCHMUGGELWEGE DER BÖSEN RITTER 147

Kapitel 10

Die E-Mail, der digitale Briefkasten..... 149

Wie funktioniert eine E-Mail	150
Wo steht Ihr Briefkasten für E-Mails?	150
E-Mail-Postfach einrichten	151
Macht ein Pseudonym Sinn?.....	153
Wie werden E-Mails übertragen?.....	154
E-Mails abholen	154
Wenn das Postfach überläuft.....	155
Werbefinanziert oder kostenpflichtig	156
Was Sie aus Sicherheitsgründen beachten sollten	157
Wichtige Einstellungen in Ihrem E-Mail-Programm	157
Unbekannte Absender	158
Anhänge prüfen	159
Der Spamordner.....	160
Fake-Mails	161

Kapitel 11

Online-Shopping – Einkaufen im Internet 163

Aller Anfang ist gar nicht so schwer: Die Produkt- und Händlersuche	164
Wie erkennt man schwarze Schafe?.....	165
Die AGB – Lesen nötig?	166
Der Kauf kann beginnen	166
Vorab ein Wort zum Rückgaberecht	167
Ihr Warenkorb.....	167
Was passiert mit den anderen Warenkörben?.....	168
Auf dem Weg zur digitalen Kasse.....	169
Wie wird bezahlt?	170

Wenn der Paketbote klingelt.	172
Rückerstattung oder Umtausch	173
Wer trägt die Rücksendekosten?	174

Kapitel 12

eBay – der digitale Flohmarkt. 177

Wie läuft das ab bei eBay?.....	178
Sicher verkaufen	179
Sicher kaufen.	182
Welche Fallen können böse Ritter dem Käufer stellen?	183
Widerruf, Gewährleistung und Rücknahme ausgeschlossen	183
Betrügerische Zahlungsaufforderung.	184
Nicht versandte Ware	184
Datenklau	185
Identitätsdiebstahl	185

Kapitel 13

Online-Banking 187

Wie funktioniert Online-Banking?.....	188
Doppelte Sicherheit durch Zwei-Faktor-Authentifizierung.....	190
Online-Banking – schnell und unkompliziert	192
Jede Transaktion mit einer Transaktionsnummer freigeben	193
Kostet das was?.....	195
Mögliche Nachteile	195
Sicherheitsstandards beim Online-Banking	195
Ihr Beitrag zur Sicherheit.	196
Achten Sie auf den Unterschied: Banken senden keine Links!	198

Kapitel 14

Bezahlen im Internet 201

Kreditkarten.....	203
Klarna	204
Apple Pay	205
Google Pay.....	206
Amazon Pay.....	207
Skrill und Neteller	207
Paysafe	208
PayPal	209
Seien Sie wachsam!	210

Kapitel 15	
Digitale Produkte – was man nicht im Laden kaufen kann	215
Apps – Kleine Programme für tausendundeinen Anwendungsfall	215
Wo kommen diese Apps her?	217
Was muss ich beim Download einer App beachten?	218
Was ist ein In-App-Kauf?	219
Was ist bei In-App-Käufen zu beachten?	220
Wichtiger Hinweis.	221
Andere digitale Produkte, die Sie per Download beziehen können	221
Lästige und gefährliche Gratis-Downloads	222
Toolbars – Hier gibt’s keine Kaltgetränke!	224
Kapitel 16	
Die »künstliche Intelligenz«	227
Kann Denken künstlich sein?	227
Wie kann man KI beschreiben?	228
Chatbots sprechen »KI«	228
In vielen Bereichen wird KI eingesetzt	229
KI und das Thema Sicherheit	230
Wichtig bei Anfragen an die KI	231
Umgang mit den Antworten der KI	232
Ein kleiner Überblick über KI-Tools	233
Kapitel 17	
Soziale Medien – Die Plauderecke in der Burg	237
Was sind soziale Medien?	238
Welche sozialen Medien gibt es?	239
Gibt es spezielle Plauderecken für Senioren?	241
Partnersuche im Internet	242
Böse Ritter in der Plauderecke	242
Auch böse Ritter sind auf Partnersuche	243
Thema Mobbing	244
Was können Sie tun bei Mobbing in sozialen Netzwerken?	245
Und was können Sie im Vorfeld tun, um Mobbing zu vermeiden?	246
Was können Sie für Ihre Sicherheit tun?	246

Kapitel 18

Einfallstor USB-Stick **249**

- Einsatzmöglichkeiten eines USB-Sticks 250
- Der USB-Stick, einfach, aber tückisch! 251
- Vorsicht Falle! 252
- Datenverlust vermeiden beim Abziehen des Sticks 254
- Dateitypen richtig erkennen 255

TEIL V

DER TOP-TEN-TEIL **259**

Kapitel 19

Die zehn besten Websites für Senioren **261**

- BAGSO 261
- Deutschland sicher im Netz 262
- Internet-ABC 262
- Digital-Kompass 262
- Senioren und Technik 263
- Jonah Hadt 263
- Silver Tipps 263
- Helga Hilft! 264
- Levato 264
- Landesanstalt für Kommunikation Baden-Württemberg 265

Kapitel 20

Zehn Tipps für mehr Komfort bei körperlichen Einschränkungen **267**

- Helligkeit und Kontrast 268
- Farbfilter 268
- Schriftgröße und Schriftarten 268
- Lupe als Vergrößerungsfunktion 268
- Sprachsteuerung 268
- Bildschirmleseprogramm 268
- Bildschirm-Tastatur über die Maus 269
- Maussteuerung 269
- Videostart nur manuell 269
- Untertitel bei Videos 269

Abbildungsverzeichnis **271**

Stichwortverzeichnis **281**