

Auf einen Blick

Über die Autoren	7
Vorworte	17
Einleitung	19
Kapitel 1: Basiswissen und Softskills	23
Kapitel 2: Struktur und Organisation	27
Kapitel 3: Software	37
Kapitel 4: Account-Pflege	55
Kapitel 5: Endgeräte absichern	85
Kapitel 6: Sichere Online-Anbieter finden und prüfen	117
Kapitel 7: Spam- und Phishing-Mails erkennen	137
Kapitel 8: Häufig gestellte Fragen	147
Kapitel 9: Zehn typische Betrugsmaschen im Internet	157
Kapitel 10: Die zehn besten Tipps für das sichere Surfen im Internet ...	167
Stichwortverzeichnis	173



Inhaltsverzeichnis

Über die Autoren	7
Vorworte	17
Einleitung	19
Über dieses Buch	20
Törichte Annahmen über den Leser	20
Konventionen in diesem Buch	20
Symbole, die in diesem Buch verwendet werden	21
Kapitel 1	
Basiswissen und Softskills	23
Digitale Sicherheit bei digitalen Gefahren	23
Schaffen Sie Risikobewusstsein	24
Der souveräne Umgang mit Geräten, Apps und Cloud	25
Kapitel 2	
Struktur und Organisation	27
Die Ordnung in Jahren – Eine gewohnte Routine!	27
Von Anfang an an die Account-Hygiene denken	29
Webseiten in Kategorien einteilen und individuelle E-Mail-Adressen verwenden	30
Für jede Kategorie eine eigene E-Mail-Adresse verwenden ...	32
Die E-Mail-Adresse einfach erweitern	33
Schöne, saubere digitale Welt	34
Kapitel 3	
Software	37
Der Virenschutz – Hilfe gegen Schadsoftware	38
Ich verwende Windows. Da sollte ich einen Virenschanner installieren, oder?	38
Ist ein kostenpflichtiger Virenschutz besser als ein kostenfreier?	38
Braucht mein Apple-Computer mit macOS einen Virenschanner?	39
Ich verwende Linux. Da brauche ich keinen Virenschanner, oder?	39
Braucht mein Smartphone einen Virenschanner?	39
Wann Sie einen Virenschanner benutzen sollten!	39

Browser, Plugins und Pannen	40
Passwort-Safe – Das digitale Bankschließfach	41
Verschlüsselte Festplatten und USB-Sticks	43
Massenspeicher verschlüsseln.	44
Verschlüsselten Massenspeicher verwenden	49

Kapitel 4

Account-Pflege 55

Trennung von Accounts nach Anwendungsfall.	57
Starke Passwörter – Eine sichere Grundlage.	58
Die Zwei-Faktor-Authentifizierung – Eine zusätzliche Hürde ..	60
Soziale Netzwerke	61
Facebook	62
Twitter	69
Instagram	69
TikTok	72
Ein Wort zu beruflichen Netzwerken.	74
Xing.	74
LinkedIn	76
Messenger-Dienste	77
WhatsApp	77
Signal	80
Threema	80
Telegram	81
Wire	82
Element	83

Kapitel 5

Endgeräte absichern 85

Mobile Geräte.	85
Automatische Updates	86
Sichere Zugangsdaten auf dem Mobilgerät	89
Drittanbieter-Sperre	91
Sperrern von Apps mit Biometrie	92
Vorbereitet auf Verlust	94
Stationäre Geräte	100
Automatische Updates	100
Sichere Zugangsdaten zum Rechner.	104
Offline-Backup	107
Nutzerkonto ohne Admin-Rechte	109
Verschlüsselung des Systems.	112

Kapitel 6	
Sichere Online-Anbieter finden und prüfen.....	117
Die Seriosität einer Internetadresse erkennen.....	117
Das »s« in »https« steht nicht für Vertrauenswürdigkeit... ..	118
Wenn ein Betrüger versucht, Ihnen ein X für ein U zu verkaufen.....	118
Die Bestandteile einer Internetadresse –	
Das www ist nicht nötig	119
Merkmale einer vertrauenswürdigen Webseite	122
Warnhinweise erkennen und beachten.....	123
Verdächtige Webseiten überprüfen lassen	125
Gütesiegel erkennen und prüfen	126
Unternehmensregister und andere Unternehmensdaten sinnvoll nutzen.....	128
Ist die Umsatzsteuer-Identifikationsnummer gültig?	128
Sind Bilanzen und andere Dokumente veröffentlicht?	129
Für die letzten Zweifel: Der Handelsregisterauszug.....	130
Sicher bezahlen im Internet.....	132
Zahlung auf Rechnung	134
SEPA-Lastschrift	135
Abbuchungsauftrag unterschreiben.....	135
Zahlung mit Kreditkarte	135
Online-Bezahlsysteme.....	136
 Kapitel 7	
Spam- und Phishing-Mails erkennen.....	137
Wie erkenne ich böartige Nachrichten?	139
Spear-Phishing – Die gezielte Phishing-Attacke	142
Die gesunde Portion Skepsis	142
Netiquette und die richtige Kommunikation.....	143
Vishing – Der falsche Telefonanruf.....	145
 Kapitel 8	
Häufig gestellte Fragen	147
Ich habe auf einen Phishing-Link geklickt.	
Was kann ich nun tun?	147
Brauche ich eine Anti-Viren-Software?	147
Ich glaube, ich wurde gehackt. Wie gehe ich am besten vor?... ..	148
Ich will, dass ein Anbieter meine Daten löscht.	
Wie schaffe ich das?	149
Die Polizei hat mich mit der 110 angerufen.	
Ist der Anruf echt?.....	150
Ist es sicher, Passwörter im iCloud-Schlüsselbund zu sichern?	150

Ich weiß nicht, wo ich angemeldet bin, kann ich das irgendwo nachgucken?	151
Warum wird das Darknet nicht verboten?	151
Ich habe nichts zu verstecken. Warum sollte ich meine Daten schützen?	152
Ich werde per E-Mail erpresst. Woher hat der Erpresser mein Passwort?	152
Wie anonym bin ich im Inkognito-Modus der Standard-Browser?...	153
Wie kann ich meine Kinder zum sicheren Umgang im Netz bewegen?	153
Welche Maßnahmen sind beim Betreiben von SmartTVs zu empfehlen?	154
Ich suche online eine Ferienwohnung. Welche Betrugsmaschen gibt es?	154
Was muss ich bei Gewinnspielen im Internet beachten?	155
Beim Surfen öffnen sich ständig Fenster, auf die ich nicht geklickt habe.	156
Ich werde immer wieder auf Seiten weitergeleitet, die unseriös sind.	156

Kapitel 9
Zehn typische Betrugsmaschen im Internet **157**

Ware existiert nicht, wird aber trotzdem verkauft	157
Wie schützen Sie sich?	157
Der Dreiecksbetrug – Vorsicht, schwer zu durchschauen!	158
Wie schützen Sie sich?	158
Die Stellenanzeige - Zu verlockend? Vorsicht ist geboten	159
Wie schützen Sie sich?	159
Romance Scamming – Wenn digitale Liebe nicht echt ist	160
Wie schützen Sie sich?	161
Paketbetrug per SMS – Ein Klick vom Betrüger entfernt	161
Wie schützen Sie sich?	162
Einsammeln von Daten – Besser nicht ins Netz gehen	162
Wie schützen Sie sich?	163
Windows Updates – Return of the Suchleiste	163
Wie schützen Sie sich?	163
Erpressung in allen Formen und Varianten	164
Wie schützen Sie sich?	164
Gutscheinbetrug – Tausche Plastik gegen Geld	165
Wie schützen Sie sich?	165
Vorschussbetrug – Wenn Geld auch nicht gegen Geld fließt. . .	165
Wie schützen Sie sich?	166

Kapitel 10
Die zehn besten Tipps für das sichere Surfen
im Internet. 167

- Erneuern, verwalten und pflegen Sie Ihre Passwörter! 167
- So viel Software wie nötig, so wenig wie möglich ... und mit Update! 168
- Daten, die privat sind, sollten privat bleiben! 168
- Vorbereitet sein, Backup erstellen, sich sicher fühlen! 168
- Drei Augen sehen mehr: Nutzen Sie Antivirus-Software! 169
- Phishing? Schlagen Sie den Angreifern die Tür vor der Nase zu! 169
- Gehen Sie nicht auf ungeschützte Webseiten! 170
- Vermeiden Sie ungesicherte öffentliche Netzwerke! 170
- Prüfen und pflegen Sie Ihre Einstellungen! 171
- Virtual Private Network nutzen und unterwegs sicherer sein! 171

Stichwortverzeichnis 173

