

So geht's leichter...



E-Mail

- **Mit und ohne Outlook**
- **Mehr Sicherheit**
- **Backups anfertigen**
- **Webmailer nutzen**

Inhaltsverzeichnis

| | |
|---------------------------------------------------|-----------|
| E-Mail nutzen – aber richtig | 3 |
| Das Einrichten eines E-Mail-Kontos | 4 |
| Die Windows Mail-App | 4 |
| Microsoft Outlook | 5 |
| Einstellen des Abrufintervalls | 6 |
| Werbung und verlorene E-Mails | 7 |
| SPAM-Ordner und Junk-Email | 7 |
| Intelligenter SPAM-Filter in Office 365: Clutter | 8 |
| Wenn keine Mails mehr ankommen | 9 |
| Mailblockaden durch SPAM-Listen | 10 |
| Praxistipps zur Zeitersparnis | 12 |
| Senden einer E-Mail von einem anderen Konto | 12 |
| Wenn Mails nur noch grau und unformatiert sind | 14 |
| Auffinden verlorenen Entwürfe in Outlook | 15 |
| Antworten in vordefinierten Formularen in Outlook | 17 |
| Erstellen eines E-Mail-Templates | 18 |
| Fokus auf das Wichtige: Focused Inbox | 19 |
| Integration von Twitter in Outlook | 20 |
| E-Mail-Sicherheit | 22 |
| Zugangsschutz: Anforderungen an Passwörter | 22 |
| Ist es schon zu spät? | 22 |
| Das sichere Passwort | 23 |
| Verwendung eines Passwortgenerators | 25 |
| Speichern von Passwörtern in einem Safe | 26 |
| Die Zwei-Faktor-Authentifizierung (2FA) | 28 |
| Aktivieren der Zwei-Faktor-Authentifizierung | 29 |

Windows 10-Report Ausgabe 19/09

Mitlesen, mitreden.

| | |
|--------------------------------------------------------|-----------|
| Nutzen der 2FA in Outlook | 33 |
| Backup, Migration und Wechsel von E-Mail-Konten | 34 |
| Der Backup der E-Mail-Daten aus Outlook | 35 |
| Die Migration zu Office 365 | 36 |
| Bequemer mit einer Datenspedition | 37 |
| Wechsel eines E-Mail-Kontos ohne Verluste | 39 |
| Webmailer als Alternative | 40 |
| Der private Surfmodus | 41 |
| Edge immer im privaten Surfmodus starten | 42 |
| Löschen der Internetspuren | 44 |
| Schutz vor Schädlingen durch Smartscreen | 46 |

E-Mail nutzen – aber richtig

Auch wenn Messenger-Dienste wie WhatsApp und Facebook für die schnelle Kommunikation großartig sind: Wenn Sie Informationen hin- und herschicken müssen, dann ist die gute alte E-Mail immer noch das Mittel der Wahl. Windows 10 bietet hier viele Möglichkeiten: Sowohl im Betriebssystem selbst als auch über Zusatz-Programme und das Internet können Sie Ihre Kommunikation optimieren.



Wir zeigen Ihnen, wie Sie in der Windows Mail-App und im Office-Programm Outlook Ihr E-Mail-Konto konfigurieren. Lassen Sie uns Ihnen Arbeit abnehmen, in dem Sie Abläufe automatisieren.

Wenn Sie noch ein altes POP3-Konto Ihr Eigen nennen und sich darüber ärgern, dass Sie nur auf einem PC Ihre E-Mails nutzen können: In diesem Report bekommen Sie eine Schritt-für-Schritt-Anleitung, wie Sie zu Office 365 wechseln können.

Windows 10-Report Ausgabe 19/09

Mitlesen, mitreden.

Sicherheit ist ein wichtiger Faktor der Kommunikation. Sichern Sie mit unseren Praxis-Tipps Ihre Kommunikation ab, damit niemand mithören kann.

Das Einrichten eines E-Mail-Kontos

Am Anfang steht immer die Einrichtung des E-Mail-Kontos. Normalerweise haben Sie über Ihren Internet-Anbieter automatisch eine E-Mail-Adresse. Die zugehörigen Informationen zur Einrichtung Ihres Mailprogramms finden Sie dann auf den Hilfeseiten des Anbieters.

Alternativ können Sie auch einen Webmail-Anbieter wie GMX, Web.de und andere nutzen. Nach dem Anlegen des Kontos bekommen Sie die nötigen Informationen dort ebenfalls. Am Ende dieses Reports finden Sie viele Tipps, wie Sie sicher mit Web-Mailern arbeiten können!

Die Windows Mail-App

Die Windows Mail-App ist die einfachste Möglichkeit, in Windows 10 E-Mails zu senden und zu empfangen. Um ein neues E-Mail-Konto einzurichten, klicken Sie auf das **Zahnrad** unten links im Programmfenster. Die oberste Option im sich nun öffnenden Menü führt Sie direkt zu **Konten verwalten**.

Klicken Sie auf **+ Konto hinzufügen** und wählen Sie dann den Mail-Anbieter aus. Ist Ihrer nicht in der Liste, dann können Sie das Konto über **Anderes Konto** trotzdem einrichten.

Im Normalfall erkennt die Mail-App anhand Ihrer Angaben automatisch den Mail-Anbieter und damit die benötigten Servereinstellungen. Das liegt an der so genannten Auto-Konfiguration: Die App fragt beim



Windows 10-Report Ausgabe 19/09

Mitlesen, mitreden.

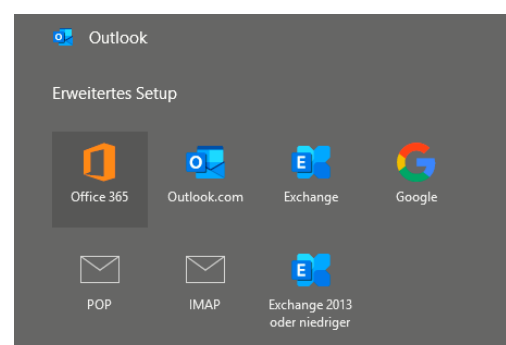
Mailserver an, und der schickt ihr die Konfigurationsinformationen zurück. Wenn Sie aber eine eigene Domain benutzen, dann funktioniert das nicht. Klicken Sie in diesem Fall solange auf **Anmelden**, bis die App aufgibt. Sie zeigt Ihnen dann eine umfangreiche Liste an benötigten Informationen an, neben dem **Benutzernamen** und **Kennwort** unter anderem **Kontotyp**, **Posteingangsserver** und **Postausgangsserver**. Nachdem Sie diese Daten korrekt eingegeben haben, können Sie Mails über dieses Konto senden

und empfangen. Schließen Sie den Einrichtungsdialog. Sie gelangen dann direkt ins Postfach.

Microsoft Outlook

Die Informationen, die Outlook benötigt, sind genau die selben wie bei der Mail-App von Windows 10. Nur der Weg dahin ist ein wenig anders.

Klicken Sie auf **Datei** > **Informationen** > **+ Konto hinzufügen**. Geben Sie wieder Ihre E-Mail-Adresse ein. Kann Outlook die benötigten Daten automatisch finden, dann müssen Sie außer einer



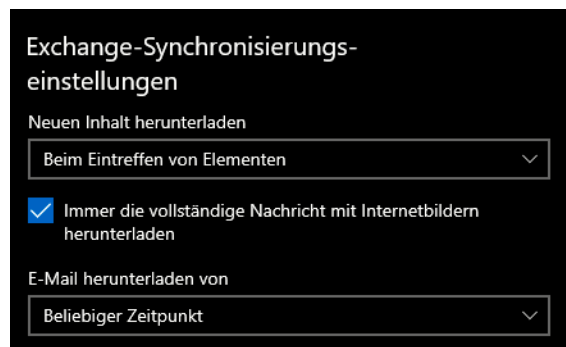
Windows 10-Report Ausgabe 19/09

Mitlesen, mitreden.

Passwortangabe nichts weiter machen. Funktioniert das nicht, dann zeigt Ihnen Outlook das Erweiterte Setup an, das von der Funktionsweise vergleichbar zu dem der Mail-App ist.

Einstellen des Abrufintervalls

Die Mail-Programme unter Windows 10 sind sparsam: Sie gehen nicht davon aus, dass Sie alle Ihre Mails mitnehmen möchten: Meist werden nur die letzten 2 bis 12 Wochen abgerufen. Das ist ungünstig, wenn Sie ohne Internet-Verbindung unterwegs sind und alte E-Mails lesen müssen. Darauf sollten Sie zumindest einen kritischen Blick richten.



In der Windows 10 Mail-App klicken Sie in den Einstellungen auf **Konten verwalten** und wählen dann das Postfach aus. Dort finden Sie den Eintrag **Postfachsynchronisierungseinstellungen ändern**. Unter **E-Mail herunterladen von** können Sie verschiedene Zeiträume auswählen. Um alle Mails, die im Postfach vorhanden sind, zu synchronisieren, klicken Sie auf **Beliebiger Zeitpunkt**.

Bei Outlook funktioniert es ähnlich: Hier finden Sie die Einstellungen unter **Datei > Informationen > Kontoeinstellungen > Kontoname und Synchronisierungseinstellungen**.

Windows 10-Report Ausgabe 19/09

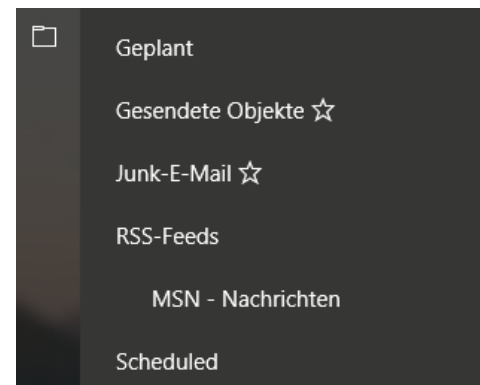
Mitlesen, mitreden.

Werbung und verlorene E-Mails

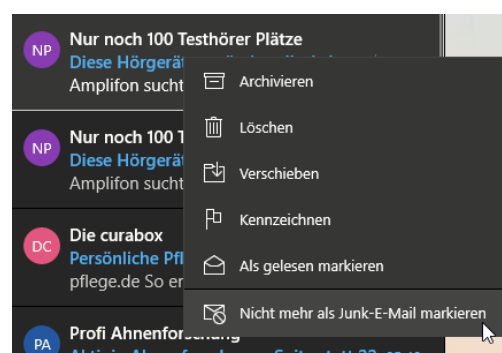
Die Kommunikation via E-Mail ist darauf ausgelegt, dass Sie sich als Benutzer darauf verlassen können. Sie schicken eine E-Mail, die kommt beim Empfänger an, und genauso soll es in die andere Richtung funktionieren. Leider machen Ihnen da nicht selten die Werbe-E-mails und die automatischen Reaktionen der Mail-Programme darauf einen Strich durch die Rechnung.

SPAM-Ordner und Junk-Email

Jeder Mail-Anbieter hat mittlerweile einen eigenen Filter für SPAM-E-Mails. Auf Grund verschiedener Regeln werden E-Mails, die als unerwünschte Werbung erkannt werden, dort eingeordnet. Nun ist nicht jede Regel perfekt und fehlerfrei, insofern kann es durchaus passieren, dass „echte“ E-Mails dort landen.



Suchen Sie sich in Ihrem Mail-Programm den SPAM-Ordner heraus. Der kann Werbung, Junk-E-Mail, SPAM etc. heißen. Durch einen Klick mit der rechten Maustaste auf den Ordner können Sie ihn zu den Favoriten hinzufügen. Damit ist er immer im oberen Teil der Ordner



sichtbar und schnell im Zugriff. Schauen Sie regelmäßig hinein!

Sie können die Erkennung von Werbung verbessern, wenn Sie selbst falsch klassifizierte E-Mails markieren. Klicken Sie mit der rechten Maustaste auf eine E-Mail,

Windows 10-Report Ausgabe 19/09

Mitlesen, mitreden.

uns wählen Sie entweder **Als Junk-E-Mail markieren** oder **Nicht mehr als Junk-E-Mail markieren**. Bei der nächsten E-Mail behandelt die Mail-App sie anders, bei Outlook funktioniert das genauso,

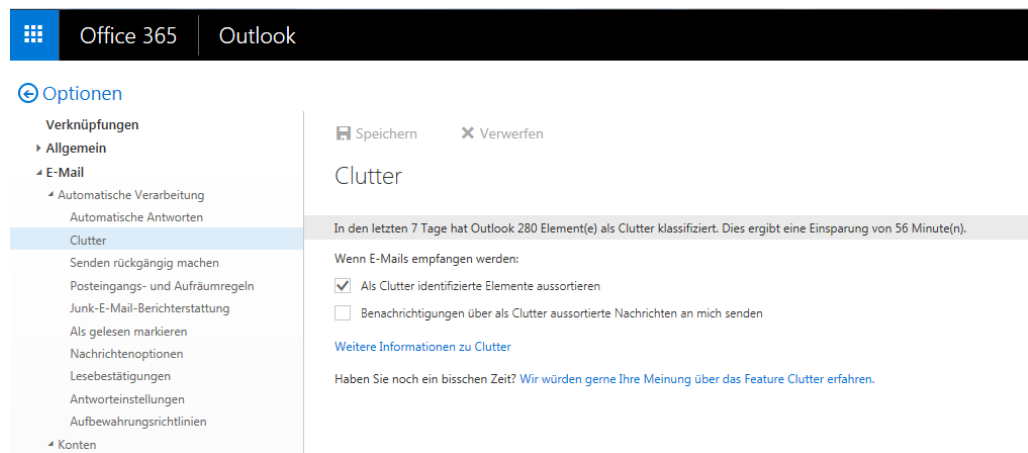
Intelligenter SPAM-Filter in Office 365: Clutter

Clutter ist die intelligente Version des Junk Email-Ordners, die mit Office 365 eingeführt wurde. Der große Unterschied: Clutter lernt hinzu und bewertet eingehende E-Mails nach ihrer Wichtigkeit für den Benutzer. Eine Mail mit einem bestimmten Titel oder Absender, die regelmäßig ungeöffnet gelöscht wird, kann dem Anwender nicht wichtig sein. Je länger Clutter aktiv genutzt wird, desto genauer wird die Erkennung, und für den Anwender verringert sich die Mailflut und damit die Zahl der Ablenkungen während der Arbeit am PC (oder mit dem Smartphone in der Freizeit). Der Aufwand, in regelmäßigen Abständen den Clutter-Ordner zu kontrollieren, ist vergleichsweise gering, da die Erkennung wirklich hervorragend funktioniert.

Was aber, wenn plötzlich wieder alle - also auch die unerwünschten - Mails in den Posteingang kommen? Im Outlook am PC oder am mobilen Gerät lässt sich Clutter nicht aktivieren? Hier muss das Office 365 Webfrontend her: nach Anmeldung unter <http://outlook.office365.com> führt ein Klick auf das Zahnrad und dann auf "E-Mail" unter "Ihre App-Einstellungen" in den Einrichtungsbildschirm. Dort findet sich unter "E-Mail", "Automatische Verarbeitung", "Clutter" der entsprechende Einrichtungsdialog.

Windows 10-Report Ausgabe 19/09

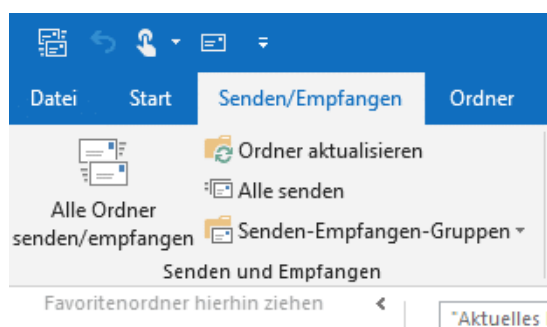
Mitlesen, mitreden.



Ist Clutter nicht aktiv, dann fehlt der Haken neben "Als Clutter identifizierte Elemente aussortieren". Wird dieser gesetzt, dann ist Clutter wieder aktiv und steuert die unerwünschten E-Mails aus. Der Clutter-Ordner liegt auf dem Mail-Server. Das bedeutet, dass Sie ihn sowohl mit der Windows 10 Mail-App als auch mit jedem anderen E-Mail-Programm nutzen können.

Wenn keine Mails mehr ankommen

Wenn Sie auf die Kommunikation per E-Mail angewiesen sind, dann



verlassen Sie sich darauf, dass der Empfang und Versand einwandfrei funktioniert. Das ist normalerweise auch so.

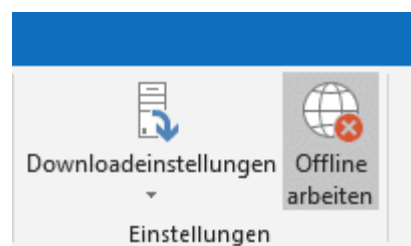
Allerdings gibt es einige Fehlerursachen, die Ihnen den reibungslosen Ablauf der

Kommunikation vermiesen können. Kein Problem, wenn Sie sie kennen und kontrollieren können.

Windows 10-Report Ausgabe 19/09

Mitlesen, mitreden.

In manchen Situationen kann es vorkommen, dass Outlook die Verbindung zum Mailserver getrennt hat. Das erkennen Sie unten in der Statuszeile von Outlook an dem Symbol **Offlinemodus**. Um wieder online zu gehen, klicken Sie auf **Senden/Empfangen > Offline arbeiten**, um den Offline-Modus zu deaktivieren. Die Windows 10 Mail-App bietet diese Funktion leider nicht. Das hilft nur das Beenden und Neustart der App.



Eine weitere Ursache ist eine Störung im Maildienst des Anbieters. Wenn alle anderen Tipps nicht helfen, dann melden Sie sich auf der Webseite des Mailanbieters an. Wenn das schon nicht geht, ist definitiv eine Störung vorhanden. In einem solchen Fall bleibt Ihnen nicht viel anderes übrig, als abzuwarten.

Mailblockaden durch SPAM-Listen

Die SPAM-Behandlung auf dem eigenen PC ist hilfreich, weil Sie Ihnen eine Menge an Kontrolle gibt. Die Mail-Anbieter selbst plagt aber eine ganz andere Herausforderung: SPAM kommt ja irgendwo her. Meist von verseuchten Rechnern, die (Zehn-) Tausende E-Mails in einem Rutsch verschicken. Ist das der Fall, dann kann es schnell passieren, dass ein Mailserver gesperrt wird. Auch wenn nicht nur der Spammer, sondern auch normale Anwender diesen nutzen.

Die Folge: Mails dieses Servers werden einfach blockiert, bevor sie überhaupt in Ihr Postfach gelangen. Übertragen: Der Briefträger bekommt die Werbung gar nicht, sondern sie wird bereits im Verteilzentrum weggeworfen.

Windows 10-Report Ausgabe 19/09

Mitlesen, mitreden.

Das hat Auswirkungen in zwei Richtungen: Sie bekommen bestimmte E-Mails nicht mehr und beschwerten sich beim Absender. Der aber kann das nicht nachvollziehen. Im besten Fall bekommt er eine Fehlermeldung, im schlechtesten gar keine Information.

This message was created automatically by mail delivery software.

A message that you sent could not be delivered to one or more of its recipients. This is a permanent error. The following address(es) failed:

andreas@aerle.net:

SMTP error from remote server for RCPT TO command, host: aerle-net.mail.protection.outlook.com (104.47.0.36) reason: 550 5.7.1 Service unavailable, Client host [82.165.159.36] blocked using Spamhaus. To request removal from this list see <https://www.spamhaus.org/query/ip/82.165.159.36> (AS16012611) [HE1EUR01FT029.eop-EURO1.prod.protection.outlook.com]

Gerade beim automatisierten E-Mail-Versand, zum Beispiel bei abonnierten Newslettern, erkennen die versendenden Systeme, dass

wiederholte Fehler auftreten. Nach einer gewissen Zeit werden die betroffenen E-Mail-Adressen automatisch entfernt. Wenn die Blockade des Mailservers dann irgendwann aufgehoben ist, sind Sie automatisch aus dem Verteiler rausgefallen.

Wir versuchen Ihnen immer gleich die Lösungen mitzuliefern. In diesem Fall aber haben Sie als Empfänger leider keine Einflussmöglichkeit.

Einzig eine Möglichkeit zur Identifikation des Problems können wir Ihnen bieten: Es gibt verschiedene Anbieter von SPAM-Blockierungslisten, einer davon ist [SPAMHaus.org](https://www.spamhaus.org). Dort können Sie den Namen oder die IP Ihres Mailservers eingeben und bekommen die Information, ob dieser gesperrt ist. Ist das der Fall,

Blocklist Removal Center

Blocklist Lookup Results

194.25.134.18 is not listed in the SBL

194.25.134.18 is not listed in the PBL

194.25.134.18 is not listed in the XBL

► **Not Listed.** If the IP address or domain you are checking does not show as listed in the results above, then it is not currently in any Spamhaus blocklist. If you are getting email reject messages which say it is listed by a Spamhaus blocklist, then see [this FAQ](#) for a possible solution.

► **Listed.** If the IP address or domain you are checking is listed in any of our blocklists above, this page will tell you which one(s) and will give you a link to the exact record. Follow the link. The linked page will explain why the address is listed and what to do to have it removed.

dann können Sie über das Meldeformular einen Antrag auf Entsperren stellen. Ob und wann eine Reaktion darauf erfolgt, ist vollkommen ungewiss.

Tipp Ein schon länger existierendes Problem besteht zwischen Microsofts Outlook und T-Online. Outlook erkennt Mailserver von T-Online als SPAM-Schleudern und blockiert diese. Die betroffenen Anwender wundern sich über ausbleibende E-Mails. Beide Unternehmen allerdings lassen relativ wenig Motivation erkennen, das Problem zu lösen. Der Leidtragende ist einmal mehr der Anwender.

Praxistipps zur Zeitersparnis

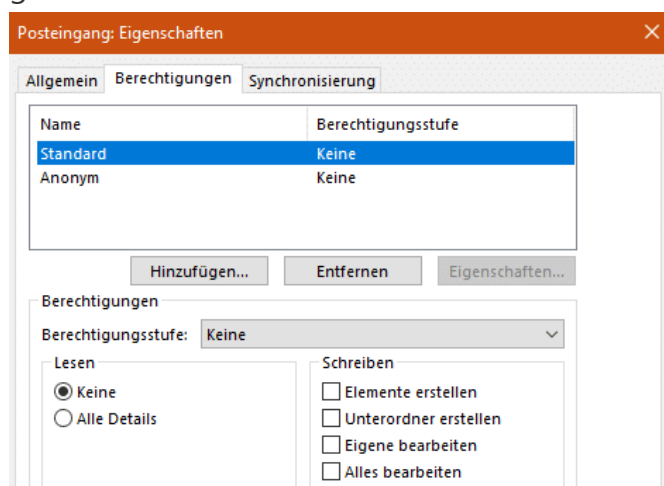
Senden einer E-Mail von einem anderen Konto

Der Mailverkehr im eigenen Namen ist vollkommen unkompliziert. Sie schreiben die E-Mail, und das Mailprogramm trägt Sie als Absender ein. Das funktioniert automatisch aus den Informationen, die in Ihrem E-Mail-Konto hinterlegt sind. Und so ist auch bei Antworten automatisch Ihre E-Mail-Adresse als Empfänger hinterlegt. Was aber, wenn Sie im Namen eines anderen Benutzers schreiben müssen? Beispielsweise, wenn Sie einen Kollegen vertreten müssen, die Antworten aber an Sie

Windows 10-Report Ausgabe 19/09

Mitlesen, mitreden.

gehen sollen. Kein Problem in Outlook!



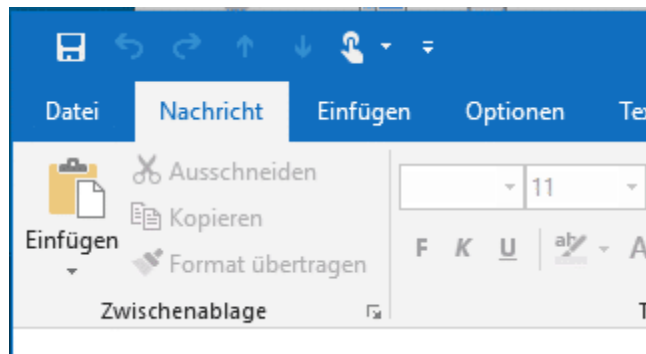
Die Voraussetzung ist, dass der Kollege Ihnen Berechtigungen auf sein Postfach eingerichtet hat. Das geht recht einfach: Klicken Sie mit der rechten Maustaste auf den freizugebenden Ordner (z.B. den Posteingang), dann auf Eigenschaften > Berechtigungen. Über Hinzufügen kann dann ein Benutzer hinzugefügt werden. Unten können Sie ganz fein auswählen, welche Rechte der hinzugefügte Nutzer auf dem Postfach haben soll. Für die Stellvertretung muss das Erstellen von Elementen aktiviert sein.

Wenn Sie nun im Namen des Kollegen eine E-Mail schreiben wollen, dann klicken Sie einmalig in einer neuen E-Mail auf **Optionen** > **Von**. Wählen Sie dann das freigegebene Postfach aus. In der Mail finden Sie nun über den Adressangaben der E-Mail ein zusätzliches Auswahlfeld für das Postfach, von dem die E-Mail abgeschickt wird. Für den Empfänger sieht die E-Mail genau so aus, als hätte der Vertretene diese selbst geschickt.

Windows 10-Report Ausgabe 19/09

Mitlesen, mitreden.

Wenn Mails nur noch grau und unformatiert sind

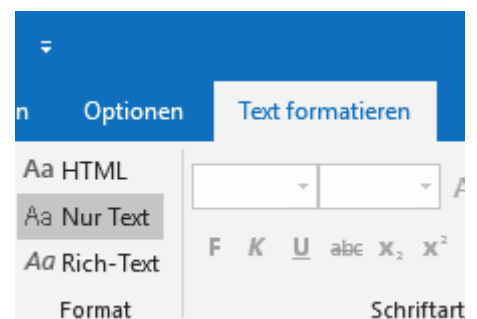


Mails leben nicht nur von dem Text, sondern vor allem auch von Formatierungen und Bildern. Mit Outlook als E-Mail-Client können Sie im Normalfall, wie mit einer kleinen

Textverarbeitung den Text zu gestalten. Wenn die entsprechenden Schaltflächen in einer neuen E-Mail aber ausgegraut sind, dann ist guter Rat teuer. Keine Sorge: das bekommen Sie schnell in den Griff!

Das Problem liegt meist in der Formatierung der E-Mail. Normalerweise sollte diese direkt als HTML (das Format von Internetseiten) oder RTF (Das Rich Text Format von Word) angelegt werden. Dann können Sie frei Formatierungen und Multimedia-Elemente in den Text integrieren. Bekommen Sie aber eine E-Mail, die vom Absender im reinen Textformat geschickt wurde, dann wird die Antwort automatisch auch als Text-E-Mail angelegt.

Die Lösung ist relativ einfach: Gehen Sie in der E-Mail auf **Text formatieren**, dann wählen Sie unter Format **HTML** oder **Rich-Text** aus. Die E-Mail wird automatisch umgewandelt und Sie können Sie ab sofort nach Wunsch formatieren.



Wenn neu angelegte E-Mails immer erst einmal im Text-Format sind, dann sollten Sie die Voreinstellungen ändern: Klicken Sie im Outlook Hauptfenster auf **Datei > Optionen > E-Mail** und wählen Sie unter

Windows 10-Report Ausgabe 19/09

Mitlesen, mitreden.

Nachrichten verfassen die Option **Nachrichten in diesem Format verfassen** > **HTML** aus. Jede neue E-Mail wird nun als HTML-Mail angelegt. Sollte der E-Mail-Client des Empfängers damit nicht umgehen können, dann werden Bilder als Anhang angezeigt und die Formatierungen gehen verloren. Lesbar ist der Inhalt aber immer noch.



Ändern Sie die Einstellungen für von Ihnen erstellte und empfangene Nachrichten.

Nachrichten verfassen



Ändern Sie die Bearbeitungseinstellungen für Nachrichten.

Nachricht in diesem Format verfassen: HTML



Vor dem Senden immer die Rechtschreibung prüfen

Rechtschre

Originalnachricht bei Antworten und Weiterleitungen ignorieren



Erstellen oder ändern Sie Signaturen für Nachrichten.



Verwenden Sie Briefpapier, um Standardschriftart und Formatvorlagen sowie Farben und Hintergründe zu ändern.

Br

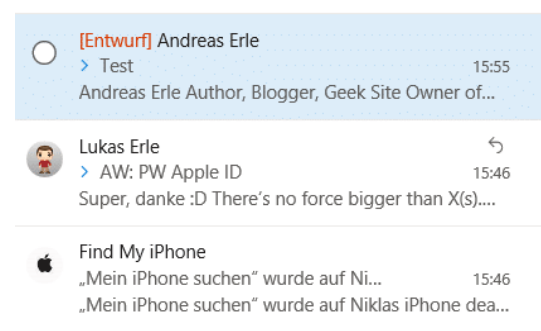
Auffinden verlorenen Entwürfe in Outlook

Schnell reagieren Sie auf eine neue E-Mail, obwohl Sie gerade noch eine andere schreiben. Idealerweise wird die unterbrochene E-Mail dann unter **Entwürfe** gespeichert. Manchmal aber sehen Sie in der Übersicht im Posteingang "[Entwurf]", aber kommen an den Mailentwurf selbst nicht mehr heran. Keine Sorge, dieser ist nicht verschollen, sondern lässt sich schnell wieder auffinden.

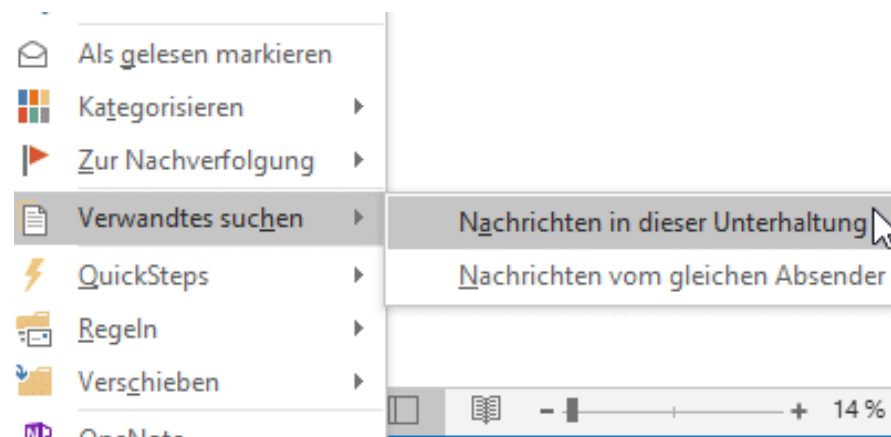
Windows 10-Report Ausgabe 19/09

Mitlesen, mitreden.

In einem solchen Fall hat Outlook den Entwurf nicht separat in dem Ordner Entwürfe gespeichert, sondern in den Mailverlauf eingebettet. Gehen Sie auf eine der E-Mails, die zu diesem Gesprächsverlauf gehören. Dazu klappen Sie diesen durch einen Klick auf das Dreieck neben dem Betreff auf.



Outlook öffnet ein Kontextmenü. Klicken Sie darin auf **Verwandtes suchen > Nachrichten in dieser Unterhaltung**. Outlook sucht nun in allen Mail-Ordern nach Nachrichten, die den entsprechenden Betreff haben, und zeigt Ihnen die Suchergebnisse in einer Liste an.



In dieser Liste finden Sie auch den Entwurf der E-Mail, die Sie gerade bearbeitet haben. Doppelklicken Sie auf diesen, um ihn als separate E-Mail zu öffnen. Sie können nun nach Herzenslust weiterschreiben und die fertige E-Mail dann verschicken.

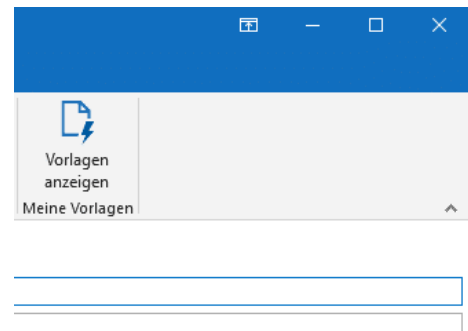
Windows 10-Report Ausgabe 19/09

Mitlesen, mitreden.

Antworten in vordefinierten Formularen in Outlook

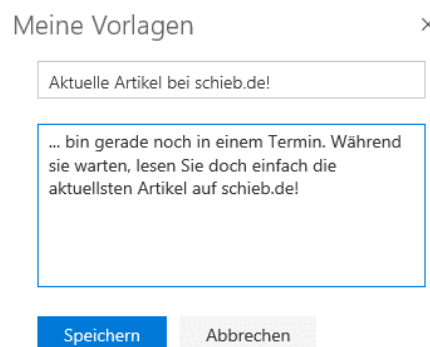
Wenn Sie eine E-Mail bekommen, dann ist es oft dieselbe E-Mail, die Sie als schnelle Antwort verschicken wollen. Diese immer wieder neu zu schreiben und abzuschicken, ist viel zu viel Aufwand. Auch eine Textdatei vorzuhalten, die die Standard-Antworten enthält, macht wenig Sinn. Outlook 365 bietet im Standard die Möglichkeit, auf Standard-Vorlagen zuzugreifen und eigene anzulegen.

Im Menüband finden Sie einen Button Vorlagen anzeigen, wenn Sie eine neue, leere E-Mail öffnen. Klicken Sie darauf, dann bekommen Sie erst einmal die Standard-Vorlagen für Verspätungen und Verzögerungen angezeigt.



Wählen Sie eine der Vorlagen aus, um diese in die E-Mail einzufügen. Nun können Sie die E-Mail direkt an den oder die gewünschten Empfänger versenden.

Interessanter ist es, wenn Sie noch eigene Vorlagen anlegen. Klicken Sie dazu auf (+) Vorlage, um ein neues Template zu öffnen. Geben Sie der



Vorlage einen sprechenden Namen, sodass Sie sie aus der Liste später schnell identifizieren können. Geben Sie dann den Text der E-Mail in das Feld darunter ein.

Ein Klick auf Speichern fügt die neue Vorlage dann in die Liste der verfügbaren ein. Um nun eine Vorlage

Windows 10-Report Ausgabe 19/09

Mitlesen, mitreden.

zu verändern oder zu löschen, bewegen Sie den Mauszeiger über sie und klicken Sie dann auf die Mülltonne oder den Stift.

Erstellen eines E-Mail-Templates

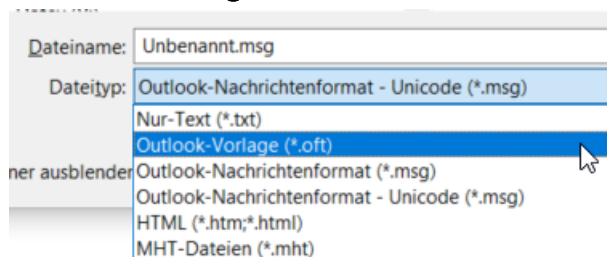
Neben standardisierten Antworten auf E-Mails werden Sie immer mal wieder neue E-Mails verschicken, die ähnlich sind. Beispielsweise die Einladung zu einem Termin, die bis auf Datum, Uhrzeit und vielleicht Ort genau gleich ist. Da ist es unnötiger Aufwand, diese immer wieder neu zu schreiben. Outlook kennt dafür die so genannten Templates, die Sie mit wenigen Schritten einrichten können.

Dazu legen Sie eine neue Email in Outlook an. Schreiben Sie den Inhalt einmal herunter. Dabei lassen Sie Platzhalter für die veränderlichen Angaben, z.B. indem Sie sie durch X ersetzen.

Hallo zusammen,
unser nächstes Treffen findet statt am xx.xx.xxxx. Wie gewohnt treffen wir uns um xx:xx Uhr im Restaurant „Schieb’s Braustübchen“.

Viele Grüße und bis dann,
Andreas

Statt die E-Mail dann abzuschicken, klicken Sie auf **Datei > Speichern unter**. Wählen Sie unter **Dateityp** statt des normalen Nachrichtenformats **Outlook-Vorlage** aus. Nachdem Sie der Vorlage nun einen sprechenden



Namen gegeben haben, speichern Sie sie.

Um nun diese Vorlage zu verwenden, klicken Sie in Outlook auf **Datei > Neue Elemente > Weitere Elemente > Formular**

auswählen. Wählen Sie unter **Suchen in:** ganz oben in der Formularauswahl **Vorlagen im Dateisystem**. In der sich nun öffnenden

Windows 10-Report Ausgabe 19/09

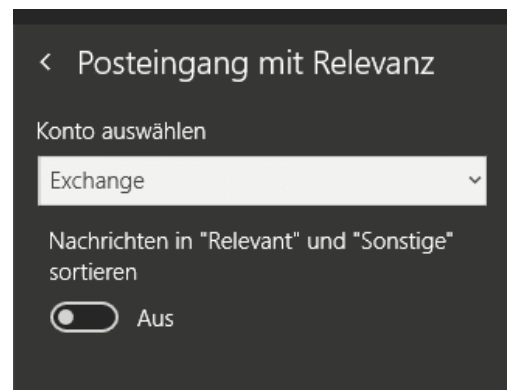
Mitlesen, mitreden.

Liste finden Sie alle Ihre Vorlagen und können die gewünschte auswählen.

Fokus auf das Wichtige: Focused Inbox

Sie nutzen vermutlich verschiedene Methoden, um sich auf die wirklich wichtigen Mails konzentrieren zu können. Dazu gehört ganz vorne die Nutzung der Junk-E-Mail- und Clutter-Ordner, die die Mail-Spreu vom Weizen trennen. Nach unterschiedlichen Regeln werden "echte" von Werbungs-E-Mails getrennt. Das ist aber noch nicht alles: Auch bei den tatsächlich an Sie gerichteten E-Mails sind einige wichtiger, andere weniger. Sowohl die Windows 10-interne Mail-App als auch Outlook unterstützen das.

Der so genannte Posteingang mit Relevanz (manchmal auch Englisch als Focused Inbox bezeichnet) ist vollkommen unabhängig von der Klassifizierung von SPAM. Es gibt E-Mails, die für Sie relevant sind, aber eben nicht vordringlich. Ein gutes Beispiel dafür: Der Newsletter. Sie haben ihn abonniert interessieren sich für die Inhalte. Er wird aber immer hinter wichtigen Mails zurückstehen. Sie lesen ihn dann, wenn Sie Zeit dafür erübrigen können.



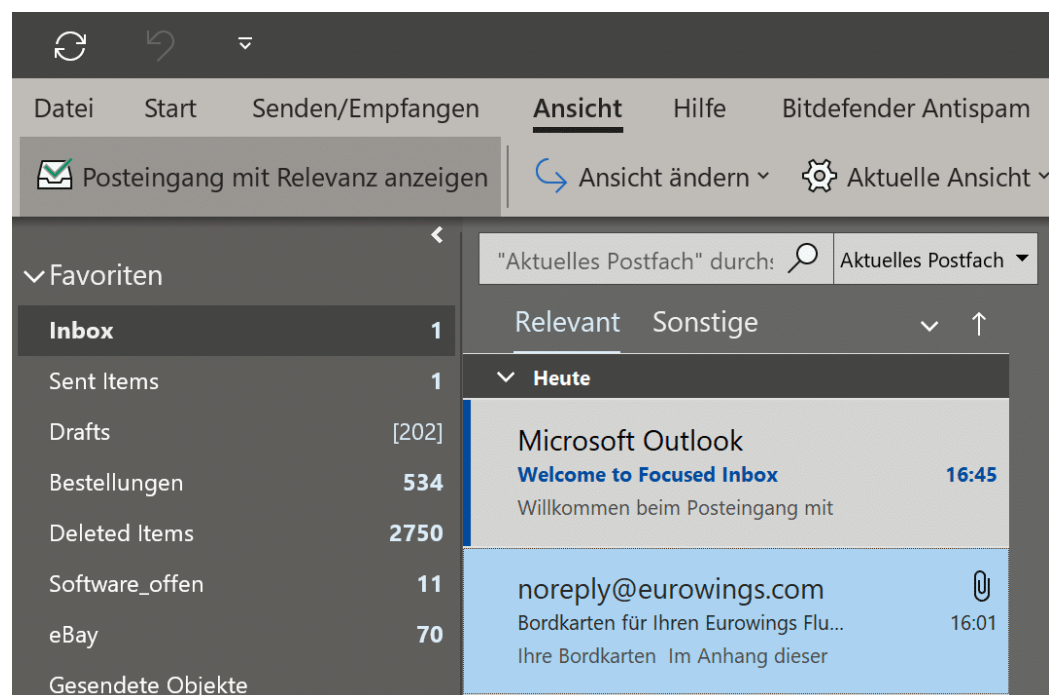
Genau hier setzt der Posteingang mit Relevanz an. Selbstlernend erkennt die Mail-App, welche Mails sie sofort öffnen und welche später irgendwann einmal. Erstere erscheinen unter **Relevant**, die anderen unter **Sonstige**. Ganz wichtig: Beide sind Bestandteil des Posteingangs!

Windows 10-Report Ausgabe 19/09

Mitlesen, mitreden.

Aktivieren oder deaktivieren können Sie diese Funktion in der Windows 10 Mail-App, wenn Sie in die Einstellungen gehen und dort auf **Posteingang mit Relevanz** klicken.

In Outlook versteckt der Posteingang mit Relevanz sich in der Registerkarte **Ansicht**. Dort können Sie ihn aktivieren wie auch später wieder deaktivieren.



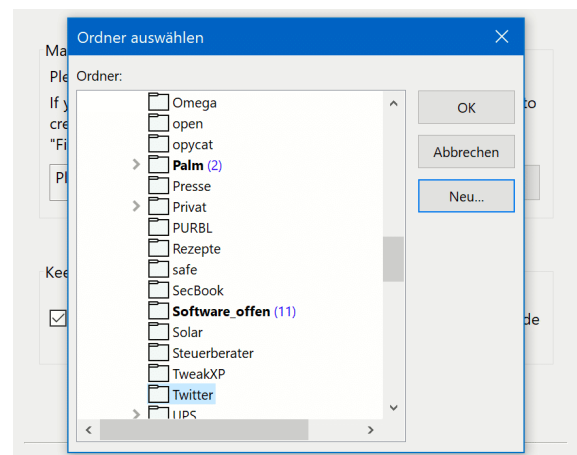
Integration von Twitter in Outlook

Outlook ist weit mehr als ein E-Mail-Programm. Neben dem Kalender und dem Adressbuch können Sie es um weitere Funktionalitäten erweitern. Das geht nicht nur über die Addins und Connectors, die Sie über Outlook selbst installieren können. Durch eine definierte Schnittstelle können Sie auch Erweiterungen von Fremdanbietern installieren. Beispielweise für die Integration von Twitter.

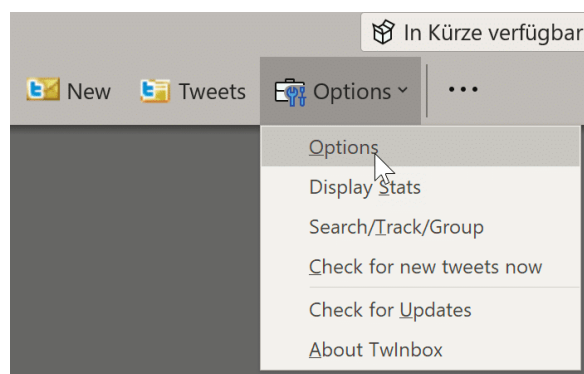
Windows 10-Report Ausgabe 19/09

Mitlesen, mitreden.

Twinbox (<https://www.techhit.com/TwInbox/quickstart.html?s=installer>) ist eine kostenlose App, die Ihr Twitter-Konto in Outlook integriert. Nicht als separates Plugin, sondern als Kombination aus Symbolleiste und Nachrichtenordner. Nach der Installation müssen Sie einen Ordner in Outlook auswählen oder anlegen. In diesen werden die Tweets gespeichert. Alternativ können Sie auch eine neue Datendatei nur für Twitter anlegen.



In Outlook erscheint eine neue Symbolleiste. Diese erlaubt den Zugriff auf die Timeline der abonnierten und auf die Mentions der eigenen Tweets. Einmalig müssen Sie unter **Options** Ihr Twitter-Konto verbinden. Danach können Sie unter Tweets direkt in den Twitter-Ordner springen.



Ein Klick auf **New** erlaubt es Ihnen, einen neuen Tweet von Ihrem Konto zu verfassen. Besonders schön dabei: Tweets stellt die App deutlich übersichtlicher dar als der Twitter-Client. Unter anderem sehen Sie direkt die

Informationen des postenden Kontos. Wenn Sie nun noch den Twitter-Ordner manuell zu den Favoriten hinzufügen, dann müssen Sie nicht einmal die Symbole des Programms nutzen.

E-Mail-Sicherheit

E-Mails sind nicht nur zur Kommunikation wichtig. Sie müssen sich bei vielen Online-Diensten mit Ihrer E-Mail-Adresse anmelden, die dann gleichzeitig der Benutzername wird. Ist Ihre E-Mail-Adresse kompromittiert, dann haben Sie eine Vielzahl von Problemen. Grund genug, alle Sicherheitsmaßnahmen zu ergreifen, die möglich sind. Zum einen sollten Sie sich Ihre Passwörter sehr genau überlegen. Zum anderen bieten Mailprogramme zusätzliche Sicherheitsmaßnahmen wie die Zwei-Faktor-Authentifizierung, bei der Sie neben dem Passwort noch ein zweites, regelmäßig wechselndes Kennwort benötigen.

Zugangsschutz: Anforderungen an Passwörter

Ohne zusätzliche Maßnahmen ist „nur“ das Passwort der wirklich geheime und geheim zu haltende Teil Ihrer Zugangsdaten zum Email-Konto und anderen Diensten. Grund genug, bei der Vergabe ein wenig Zeit zu investieren und ein möglichst sicheres Passwort zu vergeben!

Ist es schon zu spät?

Immer wieder kommen Datenlecks und -pannen in die Nachrichten: Durch Sicherheitsvorfälle werden E-Mail-Adressen, Nutzernamen und Passwörter gestohlen und im Internet verkauft. Der Käufer hat dann so lange theoretisch Zugriff auf all Ihre Benutzerkonten, wie Sie das Passwort nicht geändert haben.

Windows 10-Report Ausgabe 19/09

Mitlesen, mitreden.

Die bekanntesten Sicherheitsvorfälle (zumindest die, die bekannt geworden sind), sind auf der Seite <https://haveibeenpwned.com/> zusammengefasst. Dort können Sie nach Eingabe Ihres Passwortes sehen, ob und bei welchem Hack Ihre Zugangsdaten erbeutet wurden.

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

Adobe: In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, encrypted password and a password hint in plain text. The password cryptography was poorly done and many were quickly resolved back to plain text. The unencrypted hints also disclosed much about the passwords adding further to the risk that hundreds of millions of Adobe customers already faced.
Compromised data: Email addresses, Password hints, Passwords, Usernames

Anti Public Combo List (unverified): In December 2016, a huge list of email address and password pairs appeared in a "combo list" referred to as "Anti Public". The list contained 458 million unique email addresses, many with multiple different passwords hacked from various online systems. The list was broadly circulated and used for "credential stuffing", that is attackers employ it in an attempt to identify other online systems where the account owner had reused their password. For detailed background on this incident, read Password reuse, credential stuffing and another billion records in Have I been pwned.
Compromised data: Email addresses, Passwords

Dropbox: In mid-2012, Dropbox suffered a data breach which exposed the stored credentials of tens of millions of their customers. In August 2016, they forced password resets for customers they believed may be at risk. A large volume of data totalling over 68 million records was subsequently traded online and included email addresses and salted hashes of passwords (half of them SHA1, half of them crypt).
Compromised data: Email addresses, Passwords

Exploit.In (unverified): In late 2016, a huge list of email address and password pairs appeared in a "combo list" referred to as "Exploit.In". The list contained 593 million unique email addresses, many with multiple different passwords hacked from various online systems. The list was broadly circulated and used for "credential stuffing", that is attackers employ it in an attempt to identify other online systems where the account owner had reused their password. For detailed background on this incident, read Password reuse, credential stuffing and another billion records in Have I been pwned.

Wenn Sie betroffen sind, dann ändern Sie so schnell wie möglich das Passwort, und wiederholen Sie dies häufiger. Auch wenn Sie das nach dem Vorfall wissentlich oder unwissentlich schon gemacht haben: Besitzer der erbeuteten Daten wissen zumindest, dass die Benutzernamen und E-Mail-Adressen existieren und müssen sich so nur noch darauf konzentrieren, das Passwort herauszufinden.

Das sichere Passwort

Eigentlich ist der Begriff irreführend. Ein „sicheres“ Passwort ist ebenso theoretisch wie ein Perpetuum Mobile, denn mit genügend Rechenpower und Zeit lässt sich wohl jedes Passwort irgendwann herausfinden. Sie können den Aufwand aber zumindest so hochtreiben, dass die Wahrscheinlichkeit, dass das passiert, gegen Null geht.

Was ist nun ein sicheres Passwort? Das Bundesamt für Sicherheit in der Informationstechnik (BSI) gibt unter <https://www.bsi-fuer-buerger.de> im Bereich **PASSWORT** einige Hinweise:

1. **ES SOLLTE EINFACH ZU MERKEN SEIN:** Je schwerer ein Passwort zu merken ist, desto höher ist die Wahrscheinlichkeit, dass sie es sich

Windows 10-Report Ausgabe 19/09

Mitlesen, mitreden.

aufschreiben. Das widerspricht dem Anspruch, dass es nur Ihnen selbst bekannt sein soll. Das so beliebte kleine, gelbe PostIt als Zwischenspeicher ist eben nicht sicher!




 Bundesamt
für Sicherheit in der
Informationstechnik

LEICHTE SPRACHE GEBÄRDENSPRACHE KONTAKT Suchbegriff

BSI FÜR BÜRGER
ENS INTERNET - MIT SICHERHEIT

Risiken **Empfehlungen** Digitale Gesellschaft Service

Passwörter

Passwörter

Wer die Wahl hat, hat die Qual – heißt es. Besonders bei der **Wahl der richtigen Passwörter** tun sich viele Internetnutzer schwer. Wen wundert's da, dass schlecht gewählte Passwörter wie 123456 oder qwert auf der Hitliste besonders häufiger IT-Sicherheitsdefizite ganz weit oben stehen. Bei denen, die sich stattdessen die Mühe machen, ein etwas komplizierteres Passwort zu nutzen, kommt es nicht selten vor, dass ein und dasselbe Passwort für viele verschiedene Programme beziehungsweise Zugänge genutzt wird. Hacker freut das alles natürlich. Sie haben Werkzeuge, die vollautomatisch alle möglichen Zeichenkombinationen ausprobieren, ganze Wörterbücher einschließlich gängiger Kombinationen aus Worten und angefügten Zahlen testen oder einmal im Internet veröffentlichte Zugangsdaten bei allen möglichen Diensten durchprobieren. Um das zu verhindern, sollte ein Passwort bestimmte Qualitätsanforderungen erfüllen und immer nur für einen Zugang genutzt werden.

Hinzu kommt, dass Passwörter nicht nur zum Schutz von vertraulichen Daten dienen. Ein Beispiel: Inzwischen ist es üblich, dass man sich bei unterschiedlichsten Anbietern im Internet ein Konto oder einen Zugang (Account) anlegen kann. Die Anmeldung an diesem Account wird mit einem Passwort geschützt. Was könnte passieren, wenn sich jemand unter Ihrem Namen dort anmeldet? Wer möchte schon gerne, dass Fremde unter dem eigenen Namen E-Mails verschicken oder teure Waren im Internet ersteigern können?

Deshalb: Orientieren Sie sich an den folgenden Empfehlungen zur Erstellung und zum [Umgang mit Passwörtern](#) – und schon tun Sie etwas für Ihre Sicherheit.

Inhaltsverzeichnis

Umgang mit Passwörtern

Verwandte Themen

Online Banking

Bankgeschäfte online zu erledigen ist bequem und zugleich besonders sicherheitsrelevant.

2. **ES SOLLTE MINDESTENS 8 ZEICHEN HABEN:** Mehr (an Buchstaben) ist hier tatsächlich mehr (an Sicherheit). Bei den Passwörtern für Ihr WLAN werden gar 20 Zeichen empfohlen.
3. **NUTZEN SIE SONDERZEICHEN, GROß- UND KLEINSCHRIFT UND ZIFFERN:** Je komplexer das Passwort ist, desto schwerer ist er herauszubekommen. Wichtig dabei auch:
4. **VERWENDEN SIE KEINE ÜBER SIE BEKANNTEN ODER HERAUSZUFINDENDEN DATEN ALS PASSWORT:** Namen von Familienmitgliedern, Haustieren, Freunden, Geburtstage, Hochzeitstage etc. eignen sich nicht als Passwort. Auch keine Wörter, die in einem Wörterbuch

Windows 10-Report Ausgabe 19/09

Mitlesen, mitreden.

vorkommen, oder Zeichen- oder Ziffernfolgen, die auf- oder absteigend sind wie 123456 oder abcdef.

Verlieren Sie nicht den Mut: Diese Anforderungen lassen sich tatsächlich umsetzen.

Wichtig Passwörter aus dem Wörterbuch auszuwählen, ist keine gute Idee: So genannte Wörterbuch-Angriffe (Dictionary Attacks) sind nicht selten: Automatisiert wird der Benutzername immer wieder angemeldet, das Passwort wird eines nach dem anderen aus einem Wörterbuch genommen. Bei den heutigen Rechenkapazitäten ist es nur eine Frage der (kurzen) Zeit, bis das richtige Passwort erraten wäre!

Passwörter müssen nicht lesbar sein oder aus tatsächlich vorhandenen Begriffen bestehen, damit Sie sich daran erinnern können. Der Ausgangspunkt zu einem guten Passwort kann beispielsweise ein für Sie ganz persönlich leicht zu merkender Satz oder eine Zeile aus einem Lied. „Ich habe im Sommer 2018 den Motorradführerschein gemacht!“ beschreibt ein Ereignis, an das Sie sich sicherlich noch lange erinnern werden. Nehmen Sie davon nur die Anfangsbuchstaben (unter Beachtung der Groß- und Kleinschrift) und lassen Sie Ziffern und Satzzeichen an ihrem Platz, und schon haben Sie *IhIS2018dMg!* als Passwort. Dieses Passwort errät niemand, der nicht Ihren speziellen Satz kennt.

Verwendung eines Passwortgenerators

Eine weitere Möglichkeit ist die Verwendung eines Passwortgenerators, also eines Programms bzw. einer Webseite, die Ihnen nach bestimmten Vorgaben sicher Passwörter generiert. Kostenlos finden Sie dies beispielsweise unter <https://www.lastpass.com/de/password-generator>

Windows 10-Report Ausgabe 19/09

Mitlesen, mitreden.

Wählen Sie gewünschte **PASSWORTLÄNGE** ein, wählen Sie ob **GROßBUCHSTABEN**, **KLEINBUCHSTABEN**, **ZIFFERN** und/oder **SONDERZEICHEN** verwendet werden sollen. Auf Wunsch können Sie dann das Passwort noch für das Lesen oder Sprechen optimieren, diese Einstellungen beeinflussen die Verwendung von Sonderzeichen bzw. leicht verwechselbaren Zeichen im Passwort.

PASSWORTGENERATOR

Sicheres Passwort erstellen

Verwenden Sie unseren Online-Passwortgenerator, um sofort ein sicheres, zufälliges Passwort zu erstellen.

MqK^#MZa

Passwort anpassen

Passwortlänge

8

Einfach auszusprechen Großbuchstaben

Einfach zu lesen Kleinbuchstaben

Alle Zeichen Ziffern

Sonderzeichen

Passwort kopieren

Aus LastPass können Sie das Kennwort dann über das Symbol mit den beiden Seiten oben rechts in die **ZWISCHENABLAGE** kopieren und vor dort aus weiterverwenden.

Speichern von Passwörtern in einem Safe

Es bedarf keiner langen Erklärung, dass das Aufschreiben von Passwörtern keine wirklich gute Idee ist. Auch wenn es kaum zu glauben ist: Viele erfolgreiche Angriffe auf Systeme kommen nicht über einen technischen Einbruch über das Internet oder interne Netzwerk, sondern

Windows 10-Report Ausgabe 19/09

Mitlesen, mitreden.

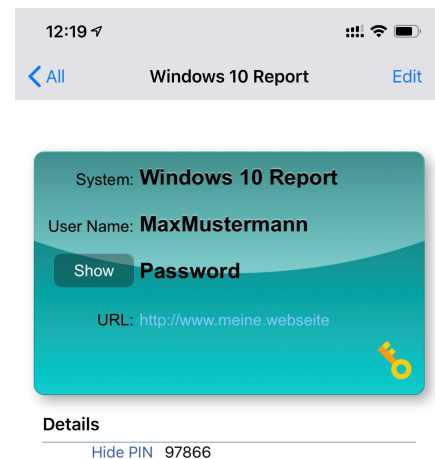
über kleine, gelbe Klebezettelchen, auf denen Anwender ihre Passwörter aufschreiben und „ganz geheim“ am Monitor oder unter der Schreibtischauflage verstecken. Auch eine Excel-Tabelle ist nur eine bedingt gute Idee!

Natürlich fordert der Anspruch, komplexe und unterschiedliche Passwörter zu verwenden und sich diese auch noch zu merken, aber auch dafür gibt es sichere Lösungen: Die so genannten Passwortsafes.

Dies sind Programme, in denen Sie Ihre Passwörter speichern können und die die Datei, in denen diese abgelegt werden, verschlüsselt und so vor unberechtigtem Zugriff schützt.

Bekanntere Passwort-Safes sind zum Beispiel 1Password (<https://1password.com>) und KeePass (<https://keepass.info>). Wenn Sie mit verschiedenen Plattformen auf Desktop, Tablet und Smartphone arbeiten, dann ist Iliums eWallet (<https://www.iliumsoft.com/>) eine gute Wahl.

eWallet bietet die Synchronisation der (256bit-verschlüsselten) Passwortdatei mit verschiedenen Online-Speichern an und hat für alle großen Plattformen (Windows, MacOS, iOS, Android) einen entsprechenden Client. Diese kosten zwar jeweils knapp EUR 10,-, lösen Ihnen aber die Herausforderung, dass Sie die Passwörter synchron halten und von überall her darauf zugreifen können. Eine einmal eingegebene Passwort-Karte ist nach Beendigung des Speichervorgangs sofort auf den anderen Geräten verfügbar, bei Änderungen verhält es sich ebenso.



Wenn Sie die Windows-Version von eWallet verwenden möchten, dann müssen Sie von der Ilium-Webseite die **Desktop-Version** herunterladen, nur diese ist mit den anderen Plattformen kompatibel. Die im Windows 10-Store verfügbare „eWalletGo“-App leider nicht: Sie verwendet ein eigenes Format und ist nicht für alle Systeme verfügbar!

Die Zwei-Faktor-Authentifizierung (2FA)

So gut und sicher sie ein Passwort auch entwerfen und speichern, es besteht immer noch die latente Gefahr, dass es jemand in Erfahrung bringt und verwenden kann. Die Idee der Zwei-Faktor-Authentifizierung (abgekürzt 2FA) ist die folgende: Wenn Sie sich mit dem Passwort angemeldet haben, wird noch ein weiteres Authentifizierungsmerkmal angefordert. Das kann ein Hardware-Token, sein, in vielen Fällen ist es eine sich in kurzen Zeitintervallen ändernde Nummer, die beispielsweise von einem Hardware-Stick abgelesen werden muss. Nur wer das Kennwort des Kontos und gleichzeitig die gerade aktuelle Nummer hat, der kann sich anmelden. Dem Unberechtigten wird – wenn der das Passwort entwendet hat – die zweite Nummer fehlen, und eine Anmeldung ist nicht möglich.



Microsoft stellt die Zwei-Faktor-Authentifizierung für die eigenen Online-Konten zur Verfügung. Statt eines Hardware-Schlüssels verwendet man einfach das, was Sie (fast) immer im Zugriff haben: Ihr Smartphone.

Windows 10-Report Ausgabe 19/09

Mitlesen, mitreden.

Aktivieren der Zwei-Faktor-Authentifizierung

Keine Frage: Ein zusätzlicher Schritt bei der Anmeldung bedeutet gleichzeitig, dass Sie länger für selbige brauchen, aus diesem Grund ist die Zwei-Faktor-Authentifizierung auch im Standard deaktiviert.




Um sie für Ihr Microsoft-Konto zu aktivieren, wechseln Sie zur Microsoft Konto-Sicherheitsseite <https://account.microsoft.com/security> und melden sich mit Ihrer E-Mail-Adresse und Ihrem Passwort an.

Microsoft | Konto Ihre Informationen Datenschutz Sicherheit Rewards Mehr ▾

Suche 🗉 Andreas 🧑

Grundlegendes zur Sicherheit

Erhöhen Sie die Sicherheit Ihres Kontos.

| | | |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Ändern des Kennworts</p>  <p>Verwenden Sie ein sichereres Kennwort oder ändern sie es, wenn Sie vermuten, dass eine andere Person es kennt.</p> <p>Kennwort ändern ></p> | <p>Aktualisieren Sie Ihre Sicherheitsinformationen</p>  <p>Stellen Sie sicher, dass Ihre Informationen auf dem neuesten Stand sind. So können Sie nachweisen, wer Sie sind, falls Sie einmal Ihr Kennwort vergessen haben.</p> <p>INFO AKTUALISIEREN ></p> | <p>Letzte Aktivität überprüfen</p>  <p>Prüfen Sie, wann und wo Sie sich angemeldet haben, und lassen Sie uns wissen, wenn etwas ungewöhnlich aussieht.</p> <p>Aktivität überprüfen ></p> |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Fertig mit den Grundlagen? Erkunden Sie [weitere Sicherheitsoptionen](#), um die Sicherheit Ihres Kontos zu gewährleisten.

Klicken Sie dann auf **WEITERE SICHERHEITSOPTIONEN** am unteren Rand der Seite und auf **ZWEISTUFIGE ÜBERPRÜFUNG EINRICHTEN**. Sie werden nun durch die Einrichtung geführt.

An deren Ende empfiehlt Ihnen Microsoft den Download der eigenen „Authenticator“-App. Diese finden Sie kostenlos im App Store (für iOS-Geräte) oder im Google Play Store (für Android-Geräte).

Fügen Sie Ihr Microsoft-Konto durch Tippen auf das Plus-Zeichen hinzu und melden Sie sich mit Ihrer E-Mail-Adresse und dem Passwort an.

Windows 10-Report Ausgabe 19/09

Mitlesen, mitreden.

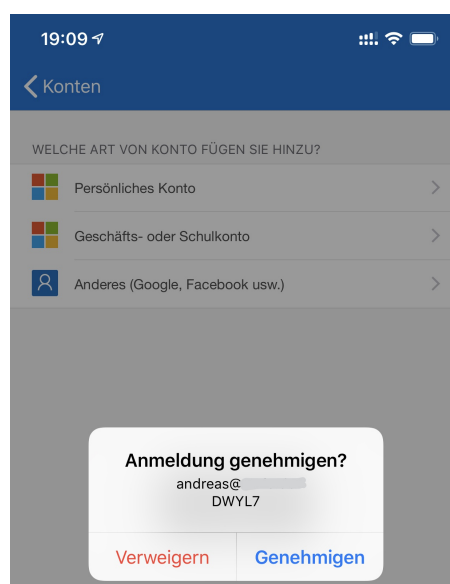
Nachdem der Vorgang erfolgreich abgeschlossen wurde, bekommen Sie – soweit Sie in der App einmal auf Nachfrage die Berechtigung erteilen, Push-Nachrichten zu versenden – bei jeder Anmeldung am Konto die Anforderung auf dem Smartphone, diese zu genehmigen.

Bei Smartphones mit biometrischem Zugangsschutz wie einem Fingerabdrucksensor oder einer 3D-Kamera muss die Genehmigung selbst dann sogar noch darüber freigegeben werden. Mehr Schutz geht (für den Privatanwender) kaum!

Bei Office 365 ist die Aktivierung ein wenig anders: Melden Sie sich als Administrator an Office 365 an und gehen Sie dann auf **BENUTZER**, klicken Sie den Benutzer, der die Zwei-Faktor-Authentifizierung bekommen soll, an. Ganz unten auf der Seite finden sie unter **WEITERE EINSTELLUNGEN** den Link zu **MULTI-FACTOR AUTHENTICATION VERWENDEN**.

Rechts auf dem Bildschirm finden Sie dann den Link zum **AKTIVIEREN** der Einstellung. Damit ist die Zwei-Faktor-Authentifizierung eingerichtet, aber nicht aktiviert. Im Gegensatz zum „normalen“ Microsoft-Konto kann bei Office 365 neben der Authenticator-App auch ein Anruf oder eine SMS als zweiter Faktor verwendet werden, sie Auswahl liegt dann beim Benutzer selbst.

Bei der ersten Anmeldung des Benutzers meldet Office 365 dann auch, dass noch weitere Informationen nötig sind. Klicken Sie dann einfach auf **WEITER**.



Windows 10-Report Ausgabe 19/09

Mitlesen, mitreden.



Zusätzliche Sicherheitsüberprüfung

Sichern Sie Ihr Konto durch Hinzufügen von Telefonüberprüfung zu Ihrem Kennwort. [Video](#)

Schritt 1: Auf welchem Weg sollen wir Sie kontaktieren?

| | |
|---------------------------|--|
| Authentifizierungstelefon | |
| Telefon (geschäftlich) | |
| Mobile App | |

Methode

Code per SMS an mich senden

Rückruf

Im folgenden Dialog können Sie auswählen, ob Sie telefonisch kontaktiert werden möchten (dazu müssen Sie dann Ländervorwahl und Rufnummer eingeben) oder die oben schon beschriebene **MOBILE APP**.

Wählen Sie diese Option aus. Sie müssen sich nun entscheiden, ob sie immer einen **PRÜFCODE** (den die App Ihnen dann anzeigt) eingeben möchten oder über eine **PUSH-BENACHRICHTIGUNG** die Anmeldung bestätigen möchten.

Wie möchten Sie die mobile App verwenden?

Benachrichtigungen zur Überprüfung empfangen

Prüfcode verwenden

Um diese Überprüfungsmethoden zu verwenden, müssen Sie die Microsoft Authenticator-App einrichten.

[Einrichten](#)

Konfigurieren Sie die mobile App.

Windows 10-Report Ausgabe 19/09

Mitlesen, mitreden.

Die zweite Variante ist hier die deutlich komfortablere, weil sie nur einen Klick erfordert statt der Eingabe einer Ziffernkette. Klicken Sie dann auf **EINRICHTEN**. Im Gegensatz zur Authentifizierung eines Microsoft-Kontos müssen Sie sie beim Hinzufügen in der Authenticator-App nicht mit Ihren Zugangsdaten anmelden, sondern benötigen einen Code und eine Web-Adresse, die die Webseite Ihnen nun unter dem QR-Code anzeigt.

Mobile App konfigurieren

Führen Sie die nachfolgenden Schritte aus, um die mobile App zu konfigurieren.

1. Installieren Sie die Microsoft Authenticator-App für [Windows Phone](#), [Android](#) oder [iOS](#).
2. Fügen Sie in der App ein Konto hinzu, und wählen Sie "Geschäfts, Schul- oder Unikonto" aus.
3. Scannen Sie das nachfolgende Bild.



Wenn Sie das Bild nicht scannen können, geben Sie die nachfolgenden Informationen in Ihrer App ein.

Code: 786 416 632

URL: <https://co1pfpad04.phonefactor.net/pad/802807894>

Wenn in der App ein sechsstelliger Code angezeigt wird, wählen Sie "Weiter" aus.

In der Authenticator-App tippen Sie auf das **+**, um ein neues Konto anzulegen, und dann auf **GESCHÄFTS- ODER SCHULKONTO**. Geben Sie nun Code und URL aus der Admin-Oberfläche von Office 365 ein und klicken Sie auf **WEITER**. Die App und Ihr Office 365-Konto synchronisieren sich nun miteinander. Bei jeder Anmeldung an Ihr Konto müssen Sie nun neben dem Passwort auch noch (je nach Konfiguration) einen Code eingeben oder die Anmeldung über Ihr Handy bestätigen.

Windows 10-Report Ausgabe 19/09

Mitlesen, mitreden.

Nutzen der 2FA in Outlook

Die Zwei-Faktor-Authentifizierung funktioniert wunderbar, wenn der Zugriff über den Webbrowser stattfindet. Greifen Sie aber mit einem Programm auf das Postfach zu, dann kann das Vorgehen von Programm zu Programm abweichen. In der Summe gibt es zwei Möglichkeiten:

Abfrage von Passwort und Authentifizierungscode

Im idealen Fall ist Ihre E-Mail-Software in der Lage, mit der Anforderung eines zweiten Faktors direkt umzugehen und sie zu verarbeiten. Outlook 2016 und 365 wie auch die interne E-Mail-App gehören dazu. Bei den aktuellen Versionen von Windows

wird der Authentifizierungscode der App nur einmalig abgefragt. Direkt danach schaltet sich Windows Hello ein und fordert einmalig die Anmeldung über eine der in Windows hinterlegten Methoden (Wie Fingerabdruck, Gesicht oder Token) an. Wenn Sie die ausgeführt haben, dann wird Windows Hello bei jeder



[REDACTED] Anmeldung am Postfach als zweiter Faktor verwendet. Deutlich bequemer, als wenn Sie immer Codes eingeben müssen!

Ihr Microsoft-Konto für Hello aktivieren

Sie müssen Windows Hello verwenden, um das Hinzufügen von "worldofppc@outlook.de" abzuschließen.

Verwendung von App-Kennwörtern

Ältere Versionen von Outlook, Smartphones und andere Programme, die nicht nativ den zweiten Faktor bei der Anmeldung anfordern können, werden ausgetrickst. Wechseln Sie wieder in die Sicherheitseinstellungen Ihres Microsoft-Kontos und klicken Sie auf

Windows 10-Report Ausgabe 19/09

Mitlesen, mitreden.

Zusätzliche Sicherheitsoptionen. Unter App-Kennwörter können Sie ein **zufälliges App-Kennwort** erzeugen, das aus einer Kombination aus Ihrem Passwort und einem zufälligen Code berechnet wird. Das ist weder lesbar noch von einem Fremden zu erraten.

Verwenden Sie dieses App-Kennwort zur Anmeldung

Geben Sie das App-Kennwort in das Kennwortfeld der App oder des Geräts ein, die bzw. das keine Sicherheitscodes unterstützen. [Diese Schritte ausführen](#).

App-Kennwort

ntmiqpsxgtbrrexy

Für jede App oder jedes Gerät, die bzw. das keine Sicherheitscodes unterstützt, müssen Sie stattdessen ein neues App-Kennwort erstellen. [Weiteres App-Kennwort erstellen](#)

Fertig

Geben Sie dieses Kennwort statt des Kontokennwortes ein. Das E-Mail-Programm fragt nicht mehr nach dem zweiten Faktor, ein Fremder, der nur Ihr eigentliches Passwort hat, kommt aber nicht an die E-Mails.

Backup, Migration, Wechsel von Konten

Ihre E-Mails sind schnell ein nicht mehr wegzudenkender Bestandteil Ihrer Arbeit. Wenn Sie noch ein lokal verwaltetes E-Mail-Konto haben, dann sollten Sie sich einmal die Vorteile eines Wechsels zu einem Online-Anbieter ansehen: Office 365 als der von Microsoft etablierte Dienst, der Windows 10 und Office verbindet, ist ein gutes Beispiel.

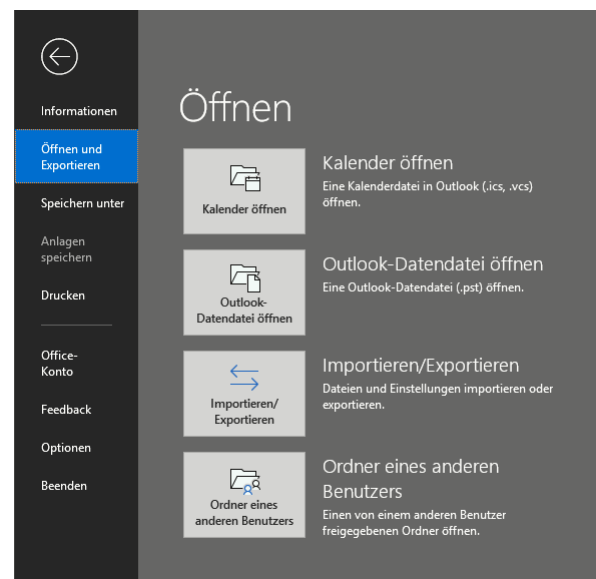
Windows 10-Report Ausgabe 19/09

Mitlesen, mitreden.

Der Backup der E-Mail-Daten aus Outlook

Der erste Schritt zum Transfer der Daten ist der Export aus Outlook in eine PST-Datei. Outlook verwendet dieses Format, um komplette Postfächer konsolidiert in einer einzigen Datei zu sichern und damit portabel zu machen. Allerdings haben die Produktverantwortlichen es konsequent in allen Versionen von Outlook geschafft, die Exportfunktion zu verstecken:

In Outlook müssen Sie unter **Datei** auf **Öffnen > Importieren** klicken.

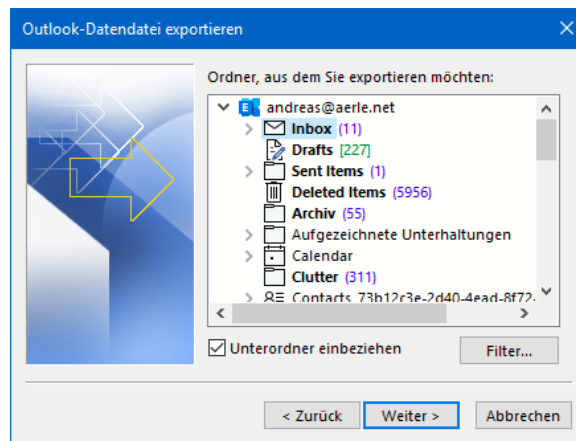


In dem sich nun öffnenden Dialog (der eigentlich dem Import dient) befindet sich eine Option "In Datei exportieren". Diese klicken Sie nun an und wählen **Outlook Datendatei (PST-Datei)** als Ziel.

Wichtig ist nun, die oberste Ebene des Postfaches auszuwählen, damit nicht nur die E-Mails, sondern auch die Kontakte und Termine (so diese in dem zu exportierenden Konto vorhanden sind) miterfasst werden. Ebenso sollte zwingend der Haken bei **Unterrordner einbeziehen** gesetzt sein, damit nicht nur der Posteingang, sondern auch die Ordner, die der Anwender darin angelegt hat, erfasst und mitkopiert werden.

Windows 10-Report Ausgabe 19/09

Mitlesen, mitreden.



Zum Abschluss müssen der Name und der Speicherort der Datei angegeben werden. Beide sollten sinnvoll gewählt werden, um die Datei für den Import wiederzufinden.

Je nach Größe des Postfaches dauert der Exportvorgang von einigen Sekunden bis zu

einigen Stunden.

Die Migration zu Office 365

Der folgende erste Schritt ist nur nötig, wenn das Office 365-Konto noch nicht in Outlook konfiguriert ist.

Um ein neues Konto anzulegen, muss unter **Datei** auf **Konto hinzufügen** geklickt werden:

Im nun folgenden Bildschirm müssen der Absendername (der dem Empfänger einer E-Mail statt der E-Mail-Adresse angezeigt wird), das Office 365-E-Mail-Adresse und das Kennwort dafür (zweimal) eingegeben werden. Outlook erkennt automatisch, dass es sich bei der Domäne der Adresse um eine Office 365-Adresse handelt und konfiguriert die Serverinformationen und alle weiteren nötigen Dinge automatisch.

Nachdem nun die Altdaten in Form einer PST-Datei vorliegen und das Office 365-Konto in Outlook eingerichtet ist, ist der Import der Daten nur noch ein kleiner, wenn auch gegebenenfalls zeitaufwändiger Akt:

Windows 10-Report Ausgabe 19/09

Mitlesen, mitreden.

Unter **Datei > Öffnen und Exportieren** klicken Sie auf **Importieren/Exportieren**.

Diesmal handelt es sich ja tatsächlich um einen Datenimport, darum ist die markierte Option auch die richtige.

Wählen Sie als Dateityp hier wieder die Outlook-Datendatei an. Über **Durchsuchen** lokalisieren Sie dann die gewünschte zu importierende PST-Datei auf der Festplatte.

Der Import dauert nach einem letzten Klick auf **Weiter** dann wieder zwischen Sekunden und Stunden, dies ist abhängig von der Zahl der zu importierenden Elemente.

Schön während des Importvorgangs gleicht Outlook die Daten mit Office 365 in der Cloud ab, jedes Gerät (egal ob Smartphone, Tablet oder Desktop/Notebook), auf dem das Office 365-Konto konfiguriert ist, bekommt dann Stück für Stück die Daten zugestellt. Der Vorgang ist abgeschlossen, wenn Outlook unten rechts "Alle Ordner sind auf dem aktuellen Stand" anzeigt.

Bequemer mit einer Datenspedition

Ein Umzug ist immer eine langwierige und nervenzehrende Aktion. Wenn Sie sich diesen Stress ersparen wollen, dann gibt es wie beim Möbelumzug eine Alternative über Dienstleister.

Windows 10-Report Ausgabe 19/09

Mitlesen, mitreden.

audriga E-MAIL UMZUG

EINFÜHRUNG ANBIETERAUSWAHL EINSTELLUNGEN UMZUG BESTÄTIGEN UMZUGSSTATUS

Auswahl der E-Mail-Anbieter

Bitte wählen Sie aus, zwischen welchen Anbietern Sie E-Mail-Postfächer umziehen möchten

Neuen Anbieter eingeben

Tippen Sie einen Namen ein, um weitere Anbieter zu sehen...

1&1
Apple iCloud
DomainFactory
GMX
Google Mail / Google Apps
Host Europe
Jimdo (Webmail)
Strato
Web.de
Yahoo! Mail

Fehlenden Anbieter oder Server selbst hinzufügen
Fehlenden Anbieter vorschlagen

Weiter

Anbieter wie audriga (<http://www.audriga.com>) führen den kompletten Umzug Ihres Email-Postfaches automatisiert durch. Sie geben nur den Quell-E-Mail-Dienst und den Zieldienst an. Für beiden müssen Sie die Zugangsdaten eingeben, damit der Dienst vom einen lesen und in den anderen schreiben kann. Für EUR 11,90 werden Ihre Daten dann übertragen. Sie bleiben per E-Mail (und auf Wunsch in der Verwaltungskonsole online) über den Fortschritt informiert.

Wichtig Nachdem Sie den Umzug gestartet haben, sollten Sie keine Veränderungen mehr am alten Postfach vornehmen. Diese würden verloren gehen. Idealerweise stellen Sie vorab Ihr altes Postfach schon so ein, dass es die eingehenden E-Mails automatisch an das neue Postfach weiterleiten lassen. Dann sind diese nach Abschluss des Umzuges schon direkt dort verfügbar.

Windows 10-Report Ausgabe 19/09

Mitlesen, mitreden.

Wechsel eines E-Mail-Kontos ohne Verluste

Eine E-Mail-Adresse ist fürs Leben. Das ist zumindest der Plan, den Sie beim Anlegen der Adresse haben. Aber dann kommt es anders: Sie heiraten, werden adoptiert, wollen den damals so cool klingenden Spitznamen nicht mehr verwenden. Natürlich können Sie die E-Mail-Adresse anpassen. Manche Anbieter lassen das zu. Allerdings bringt dies Aufwand mit sich. Sie müssen alle Personen informieren, die Ihre alte E-Mail-Adresse kennen, sonst laufen Mails ins Leere. Das können Sie aber auch eleganter lösen!

Als erstes legen Sie sich die neue E-Mail-Adresse beim Anbieter Ihrer Wahl an. Diese kann komplett anders sein als die alte. Sie können sogar zu einem anderen Anbieter wechseln, wenn das für Sie Sinn macht. Wichtig ist nur, dass die neue Adresse bereits existiert und funktioniert.

Melden Sie sich nun über das Internet am alten Postfach an und wechseln Sie in die Einstellungen. Die automatische Weiterleitung finden Sie in den E-Mail-Einstellungen.

Layout

Verfassen und Antworten

Anlagen

Regeln

Aufräumen

Junk-E-Mail

Aktionen anpassen

E-Mail synchronisieren

Nachrichtenbehandlung

Weiterleitung

Automatische Antworten

Weiterleitung

Sie können Ihre E-Mails an ein anderes Konto weiterleiten.

Weiterleitung aktivieren

Meine E-Mails weiterleiten an:

Kopie weitergeleiteter Nachrichten beibehalten

Windows 10-Report Ausgabe 19/09

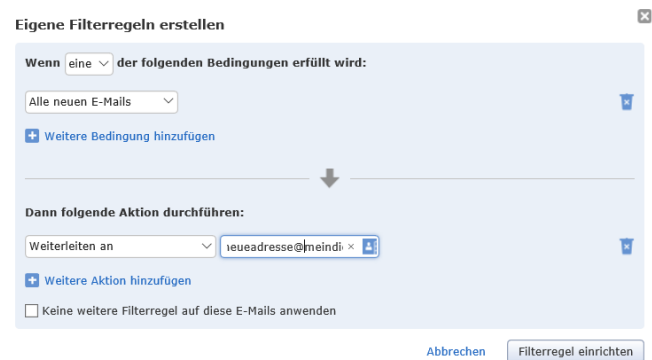
Mitlesen, mitreden.

Bei manchen E-Mail-Diensten ist die permanente Weiterleitung nicht als separate Option verfügbar. Stattdessen müssen Sie unter Regeln einrichten, dass alle E-Mails an eine externe Adresse weitergeleitet werden.

Sie müssen nun im Prinzip nicht einmal Ihre Bekannten über die neue Adresse informieren. Jede E-Mail, die an die alte Adresse geht, kommt durch die Weiterleitung im neuen Postfach an. Wenn Sie darauf

antworten, ist die Absenderadresse automatisch Ihre neue Email-Adresse. Ebenso verhält es sich, wenn Sie eine neue E-Mail schreiben. Nach kurzer Zeit schicken

die meisten Absender ihre E-Mails also an die neue Adresse. Und wenn jemand immer noch die alte Adresse nutzt, dann bekommen Sie diese zuverlässig, weil sie automatisch weitergeleitet wird.



Tip Eine Weiterleitung behält die weitergeleitete Email im ursprünglichen Postfach. Das heißt, dass dieses mit der Zeit immer voller wird. Kontrollieren Sie es regelmäßig und löschen Sie die E-Mails, sonst ist das Postfach irgendwann voll und verweigert die Annahme neuer E-Mails.

Webmailer als Alternative

Wenn Sie viel unterwegs sind, dann nutzen Sie oft wechselnde PCs. Statt mühsam über das kleine Display Ihres Smartphones E-Mails abzuholen und zu beantworten, nutzen Sie die Web-Portale der E-Mail-Anbieter.

Windows 10-Report Ausgabe 19/09

Mitlesen, mitreden.

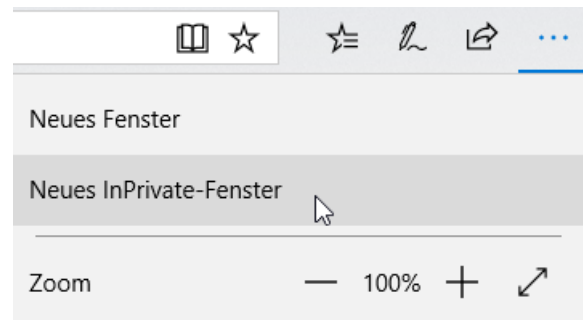
Ob Google, Microsoft, 1&1 IONOS, oder die klassischen Webmailer wie GMX und Web.de, alle bieten den Zugriff auf Ihre Postfächer allein über den Webbrowser an.

Ob Sie das nun im Büro bei einem Kollegen oder im Internetcafé nutzen, diesen PC nutzen Sie nicht allein. Der Benutzer nach Ihnen kann also im schlimmsten Fall auf Ihre Daten zugreifen, Ihre E-Mails lesen und so einiges mehr. Das können Sie allerdings mit wenigen Schritten verhindern:

Der private Surfmodus

Im Regelfall speichert Edge automatisch eine Vielzahl von Informationen: Vor allem der Verlauf, also die Liste der aufgerufenen Webseiten, ist hier oft kritisch. Greifen mehrere Benutzer auf Ihren Rechner mit Ihrem Konto zu, dann können diese sehen, welche Seiten Sie aufgerufen haben.

Wenn Sie das nicht möchten, dann starten Sie einfach eine private Surf-Sitzung. Dazu klicken Sie in Edge auf die drei Punkte oben rechts, dann auf Neues In Private-Fenster.



Edge öffnet jetzt ein neues Fenster. Alle während des Surfens in diesem Fenster angesurften Webseiten werden nicht im Verlauf gespeichert. Auch die Cookies und Temporären Dateien werden nach Schließen des Fensters automatisch gelöscht.

Wichtig

Wundern Sie sich nicht, wenn Sie sich auf bekannten Webseiten im privaten Surfmodus immer wieder anmelden müssen (statt wie bisher die Anmeldedaten zu bestätigen). Der Zugriff auf bereits

Windows 10-Report Ausgabe 19/09

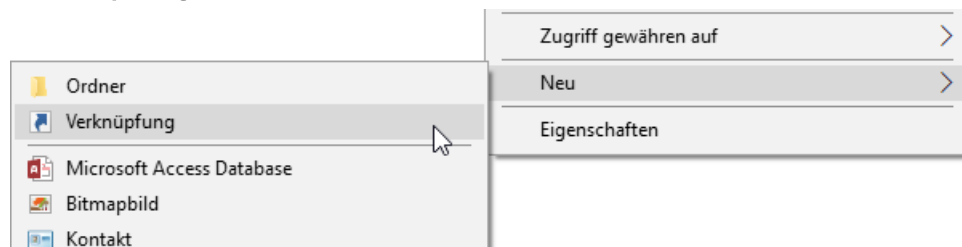
Mitlesen, mitreden.

gespeicherte Daten wird unterbunden, um die Privatheit sicherzustellen.

Edge immer im privaten Surfmodus starten

Wenn Ihr Rechner häufiger von anderen Personen benutzt wird, dann macht es vielleicht Sinn, Edge immer im privaten Surfmodus zu starten. Das erlaubt Windows 10 zwar nicht direkt. Sie können es aber über einen kleinen Trick schnell erreichen:

Legen Sie eine neue Verknüpfung auf dem Desktop an, indem Sie mit der rechten Maustaste auf das Desktop klicken und dann **neu** > **Verknüpfung** anwählen.



Als Speicherort geben Sie den Text

```
%windir%\System32\cmd.exe /c start  
shell:AppsFolder\Microsoft.MicrosoftEdge_8wekyb3d8bbwe!MicrosoftEd  
ge -private
```

ein. Als Namen der Verknüpfung im nächsten Schritt geben Sie dann **Edge (privat)** ein.












Ein Doppelklick auf diese neue Verknüpfung startet dann immer ein neues Edge-Fenster, das direkt im privaten Surfmodus geöffnet wird.

Nun ist das Symbol der Verknüpfung nicht sonderlich schön. Das können Sie ändern: Klicken Sie mit der rechten Taste auf das Symbol und wählen Sie **Eigenschaften** > **Verknüpfung** > **anderes Symbol**.

Windows 10-Report Ausgabe 19/09

Mitlesen, mitreden.

Normalerweise zieht Windows 10 passende Symbole aus der .EXE-Datei. Nun ist es so, dass Edge kein Programm im eigentlichen Sinne, sondern eine fest in Windows 10 integrierte Funktion ist. Sie bekommen also keine Auswahlmöglichkeit für ein neues Symbol angezeigt.

| | | |
|-----------------------------------------------------------------------------------------------------|---------------------------------------|----------------|
|  battery.ico | Typ: Symbol Abmessungen: 24 x 24 | Größe: 91,2 KB |
|  laccessories1.ico | Typ: Symbol Abmessungen: 128 x 128 | Größe: 169 KB |
|  ldownload1.ico | Typ: Symbol Abmessungen: 128 x 128 | Größe: 210 KB |
|  luserguide1.ico | Typ: Symbol Abmessungen: 128 x 128 | Größe: 175 KB |
|  lwarranty1.ico | Typ: Symbol Abmessungen: 128 x 128 | Größe: 154 KB |
|  network.ico | Typ: Symbol Abmessungen: 24 x 24 | Größe: 98,9 KB |
|  action.ico | Typ: Symbol Abmessungen: 128 x 128 | Größe: 149 KB |
|  battery.ico | Typ: Symbol Abmessungen: 24 x 24 | Größe: 91,2 KB |
|  network.ico | Typ: Symbol Abmessungen: 24 x 24 | Größe: 98,9 KB |
|  system.ico | Typ: Symbol Abmessungen: 24 x 24 | Größe: 75,3 KB |
|  folder.ico | Typ: Symbol | |

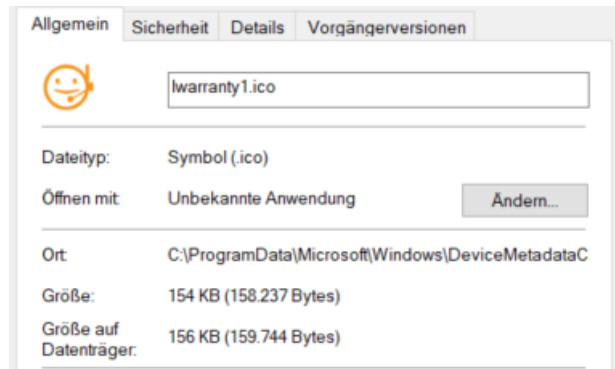
Windows verwendet Symboldateien, die die Erweiterung ICO (für Icon) haben. Sie können eine beliebige dieser Dateien für die Verknüpfung verwenden.

Starten Sie stattdessen durch Drücken von der **Windows** und **E**-Taste ein neues Explorer-Fenster. Klicken Sie auf die Festplatte C:, dann geben Sie oben rechts in der Suchleiste *.ico ein. Windows 10 zeigt Ihnen jetzt alle Symboldateien an.

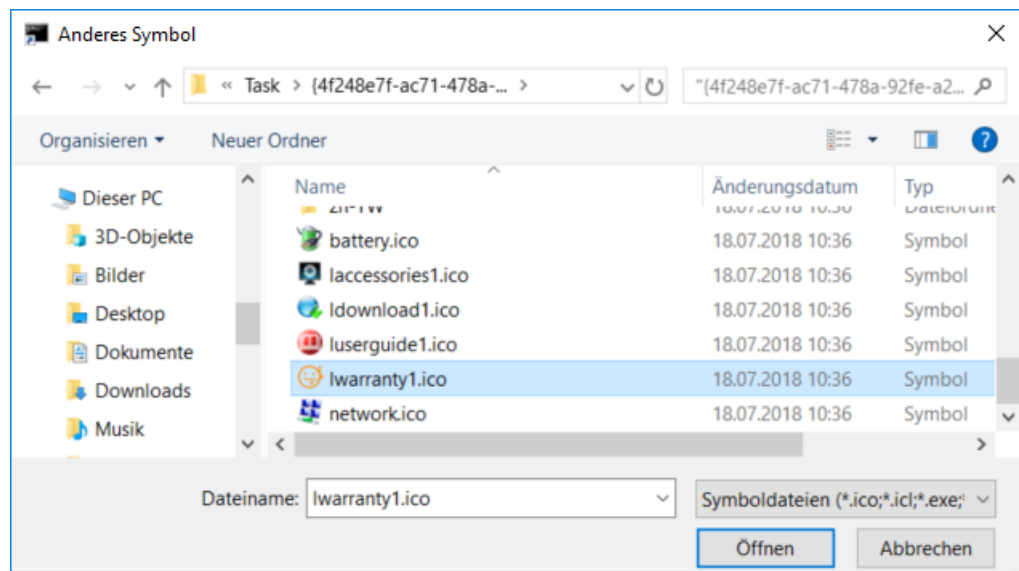
Windows 10-Report Ausgabe 19/09

Mitlesen, mitreden.

Wenn Sie darin ein Symbol gefunden haben, dann klicken Sie es einmal an, um es zu markieren. Ein Rechtsklick auf das Symbol zeigt Ihnen unter Ort den Pfad, an dem diese Symboldatei sich befindet. Markieren und kopieren sie ihn.



Diesen Pfad fügen Sie nun in den Eigenschaften des Symbols unter **Nach Symbolen in dieser Datei** suchen ein.



Nach einem Klick auf Öffnen und auf OK hat Ihre Edge-Verknüpfung dann das gewünschte neue Symbol.

Löschen der Internetspuren

In den meisten Fällen haben Sie sich an Ihrem PC nicht im privaten Surfmodus im Internet bewegt. Wenn Sie nun den PC weitergeben

Windows 10-Report Ausgabe 19/09

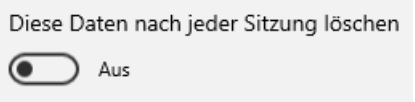
Mitlesen, mitreden.

wollen oder nicht an Ihrem eigenen PC gesurft haben, dann sollten Sie die gespeicherten Dateien löschen.

Unter **Einstellungen** > **zu löschendes Element auswählen** können Sie ganz fein festlegen, welche Dateien gelöscht werden sollen: der Verlauf, Cookies, temporäre Dateien, gespeicherte Tabs, Formulardaten, Kennwörter und vieles mehr. Wählen Sie alle möglichen Optionen, wenn Sie den Rechner komplett von ihren Spuren befreien wollen. Mit einem Klick auf **Löschen** entfernen Sie diese von der Festplatte.



Wenn Sie häufiger an einem fremden PC arbeiten, dann macht es Sinn,



den manuellen Löschvorgang zu automatisieren. Dazu aktivieren sie die Option **Diese Daten nach jeder Sitzung**

löschen. Alle Optionen, die Sie im vorigen Schritt aktiviert haben, werden dann gelöscht, wenn Sie das Browserfenster schließen.

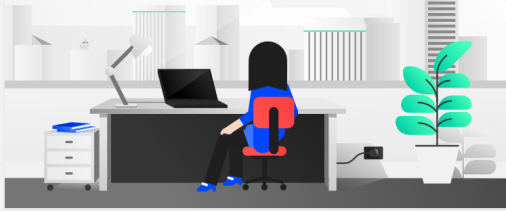
Damit haben Sie schon einmal die lokalen Spuren auf der Festplatte gelöscht. Allerdings synchronisiert Windows 10 im Standard einige dieser Daten mit der Cloud. Um diese zu löschen, klicken Sie in Windows 10 in den **Einstellungen** auf **Datenschutz** > **Meine Daten verwalten, die in der Cloud gespeichert sind**.

Ironischerweise öffnet sich dann die Kontoverwaltungsseite in Edge. Nach der Anmeldung können Sie dann den Browserverlauf, den Suchverlauf und viele andere Elemente anzeigen lassen und auch löschen.

Windows 10-Report Ausgabe 19/09

Mitlesen, mitreden.

Browserverlauf




Wenn der Browserverlauf in Cortana aktiviert ist, wird Ihr Microsoft Edge-Browserverlauf an Microsoft gesendet, damit die Features und Dienste von Microsoft diese Daten verwenden, um Ihnen zeitnahe und intelligente Antworten oder proaktive personalisierte Vorschläge bereitzustellen oder für Sie Aufgaben auszuführen.

Neben dem hier gespeicherten Browserverlauf speichert Microsoft Edge außerdem Ihren Browserverlauf auf Ihrem Gerät. Zum Löschen dieser Daten auf Ihrem Gerät wechseln Sie zu **Microsoft Edge > Mehr ... > Einstellungen**.

Bei Verwendung von InPrivate-Tabs oder -Fenstern werden Ihre Browserdaten (z. B. Ihr Verlauf, temporäre Internetdateien und Cookies) nicht auf Ihrem Gerät gespeichert, nachdem Sie die Sitzung beendet haben. [Weitere Informationen zu InPrivate-Browsen](#)

BROWSERVERLAUF ANZEIGEN UND LÖSCHEN >

Suchverlauf




Wie andere Suchmaschinen verwendet Bing Ihren Suchverlauf zur Optimierung Ihrer Suchergebnisse, einschließlich Personalisierung und automatischer Vorschläge. Cortana verwendet diese Daten, um Ihnen zeitnahe, intelligente Antworten und angepasste Vorschläge zu unterbreiten und andere Aufgaben für Sie zu erledigen.

[Sucheinstellungen anzeigen und ändern](#)

[Weitere Informationen zu InPrivate-Browsen](#)

SUCHVERLAUF ANZEIGEN UND LÖSCHEN >

Standort-Aktivität



Mit den von Ihnen angegebenen oder über Technologien wie GPS erhaltenen Positionsdaten können wir Ihnen Wegbeschreibungen und relevante Informationen über Ihren Aufenthaltsort zur Verfügung stellen.

Hier finden Sie Informationen zum [Ändern der Positionseinstellungen](#) auf Ihrem Windows-Gerät

STANDORTAKTIVITÄT ANZEIGEN UND LÖSCHEN >

Schutz vor Schädlingen durch Smartscreen

Das Internet bietet mehrere unterschiedliche Arten von Bedrohungen. Neben Viren und Phishing-Attacken handelt es sich hier vor allem um Webseiten, die Schadcode enthalten und beim Aufruf weiterverbreiten. Viele Antiviren-Programme haben eine separate Schutzfunktion dafür. Auch Windows 10 bietet mit SmartScreen eine integrierte Funktion, die Sie auf jeden Fall aktivieren sollten.

Unter **Einstellungen > Updates und Sicherheit > Windows Sicherheit > Windows Sicherheit öffnen > App- & Browsersteuerung** können Sie unter Smartscreen für Microsoft Edge aktivieren, dass Webseiten vor der Darstellung in Edge überprüft werden. Hier sollten Sie mindestens **Warnen** aktiviert haben.

SmartScreen überprüft jede Seite aktuell gegen die Microsoft Server, so werden auch neue erkannte Bedrohungen umgehend mit in die Prüfung einbezogen.

Windows 10-Report Ausgabe 19/09

Mitlesen, mitreden.

SmartScreen für Microsoft Edge

Windows Defender SmartScreen-Filter schützt Ihr Gerät vor schädlichen Websites und Downloads.

- Blockieren
- Warnen
- Deaktiviert

[Datenschutzbestimmungen](#)

Windows 10-Report Ausgabe 19/09

Mitlesen, mitreden.