

Microsoft Outlook und OneNote im Büro

Die besten Tipps & Tricks für effektives Arbeiten



- + E-Mails, Notizbücher, Aufgaben und Termine organisieren
- + Projektpläne und Dateien im Team teilen und bearbeiten
- + Auch unterwegs Kontaktdaten digitalisieren und Dokumente synchron halten

Impressum

Dieses E-Book ist ein Verlagsprodukt, an dem viele mitgewirkt haben, insbesondere:

Lektorat Isabella Bleissem

Korrektorat Angelika Glock, Ennepetal

Herstellung E-Book Maxi Beithe

Covergestaltung Mai Loan Nguyen Duy

Satz E-Book weiss.design/zienke.design

Bibliografische Information der Deutschen Nationalbibliothek: Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über *<http://dnb.d-nb.de>* abrufbar.

ISBN 978-3-8421-0697-0

1. Auflage 2019

© Rheinwerk Verlag GmbH, Bonn 2019

Vierfarben ist eine Marke des Rheinwerk Verlags.

www.rheinwerk-verlag.de

Liebe Leserin, lieber Leser,

mit dem richtigen Know-how sorgt Outlook für eine immense Arbeitserleichterung. Doch wer hat schon Zeit, in der täglichen E-Mail-Flut, bei der Vielzahl an Terminen und Projekten die geeigneten Optionen aufzuspüren? Auch OneNote ließe sich mit Gewinn für das Projektmanagement einsetzen. Aber treibt man dann nicht womöglich doppelten Aufwand?

Die Office-Profis Mareile Heiting und Carsten Thiele machen Sie mit ihren Tricks »aus der Praxis für die Praxis« in kürzester Zeit fit in den Tools – vom Einsatz des Abwesenheitsassistenten über Filterregeln und Besprechungsanfragen bis hin zu eigenen E-Mail-Vorlagen. Erstellen Sie Notizbücher mit Bildern, Videos und Links, und integrieren Sie hier nicht nur Ihre E-Mails, Kalender und Aufgaben aus Outlook, sondern auch etwa Word- und Excel-Dateien, auf die Sie in Meetings und unterwegs dank Cloud jederzeit zugreifen können. Wussten Sie, dass Sie mit Ihrem Smartphone gescannte Visitenkarten gleich in Ihre Outlook-Kontakte übertragen und Text von eingescannten Bildern in OneNote weiterbearbeiten können? Lassen Sie sich überraschen, und werden Sie Tipp für Tipp zum Organisationsprofi!

Dieses Buch wurde mit größter Sorgfalt geschrieben und hergestellt. Sollten Sie dennoch einmal einen Fehler finden oder inhaltliche Anregungen haben, freue ich mich, wenn Sie mit mir in Kontakt treten. Für Kritik bin ich dabei ebenso offen wie für lobende Worte. Doch nun wünsche ich Ihnen viel Erfolg bei der Umsetzung und so manches Aha-Erlebnis!

Ihre Isabella Bleissem

Lektorat Vierfarben

isabella.bleissem@rheinwerk-verlag.de

Inhalt

Sicher und ohne Störfaktoren in Outlook arbeiten

Nur Werbung oder Phishing? Wie gefährlich ist die E-Mail?	13
TIPP 001 Unverzichtbar: Ein kritischer Blick auf die E-Mail-Adressen	14
TIPP 002 Wichtige Indizien: Betreff, Anrede, Formatierung, Stil und Sprache ..	14
TIPP 003 Methoden, um an sensible Daten zu gelangen	15
TIPP 004 Umgang mit in E-Mails enthaltenen Links	16
TIPP 005 Finger weg von Dateianhängen	17
TIPP 006 Was tun mit der verdächtigen E-Mail?	18
TIPP 007 So prüfen Sie, ob Ihre E-Mail-Adresse bereits gehackt wurde	19
Wichtige Sicherheitseinstellungen vornehmen	20
TIPP 008 E-Mails im HTML-Format versus Nur-Text-Format	20
TIPP 009 Automatisches Herunterladen von Bildern unterbinden	21
TIPP 010 Zur Sicherheit: E-Mails immer im Nur-Text-Format lesen	22
TIPP 011 Junk-E-Mail-Optionen festlegen	23
TIPP 012 Unerwünschte Absender blockieren, erwünschte als sicher einstufen	25
Benachrichtigungen anpassen und ungestört arbeiten	27
TIPP 013 Benachrichtigungen in Outlook deaktivieren	27
TIPP 014 Benachrichtigungen anderer Anwendungen deaktivieren	28

Lassen Sie Outlook für sich sprechen

E-Mails nach formalen Vorgaben erstellen	31
TIPP 015 E-Mail mit Signatur abschließen	31
TIPP 016 Mehrere Signaturen für unterschiedliche Empfänger einrichten	33
TIPP 017 E-Mail-Adressen der Empfänger richtig erfassen	35
TIPP 018 Aussagekräftigen Text als Betreff wählen	37
TIPP 019 Kleine Hilfestellung für den Nachrichtentext	38

E-Mails grafisch aufpeppen	38
TIPP 020 Vorgefertigte Designs verwenden	39
TIPP 021 Eigene Schriftart in Kombination mit vorgefertigten Designs wählen	40
TIPP 022 Einzelne Nachrichten farbig aufpeppen	41
TIPP 023 Farbverläufe oder eigene Grafiken als Hintergrund nutzen	43
TIPP 024 Texte formatieren	44
So erstellen Sie eine E-Mail-Vorlage	45
TIPP 025 Eine neue Nachricht mit allen nötigen Elementen erstellen	45
TIPP 026 E-Mail als Outlook-Vorlage speichern	46
TIPP 027 E-Mail auf Basis der Outlook-Vorlage schreiben	47
TIPP 028 Änderungen an der Outlook-Vorlage vornehmen	48
E-Mails automatisch beantworten lassen	50
TIPP 029 Vorlage für die Antwortmail erstellen	51
TIPP 030 Den Regel-Assistenten starten	51
TIPP 031 Bedingungen festlegen, unter denen die Regel greifen soll	52
TIPP 032 Aktionen für eintreffende E-Mails auswählen	55
TIPP 033 Ausnahmen der Regeln festlegen	57
TIPP 034 Regelnamen eingeben und Regel fertigstellen	58
TIPP 035 Nicht mehr benötigte Regeln deaktivieren oder löschen	59
Microsoft Exchange Server: Abwesenheitsnotiz erstellen	61
TIPP 036 Automatische Antwort verfassen	61
TIPP 037 Automatische Antwort deaktivieren	63
Dateiinformationen vor dem Senden überprüfen	65
TIPP 038 Automatische Dokumentprüfung durchführen	65
TIPP 039 Dateieigenschaften bei Bildern entfernen	67

Das funktioniert nur selten: Gesendete E-Mails zurückrufen	69
TIPP 040 Bedingungen für einen Rückruf	69
TIPP 041 Gesendete E-Mail zurückrufen	70
TIPP 042 Alternativen zur Rückruffunktion	71
Outlook-Kontakte für Serienbriefe nutzen	74
TIPP 043 Kontakte für den Serienbrief auswählen	74
TIPP 044 Die Funktion »Serien-E-Mails« starten	75
TIPP 045 Seriendruckfelder in Word auswählen	76
TIPP 046 Fertige Serienbriefe per Vorschau prüfen	79
TIPP 047 Serienbrief fertigstellen	80

Ordnung schaffen in Outlook

So behalten Sie Ihre Unterhaltungen im Blick	83
TIPP 048 Die Unterhaltungsansicht aktivieren	83
TIPP 049 Alle Nachrichten einer Unterhaltung einblenden	85
TIPP 050 Unterhaltungseinstellungen vornehmen	85
TIPP 051 Optionen zum Aufräumen von Unterhaltungen auswählen	87
TIPP 052 Unterhaltungen aufräumen	89
Die bedingte Formatierung zum Auffinden von E-Mails nutzen	90
TIPP 053 Eine bedingte Formatierung für E-Mails festlegen	90
TIPP 054 Bedingte Formatierung entfernen	92
Die schnelle Erinnerungstütze: E-Mails mit Notizen versehen	93
TIPP 055 Eine erhaltene oder gesendete Nachricht bearbeiten	93
Ein Klick, und die Suche ist beendet: Suchordner	94
TIPP 056 Vordefinierte Suchordner aufrufen	95
TIPP 057 Suchordner erneut aufrufen, anpassen oder löschen	97
Gelöschte E-Mails automatisch endgültig entfernen	98
TIPP 058 Ordner »Papierkorb« automatisch leeren lassen	99

Die Schnellzugriffsleiste für häufig genutzte Befehle	101
TIPP 059 Eigene Befehle der Schnellzugriffsleiste hinzufügen	101
TIPP 060 Befehle aus der Schnellzugriffsleiste entfernen	102
Kontakte übersichtlich in Ordnern gruppieren	103
TIPP 061 Ordner für Kontakte erstellen	103
TIPP 062 Kontakte in den neuen Ordner verschieben	104
TIPP 063 Die Reihenfolge von Ordnern ändern	106
Eigene Ansichten für Kontaktdaten erstellen	106
TIPP 064 Die Listenansicht von Kontakten individuell anpassen	107
TIPP 065 Aktuelle Ansicht speichern	109
E-Mails, Ordner und Kontaktlisten zu Papier bringen	111
TIPP 066 Eine einzelne E-Mail ausdrucken	111
TIPP 067 Den Inhalt eines E-Mail-Ordners ausdrucken	111
TIPP 068 Eine Liste mit Kontaktdaten drucken	112
Dokument hängt in der Warteschlange – was nun?	113
TIPP 069 Druckvorgänge abbrechen oder löschen	114

Alle Termine im Blick

Zeitskala und Zeitzone im Kalender anpassen	117
TIPP 070 So ändern Sie die Zeitskala des Kalenders	117
TIPP 071 Termine mit gewünschter Zeitdauer eintragen	118
TIPP 072 Mehrere Zeitzonen anzeigen	119
Die passende Termindarstellung	121
TIPP 073 Einzelne Tage in einer Übersicht zusammenstellen	121
TIPP 074 Wichtige Termine hervorheben	122

Termine schneller finden	124
TIPP 075 Gezielt nach Terminen suchen	125
TIPP 076 Schnelle Navigation zu einem bestimmten Datum	126
Terminübersicht zu Papier bringen	127
TIPP 077 Kalenderübersicht ausdrucken	127
TIPP 078 Alle anstehenden Termine ausdrucken	129
Kalenderdateien in Outlook übernehmen	131
TIPP 079 Termine aus einer E-Mail in Outlook einfügen	131
TIPP 080 Eigene Kalenderdatei zum Versenden erstellen	133
Mehr Übersicht dank eigener Kalender	134
TIPP 081 Einen neuen Kalender anlegen	135
TIPP 082 Mehrere Kalender einblenden	135
TIPP 083 Anordnung der Kalender ändern	136
TIPP 084 Die Kalenderfarbe anpassen	137
Besprechungen innerhalb einer Firma planen	138
TIPP 085 Teilnehmer zu einer Besprechung einladen	139
TIPP 086 Einen freien Termin finden	140
TIPP 087 Besprechungsanfrage verschicken	141
Termine mit Personen außerhalb der Firma planen	143
TIPP 088 Einen Kalenderausschnitt festlegen	143
TIPP 089 Den Kalenderausschnitt per E-Mail versenden	145
TIPP 090 Per E-Mail versendeten Kalender öffnen	146

Aufgaben gekonnt planen

Das Wichtigste zuerst: So versehen Sie Ihre Aufgaben mit Prioritäten	149
TIPP 091 Schnell eine Aufgabe erfassen	149
TIPP 092 Eine neue Aufgabe mit Details anlegen	150
TIPP 093 Übersicht über anstehende Aufgaben	152

TIPP 094	Gut gegen Vergesslichkeit: Überfällige Aufgaben hervorheben	153
TIPP 095	Aufgabe als erledigt markieren oder ganz löschen	154
Aufgaben delegieren oder selbst empfangen		155
TIPP 096	Eine Aufgabe anderen zuweisen	155
TIPP 097	Delegierte Aufgabe wird angenommen	157
TIPP 098	Delegierte Aufgabe wird abgewiesen	158
TIPP 099	Selbst eine Aufgabenanfrage erhalten	159
Auch Aufgaben: E-Mails zur Nachverfolgung kennzeichnen		161
TIPP 100	Erhaltene E-Mails kennzeichnen	161
TIPP 101	E-Mail vor dem Senden zur Nachverfolgung kennzeichnen	162
TIPP 102	Kennzeichnung von E-Mails aufheben	165

Notizen und mehr digital erfassen mit OneNote

OneNote effektiv verwenden		167
TIPP 103	Welche Version darf es denn sein?	167
TIPP 104	Microsoft-Konto erforderlich – ja oder nein?	168
TIPP 105	Wie und wo werden Notizbücher gespeichert?	169
So erstellen Sie Ihr eigenes Notizbuch		170
TIPP 106	Ein neues Notizbuch anlegen	171
TIPP 107	Abschnitte erzeugen und gestalten	173
TIPP 108	Seiten hinzufügen und benennen	175
Ideen geschickt notieren		177
TIPP 109	Notizen eingeben	177
TIPP 110	Textcontainer verschieben und Containerbreite anpassen	178
TIPP 111	Notizen markieren und formatieren	180
TIPP 112	Blitzschnell Aufgabenlisten erzeugen	181
Bilder und Dateien als Gedächtnisstütze nutzen		183
TIPP 113	Ganz klassisch: Bild einfügen	184
TIPP 114	Bilder aus dem Internet wählen	185

TIPP 115	Onlinevideos einbinden	186
TIPP 116	Screenshot aus beliebiger Anwendung in OneNote einfügen	187
TIPP 117	Datei als Anlage oder Ausdruck einfügen	189
Arbeit erleichtern dank praktischer Seitenvorlagen		192
TIPP 118	Vorgefertigte Seitenvorlage von OneNote 2016 nutzen	192
TIPP 119	Eine Seite als Vorlage speichern	195
TIPP 120	Seiten auf Basis der eigenen Vorlage erstellen	197
Nicht nur für Touchscreen-Nutzer: Zeichnen in OneNote		198
TIPP 121	Zeichnen mit OneNote	198
Gesucht und schnell gefunden		200
TIPP 122	Eine einfache Suchanfrage starten	201
TIPP 123	Markierungen für Suchanfragen einfügen	202
TIPP 124	Suchanfragen anhand von Markierungen durchführen	203
TIPP 125	Eigene Markierungen erstellen	204
TIPP 126	Markierungen entfernen	205

Outlook, OneNote und OneDrive im Team

So arbeiten OneNote und Outlook perfekt zusammen		209
TIPP 127	Outlook-Termine und -Aufgaben mit OneNote-Notizen verknüpfen ...	210
TIPP 128	In OneNote erfasste Aufgabe in Outlook übernehmen	211
TIPP 129	Outlook-Aufgaben in OneNote-Notizbuch einfügen	213
TIPP 130	Besprechungsnotizen mit OneNote verarbeiten	214
TIPP 131	Inhalt einer E-Mail an OneNote senden	217
Dateien und Notizbücher in OneDrive ablegen		219
TIPP 132	Lokal gespeichertes Notizbuch in OneDrive verschieben	220
TIPP 133	Zugriff auf OneDrive via Explorer	222
TIPP 134	Zugriff auf OneDrive via Browser	224
TIPP 135	Online gespeicherte Dateien im Browser öffnen	226
TIPP 136	In der Cloud gespeicherte Notizbücher im Browser öffnen	227

OneNote-Notizen mit anderen teilen	229
TIPP 137 Notizbuch für andere Personen freigeben	230
TIPP 138 Auf freigegebenes Notizbuch zugreifen	231
TIPP 139 Notizbuch mit mehreren bearbeiten	232
TIPP 140 Freigabe zurückziehen	233
Kennwortschutz für Notizbücher und Dateien	234
TIPP 141 Abschnitte eines Notizbuchs per Kennwort schützen	234
TIPP 142 Kennwortschutz für Dateien	236
Der Scanner für unterwegs: Office Lens	237
TIPP 143 Office Lens installieren	238
TIPP 144 Mit dem Scannen beginnen	238
TIPP 145 Speicherort auswählen	240
TIPP 146 Kontaktdaten in der Kontakte-App speichern	242

Mit Shortcuts noch effektiver arbeiten

Funktionen in Outlook mithilfe von Tastenkombinationen schneller ausführen	247
Pfiffige Tastenkombinationen für OneNote	251
Stichwortverzeichnis	253

Sicher und ohne Störfaktoren in Outlook arbeiten



Wie viele E-Mails bekommen Sie am Tag? 20, 50 oder sogar mehr? Und wie viele dieser Nachrichten betreffen tatsächlich Sie persönlich? Die Zahl der unerwünscht erhaltenen E-Mails nimmt stetig zu. Während ein Teil davon einfach nur lästig ist, bringen andere große Gefahren mit sich. Zu Beginn dieses Buches erfahren Sie daher, wie Sie bei Ihrer privaten wie geschäftlichen Korrespondenz harmlose von gefährlichen E-Mails unterscheiden können und welche Schutzmaßnahmen Sie unbedingt ergreifen sollten. Außerdem zeigen wir Ihnen, wie Sie zukünftig konzentrierter arbeiten können, ohne durch Benachrichtigungen von Outlook und anderen Apps abgelenkt zu werden.

Nur Werbung oder Phishing? Wie gefährlich ist die E-Mail?

Eine E-Mail, die einem unerwünscht zugesendet wird, wird *Spam* oder auch *Junk* genannt. Enthält eine solche E-Mail lediglich Werbung, ist sie zwar lästig, im Vergleich zu infizierten E-Mails, über die Sie sich Viren und andere Schadsoftware auf den PC holen, ist sie aber harmlos. Eine große Gefahr stellen heutzutage außerdem Phishing-E-Mails dar. Das Ziel des *Phishings* (ein Kunstwort, das sich aus den Wörtern »Passwort« und »Fishing« zusammensetzt) ist, z. B. über gefälschte E-Mails und Webseiten persönliche Daten wie Passwörter oder Kreditkarteninformationen abzugreifen. Doch wie unterscheidet man gefährliche E-Mails von harmlosen?

Unverzichtbar: Ein kritischer Blick auf die E-Mail-Adressen

Amazon, eBay, ein bekanntes Kreditinstitut oder auch PayPal: Wenn Sie E-Mails von derartigen Absendern erhalten, sollten Sie als Erstes hinterfragen, ob Sie dort überhaupt Kunde sind. Haben Sie sich z. B. noch nie über die E-Mail-Adresse, an die die Nachricht geschickt wurde, beim Auktionshaus eBay angemeldet, ist dies ein erstes Indiz dafür, dass es sich um eine betrügerische E-Mail handelt. Überprüfen Sie außerdem die vollständige Adresse des Absenders. Häufig können Sie in einem solchen Fall feststellen, dass sich der angegebene Name **1** von der eigentlichen Domain **2** unterscheidet. Solche Differenzen finden sich auch in E-Mails, in denen Ihnen eine große Erbschaft, eine Beteiligung an einem Lottogewinn oder die tollsten Schnäppchen angeboten werden.



Wichtige Indizien: Betreff, Anrede, Formatierung, Stil und Sprache

Der Betreff der E-Mail lockt Sie mit einem ausgesprochen günstigen Angebot? Sie werden in der Nachricht nicht persönlich angesprochen, sondern neutral mit »Sehr geehrte



te Damen und Herren« oder auch nur mit »Hallo«? Allein diese zwei Punkte sollten Sie bereits stutzig machen. Ist die E-Mail dann auch noch in ei-

nem schlechten Deutsch verfasst, enthält zahlreiche Rechtschreib- und Grammatikfehler und ist nicht einheitlich formatiert, ist spätestens der Moment gekommen, in dem Sie wachsam sein sollten. Denn seriöse Firmen schicken ihren Kunden ganz sicher keine derartigen Nachrichten. Da Betrüger mittlerweile immer trickreicher werden, bedeutet es im Umkehrschluss leider nicht, dass eine perfekt verfasste Nachricht, in der Sie mit Ihrem Namen angesprochen werden, deshalb harmlos ist.

Methoden, um an sensible Daten zu gelangen

**Tipp
003**

Das wertvollste Gut für Betrüger sind Kreditkarteninformationen, Passwörter und andere vertrauliche Informationen. Um an diese Daten zu gelangen, versuchen Kriminelle mithilfe von geschickt formulierten Nachrichten, den Empfänger so unter Druck zu setzen, dass dieser sie freiwillig preisgibt. So wird in diesen Phishing-E-Mails z. B. behauptet, auf Ihrem Konto seien Unstimmigkeiten oder Sicherheitsrisiken (1 auf Seite 16) festgestellt worden. Um diese prüfen zu können, sollen Sie sich innerhalb einer sehr kurz gesetzten Frist bei Ihrem Online-Konto anmelden. Kommen Sie dieser Aufforderung nicht nach, droht man Ihnen damit, das Konto zu sperren. Der in der E-Mail enthaltene Link (2) führt Sie angeblich direkt zur Anmeldeseite bei Ihrer Online-Bank, Ihrem Online-Shop etc. Die aufgerufene Webseite mag der realen Seite sogar täuschend ähnlich sehen. Würden Sie auf dieser nachgeahmten Seite tatsächlich vertrauensvolle Daten eingeben, könnten die Betrüger sie abgreifen und zukünftig nutzen. Das ist allerdings nicht die einzige Gefahr: Häufig enthält eine solche Webseite auch Schadsoftware, die beim Besuch der Seite auf Ihren Computer heruntergeladen wird.

Umgang mit in E-Mails enthaltenen Links

Das Wichtigste zuerst: Klicken Sie in verdächtig anmutenden E-Mails nie auf die darin enthaltenen Links! Um zu überprüfen, ob die mit dem Link verknüpfte Webadresse wirklich z. B. zu Ihrer Bank führt, positionieren Sie den Mauszeiger über dem Link. In einer QuickInfo wird nun die damit verbundene Adresse angezeigt **3**. Eine gefälschte Webadresse kann teilweise sehr kryptisch aussehen, manchmal unterscheidet sie sich von der realen Adresse aber auch nur in einem fehlenden (z. B. »amzon« statt »amazon«) oder einem ähnlich aussehenden Buchstaben (etwa »Ibb« statt »lbb«). Was Sie beachten sollten, wenn Sie sich bei einem Ihrer Online-Konten anmelden, lesen Sie im Kasten »Das kleine Einmaleins zum Eigenschutz« auf Seite 17.

Guten Tag,

Amazon nimmt die Sicherheit Ihres Kontos sehr ernst.

Wir bitten Sie um weitere Informationen zu Ihrem Konto. Da wir nichts von Ihnen gehört haben, wurde Ihr Konto weiter eingeschränkt.

Ihr Konto wurde eingeschränkt, da Sie seit Kurzem erheblich Sicherheitsmängel haben. Als Ihre Sicherheitsstelle müssen wir diese Veränderungen und deren Zusammenhang mit Ihnen nachvollziehen können. **1**

Wir bitten Sie daher, sich als Inhaber Ihres Kontos zu identifizieren.

Klicken Sie auf den unten angezeigten Link und folgen Sie den Anweisungen.

Wird festgestellt, dass Sie falsche Informationen / falsche Zahlungsdaten eingeben oder diese Bestätigung ignorieren, wird Ihr Konto weiter eingeschränkt. Bitte kontaktieren Sie unsere Sicherheitsabteilung gemeldet. <http://webhop.se/151n> **3**
Klicken oder tippen Sie, um dem Link zu folgen.

Weiter (über den Sicherheitsserver) **2**

Nach der Bestätigung wird Ihr Account reaktiviert.
Wir danken Ihnen für Ihr Verständnis.

Das kleine Einmaleins zum Eigenschutz

Wenn Sie sich bei Ihrer Online-Bank, einem Reiseportal, einem Online-Shop oder auch einem sozialen Netzwerk anmelden wollen, tippen Sie die Webadresse zur Sicherheit immer selbst im Browser ein. Sensible Daten wie Passwörter oder Kreditkarteninformationen sollten Sie außerdem nur über eine verschlüsselte Internetverbindung eingeben. Diese erkennen Sie am »https« in der Adresszeile des Browsers. Befinden Sie sich in einem öffentlichen Netzwerk (z. B. am Flughafen oder in einem Café), sollten Sie auf die Eingabe sensibler Daten ganz verzichten. Auch bei der Passwortwahl können Sie für mehr Schutz sorgen: Achten Sie hier auf möglichst komplexe Zeichenfolgen, die aus Groß- und Kleinbuchstaben, Zahlen sowie Sonderzeichen bestehen. Verwenden Sie ein Passwort nie mehrfach, sondern legen Sie für jedes Online-Portal ein eigenes Passwort an. Sorgen Sie dafür, dass Ihr Computer, Tablet oder Smartphone immer mit den neuesten Updates versorgt ist. Der Einsatz einer Sicherheitssoftware versteht sich von selbst.

Finger weg von Dateianhängen

**Tipp
005**

Sie haben angeblich eine Rechnung nicht beglichen? Eine Kanzlei oder ein Inkassounternehmen ist nun damit beauftragt worden, den ausstehenden Betrag bei Ihnen einzufordern. Die E-Mail, in der Sie zur Nachzahlung aufgefordert werden, enthält im Dateianhang vermeintlich die Rechnung. Bei derartigen E-Mails – die im Übrigen nicht nur Mahnungen, sondern z. B. auch Bestätigungen zu Bestellungen oder Reservierungen, die Sie gar nicht vorgenommen haben, zum Inhalt haben können – ist höchste Alarmbereitschaft angesagt, denn die Dateianhänge enthalten in den meisten Fällen Schadsoftware. Durch Öffnen der Datei gelangt z. B. ein Virus

auf Ihren PC. Der Schaden, den dieser verursacht, kann vom Ausspähen all Ihrer Tastatureingaben inklusive sensibler Daten bis hin zum totalen Computerausfall reichen. Erhalten Sie eine solche E-Mail, öffnen Sie daher keinesfalls die angehängte Datei!

**Tipp
006**

Was tun mit der verdächtigen E-Mail?

Sie sind sich ziemlich sicher, dass es sich bei einer erhaltenen E-Mail um eine Phishing-E-Mail handelt? Wenn Sie in einer größeren Firma arbeiten, sollten Sie unbedingt den für solche Fälle zuständigen IT-Sicherheitsbeauftragten informieren. Auch das Unternehmen, von dem die Nachricht angeblich stammt, sollte über den Phishing-Versuch in Kenntnis gesetzt werden. Banken, aber auch große Online-Shops wie Amazon bieten hierfür meist spezielle Anlaufstellen, die Sie beim Unternehmen selbst in Erfahrung bringen können. Nutzen Sie zur Kontaktaufnahme keinesfalls die in der Phishing-E-Mail enthaltenen Daten, da auch diese meist gefälscht sind.

The screenshot shows the Amazon.de website's help section. At the top, there's a search bar with 'Alle' selected. Below it, navigation links include 'Lieferrn nach 85748 Garching ...', 'Alle Kategorien', 'Mein Amazon.de', 'Angebote', 'Gutscheine', 'Verkaufen', and 'Hilfe'. The main heading is 'Hilfe und Kundenservice'. A search bar contains 'Thema oder Schlagw' and 'Los'. A sidebar on the left lists 'Alle Hilfethemen' and 'E-Mails von Amazon', with sub-items like 'Gefälschte ("Phishing" oder "Spoofed") E-Mails melden', 'Verifizieren der E-Mail-Adresse bei neuen Kundenkonte', 'Über Amazon', 'Kundenbefragungen per E-Mail', 'Amazon Benachrichtigungen als HTML-E-Mails', 'Fax Anfragen', 'Über maschinelle Übersetzungen', and 'Über Übersetzungen'. The main content area is titled 'Gefälschte ("Phishing" oder "Spoofed") E-Mails melden' and includes a breadcrumb 'Sicherheit & Datenschutz > E-Mails von Amazon'. The text states: 'Wir nehmen Phishing oder Spoofing Angriffe auf unsere Kunden sehr ernst. Sollten Sie eine E-Mail erhalten haben, von der Sie denken, dass sie nicht von Amazon stammen könnte, melden Sie uns den Vorfall, indem Sie die betreffende E-Mail an stop-spoofing@amazon.com weiterleiten.' Below this, there's a link 'Hinweise zur sicheren Identifizierung von Amazon E-Mails finden Sie hier.' and a section 'So melden Sie uns eine gefälschte ("Phishing" oder "Spoofed") E-Mail:' with a numbered list: '1. Führen Sie eine der folgenden Aktionen aus:' followed by a sub-item 'o Beginnen Sie eine neue E-Mail und hängen Sie die verdächtige E-Mail an.' and a bolded 'Anmerkung: Wenn die E-Mail als Anhang gesendet wird, bleiben Informationen erhalten, mit deren Hilfe wir die Herkunft der E-Mail besser nachverfolgen können.'

Zusätzlich können Sie auch eine Verbraucherzentrale über den Phishing-Versuch informieren. Die betrügerische E-Mail selbst sollten Sie anschließend löschen.

So prüfen Sie, ob Ihre E-Mail-Adresse bereits gehackt wurde

**Tipp
007**

Immer wieder wird bekannt, dass Unternehmen Opfer eines Hackerangriffs wurden, bei dem Millionen sensibler Daten abgegriffen werden konnten. Diese Daten (z. B. E-Mail-Adressen in Kombination mit Passwörtern, Telefonnummern oder gar Kreditkarteninformationen) werden häufig in unrechtmäßigen Identitätsdatenbanken veröffentlicht. Dort können sie wiederum von Unbefugten eingesehen und für betrügerische Zwecke genutzt werden. Über den *Identity Leak Checker* des Hasso-Plattner-Instituts (<https://sec.hpi.de/ilc>) können Sie überprüfen, ob auch Ihre E-Mail-Adresse gehackt wurde. Nachdem Sie Ihre Adresse auf der Website des Instituts eingegeben haben, werden Sie in einer Antwortmail darüber informiert, ob diese Adresse betroffen ist. Fällt die Antwort positiv aus, sollten Sie unverzüglich alle damit verbundenen Passwörter ändern, angefangen beim E-Mail-Konto selbst bis hin zu Websites, auf denen Sie die E-Mail-Adresse zur Anmeldung nutzen.

Ergebnis Ihrer Anfrage bei HPI Identity Leak Checker							
<p>Achtung: Ihre E-Mail-Adresse taucht in mindestens einer gestohlenen und unrechtmäßig veröffentlichten Folgende sensible Informationen wurden im Zusammenhang mit Ihrer E-Mail-Adresse frei im Internet gefunden:</p>							
Betroffener Dienst	Datum	Verifiziert	Betroffene Nutzer	Passwort	Vor- und Zuname	Geburtsdatum	Anschritt
Unknown (Collection #1-#5)	Jan. 2019		2.191.498.885	Betroffen	–	–	–
<i>Dieser Datensatz wurde im Januar 2019 veröffentlicht und enthält riesige Listen von Zugangsdaten unbekannter</i>							
adobe.com	Okt. 2013	✓	152.375.851	Betroffen	–	–	–
linkedin.com	Jun. 2012	✓	160.144.040	Betroffen	–	–	–

Wichtige Sicherheitseinstellungen vornehmen

Wie Sie im vorherigen Abschnitt sehen konnten, ist einer der wichtigsten Schutzmechanismen vor gefährlichen E-Mails der gesunde Menschenverstand: Haben Sie Zweifel an der Seriosität einer Nachricht, heißt es schlichtweg Finger weg: keine Links in den E-Mails anklicken, keine Dateianhänge öffnen, sondern stattdessen die betreffenden E-Mails löschen.

Zusätzlich sollten Sie aber auch die Möglichkeiten zur Absicherung nutzen, die Ihnen die E-Mail-Programme zur Verfügung stellen. Die wichtigsten Sicherheitseinstellungen stellen wir Ihnen am Beispiel von Outlook in den folgenden Tipps vor. In größeren Unternehmen werden diese Einstellungen meist von den für die IT-Sicherheit verantwortlichen Stellen vorgenommen und auch überwacht.

**Tipp
008**

E-Mails im HTML-Format versus Nur-Text-Format

E-Mails können im *HTML-Format* oder im *Nur-Text-Format* erstellt werden. Das Nur-Text-Format hält, was der Name verspricht: Die Nachricht enthält nur schlichten Text ohne jegliche Formatierungen und ohne Bilder (abgesehen von Bildern, die einer E-Mail als Dateianhang beigefügt wurden). Eine E-Mail im HTML-Format kommt im Gegensatz hierzu weitaus farbenfroher daher, denn mithilfe von HTML (Abkürzung für *Hypertext Markup Language*, auf Deutsch »Hypertext-Auszeichnungssprache«) lassen sich nicht nur vielseitige Textgestaltungen vornehmen, sondern z. B. auch Bilder in

die E-Mail einbetten. Ein paar Beispiele hierfür lernen Sie im Abschnitt »E-Mails grafisch aufpeppen« ab Seite 38 kennen.

Bilder, die per HTML in E-Mails eingebunden werden, werden erst beim Öffnen der Nachricht von einem externen Server heruntergeladen. Dieser Vorgang wird von Unternehmen gerne genutzt, um festzustellen, ob eine E-Mail-Adresse gültig ist. Werden die Bilder also vom Server geladen und in der E-Mail angezeigt, weiß der Absender der Nachricht damit, dass Ihre E-Mail-Adresse korrekt ist. Solche Informationen sind ausgesprochen wertvoll, denn mit dem Verkauf der verifizierten Adressen lässt sich viel Geld verdienen.

Das Nachladen externer Inhalte wie Bilder bringt aber eine noch weitaus größere Gefahr mit sich, denn auf diese Weise kann auch Schadcode auf Ihren Computer eingeschleust werden.

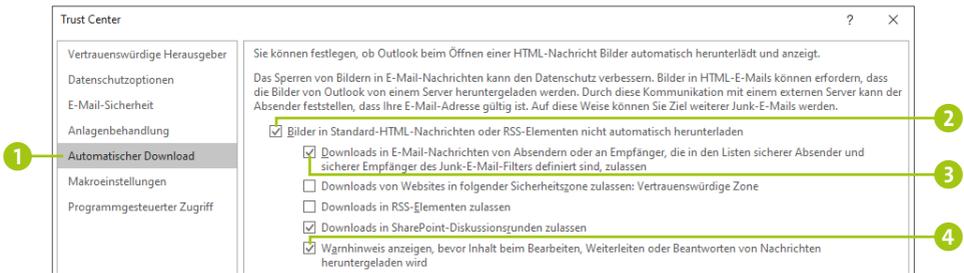
Automatisches Herunterladen von Bildern unterbinden

Tipps
009

Per Standardeinstellung verhindert Outlook das automatische Herunterladen von Bildern in E-Mails im HTML-Format. Zur Sicherheit sollten Sie diese Einstellung aber überprüfen.

1. Rufen Sie in Outlook im Register **Datei** die **Optionen** auf.
2. Markieren Sie in der linken Spalte des Dialogs **Outlook-Optionen** das **Trust Center**. Klicken Sie dann rechts auf **Einstellungen für das Trust Center**.
3. Im Dialog **Trust Center** sollte links nun bereits **Automatischer Download** ① markiert sein. Stellen Sie sicher, dass rechts **Bilder in Standard-HTML-Nachrichten oder RSS-Elementen nicht automatisch herunterladen** mit einem Häkchen versehen ist ②.

4. Wenn es Kontakte oder Firmen gibt, denen Sie absolut vertrauen, können Sie diese mithilfe des Junk-E-Mail-Filters als vertrauenswürdig kennzeichnen (siehe Tipp 012 auf Seite 25). Dürfen in E-Mails, die von diesen Kontakten stammen, die Bilder automatisch heruntergeladen werden, aktivieren Sie **Downloads in E-Mail-Nachrichten von Absendern oder an Empfänger, die in den Listen sicherer Absender ..., zulassen** 3.
5. Beim Weiterleiten, Bearbeiten oder Beantworten von E-Mails kann es passieren, dass externer Inhalt automatisch heruntergeladen wird. Damit dies nicht ohne Ihr Wissen geschieht und Sie es ggf. auch unterbinden können, sollten Sie sich durch Aktivierung des Kontrollkästchens 4 einen Warnhinweis anzeigen lassen.



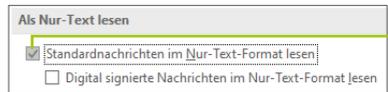
**Tipp
010**

Zur Sicherheit: E-Mails immer im Nur-Text-Format lesen

Wer keinerlei Risiko beim Empfang von E-Mails eingehen möchte, lässt sich die Nachrichten am besten immer im Nur-Text-Format anzeigen. Wenn Sie einem Empfänger vertrauen, können Sie die Darstellung später wieder in das HTML-Format konvertieren lassen. Um das Nur-Text-Format einzustellen, rufen Sie, wie in den Schritten 1 und 2 des vorherigen Tipps auf Seite 21 gezeigt, den Dialog **Trust Center** auf.

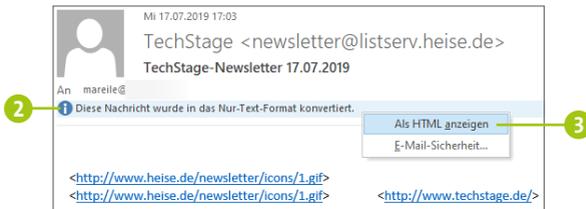
1. Markieren Sie im Dialog links **E-Mail-Sicherheit**.

2. Versetzen Sie nun rechts im Bereich **Als Nur-Text lesen** das Kästchen **Standardnachrichten im Nur-Text-Format lesen** im **Nur-Text-Format lesen** 1 mit einem Häkchen.



3. Schließen Sie alle noch geöffneten Dialoge mit **OK**, um Ihre Einstellungen zu übernehmen.

Alle E-Mails werden jetzt ausschließlich im Nur-Text-Format angezeigt. Unterhalb der Absenderadresse erscheint in der Nachricht entsprechend der Hinweis **Diese Nachricht wurde in das Nur-Text-Format konvertiert** 2.



4. Wenn Sie dem Absender vertrauen und die E-Mail in voller Schönheit sehen möchten, klicken Sie mit der rechten Maustaste auf den Hinweis und wählen im Kontextmenü **Als HTML anzeigen** 3.

Sollte Ihnen die Darstellung im Nur-Text-Format auf Dauer zu rigide sein, wiederholen Sie einfach die Schritte 1 und 2 und entfernen das Häkchen vor **Standardnachrichten im Nur-Text-Format lesen** 1 wieder.

Junk-E-Mail-Optionen festlegen

**Tipp
011**

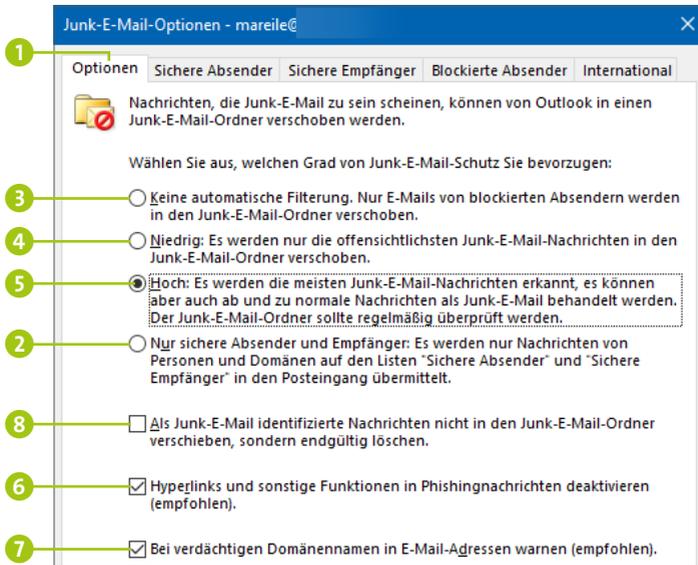
Spam bzw. Junk-E-Mails sind ausgesprochen lästig. Outlook verfügt über einen Filter, mit dem das Programm verdächtige E-Mails aufspüren kann und automatisch in den Ordner

Junk-E-Mail verschiebt. Nicht immer gelingt das Outlook allerdings perfekt, sodass ab und an auch für Sie relevante Reservierungsbestätigungen oder Nachrichten von Kunden in diesem Ordner landen. Sie sollten also regelmäßig einen Blick in den Ordner werfen und prüfen, ob hier eine eigentlich wichtige E-Mail abgelegt wurde. Um den Grad festzulegen, in dem Outlook Sie vor Junk-E-Mails schützen soll, gehen Sie folgendermaßen vor:

- 1.** Stellen Sie sicher, dass Sie sich in Outlook im Modul **E-Mail** befinden. Klicken Sie hier im Register **Start** in der Gruppe **Löschen** auf **Junk-E-Mail ► Junk-E-Mail-Optionen**.
- 2.** Der Dialog **Junk-E-Mail-Optionen** wird mit dem Register **Optionen** **1** geöffnet. Wenn Sie in der Firma häufiger auch E-Mails von Unbekannten erhalten, wird die Option **Nur sichere Absender und Empfänger** **2** zu rigide sein. Denn in diesem Fall verschiebt Outlook alle E-Mails, deren Absender Sie nicht ausdrücklich als sicher eingestuft haben, automatisch in den Junk-E-Mail-Ordner.
- 3.** Zu wenig Schutz bietet umgekehrt die Option **Keine automatische Filterung** **3**, da hier lediglich die Nachrichten von bereits blockierten Absendern als Junk-E-Mail eingeordnet werden.
- 4.** Entscheiden Sie sich also für eine der beiden Optionen **Niedrig** **4** bzw. **Hoch** **5**. Sobald Sie eine der Optionen ausgewählt haben, werden zwei weitere Kästchen eingeblendet, die Sie aktivieren sollten. Damit stellen Sie sicher, dass Hyperlinks und sonstige Funktionen in Phishing-Nachrichten deaktiviert werden **6** und Sie bei verdächtigen Domännennamen in E-Mail-Adressen gewarnt werden **7**.
- 5.** Outlook bietet Ihnen die Möglichkeit, alle Nachrichten, die es als Junk-E-Mail identifiziert, sofort zu löschen und

gar nicht erst in den Junk-E-Mail-Ordner zu verschieben **8**. Da das Programm aber, wie bereits erwähnt, nicht immer ganz zuverlässig arbeitet und so auch manche wichtige E-Mail als verdächtig eingestuft wird, sollten Sie diese Möglichkeit nicht in Anspruch nehmen.

6. Übernehmen Sie Ihre Einstellungen mit **OK**.



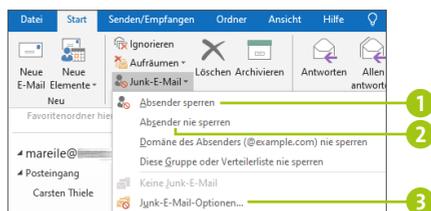
Unerwünschte Absender blockieren, erwünschte als sicher einstufen

**Tipp
012**

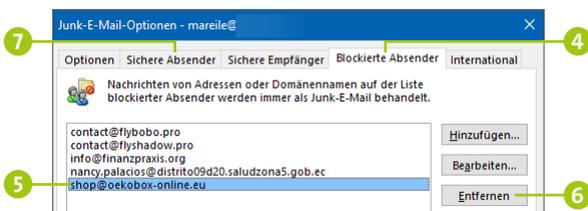
Sie bekommen immer wieder einen Newsletter, den Sie nicht bestellt und auch nicht haben möchten? Am liebsten wäre es Ihnen, wenn die E-Mails von diesem Absender sofort automatisch im Junk-E-Mail-Ordner landen würden? Nichts leichter als das.

1. Markieren Sie hierzu einfach die unerwünscht erhaltene E-Mail in der E-Mail-Übersicht. Klicken Sie dann im

Register **Start** in der Gruppe **Löschen** auf **Junk-E-Mail ▶ Absender sperren** ①. Outlook wird alle E-Mails dieses Absenders zukünftig automatisch blockieren und in den Junk-E-Mail-Ordner verschieben.



2. Gibt es umgekehrt Absender, denen Sie absolut vertrauen, können Sie diese ebenfalls kennzeichnen. Hierzu gehen Sie so vor, wie gerade am Beispiel der unerwünscht erhaltenen E-Mail gezeigt, nur dass Sie dieses Mal **Junk-E-Mail ▶ Absender nie sperren** ② wählen. Der Absender gilt damit zukünftig als sicherer Absender.
3. Wenn Sie einen Blick auf die Liste der blockierten oder auch sicheren Absender werfen wollen, rufen Sie im Register **Start** über **Junk-E-Mail** die **Junk-E-Mail-Optionen** ③ auf. Haben Sie eine E-Mail-Adresse versehentlich blockiert und möchten diese Blockierung wieder aufheben, wechseln Sie in das Register **Blockierte Absender** ④, markieren die entsprechende E-Mail-Adresse ⑤ und klicken auf **Entfernen** ⑥.



4. Analog können Sie eine E-Mail-Adresse auch im Register **Sichere Absender** ⑦ entfernen.
5. Schließen Sie den Dialog **Junk-E-Mail-Optionen** dann mit **Übernehmen** und **OK**.

Benachrichtigungen anpassen und ungestört arbeiten

Sobald eine neue E-Mail in Outlook eintrifft, ertönt ein kurzes Signal, und im Infobereich der Taskleiste wird das Symbol eines Briefumschlags eingeblendet. Zusätzlich erscheint für einen Moment ein kleines Hinweisfenster, in dem der Absender sowie der Betreff der E-Mail angezeigt werden. Viele Anwender sind nun so pflichtbewusst, dass sie sofort einen Blick auf die E-Mail werfen. Und schon vergeht kostbare Zeit, die man eigentlich für die aktuelle Aufgabe benötigt. Nimmt man noch die Benachrichtigungen von sozialen Netzwerken wie Facebook hinzu oder neue Chats in Messengern wie WhatsApp, ist man schnell nur noch mit dem Reagieren auf Nachrichten beschäftigt.

Benachrichtigungen in Outlook deaktivieren

**Tipp
013**

Alles hat seine Zeit. Das gilt für die Bearbeitung von E-Mails, aber auch für alle anderen Aufgaben. Wenn Sie sich durch neu eintreffende Nachrichten nicht mehr von anderen wichtigen Arbeiten ablenken lassen möchten, sollten Sie die Benachrichtigungen in Outlook deaktivieren.

1. Rufen Sie in Outlook das Register **Datei** auf, und klicken Sie hier auf **Optionen**.
2. Markieren Sie im Dialog **Outlook-Optionen** in der linken Spalte **E-Mail**. In der rechten Spalte blättern Sie nach unten bis zum Bereich **Nachrichteneingang**.

