# Ihr PC-Sicherheits-Berater

## So schützen Sie Ihre Privatsphäre und sensiblen Daten

**3 So erhalten Sie ein sicheres E-Mail-Konto**
Machen Sie den E-Mail-Check auf Seite 2. Ist Ihr Anbieter nicht sicher, richten Sie ein neues, sicheres Konto bei Posteo ein.

**4 Geben Sie Ihre E-Mail-Adresse nur Freunden**
Mein Tipp: Schützen Sie sich mit Wegwerf-E-Mail-Adressen vor gefährlichen Betrugs- und lästigen Werbe-Mails.

**6 Schützen Sie Ihre E-Mails vor Kriminellen**
Verschlüsseln Sie Ihre E-Mails. Nur so kontrollieren Sie, wer Ihre E-Mails liest, und kappen den Zugriff durch Kriminelle.

**7 Beugen Sie dem Verlust von E-Mails vor**
Verlassen Sie sich nicht auf Ihren E-Mail-Anbieter. Speichern Sie wichtige E-Mails mit diesem Gratis-Tool als PDF-Datei.

**100 % Sicherheit für Ihre E-Mails: So mailen Sie im Herbst 2019 endlich sorgenfrei und sicher**

### Wetten, dass Ihr E-Mail-Konto gehackt wurde?

Jeden Tag werden im Internet über 800.000 gestohlene E-Mail-Adressen und weitere Daten gefunden. Insgesamt wurden rund 10 Milliarden E-Mail-Adressen weltweit gestohlen. Nahezu jeder E-Mail-Nutzer ist betroffen.

Mindestens eines Ihrer E-Mail-Konten wurde statistisch in den letzten Jahren gehackt – und das kann gefährliche Konsequenzen haben!

Mit den Daten aus Ihrem E-Mail-Konto werden weitere Konten gehackt und Sie erhalten Betrugs-Mails mit Schadprogrammen.

**Meine Empfehlung:** Schützen Sie Ihr E-Mail-Konto, Ihre E-Mail-Adresse und Ihre E-Mails mit meinen 7 Sicherheitsschritten.

Viele Grüße, Ihr

Michael-Alexander Beisecker,
Deutschlands PC-Sicherheitsexperte Nr. 1

**Kostenlose Experten-Hilfe:**
Exklusiv für Sie als Abonnenten: Die Sofortauskunft mit zuverlässigen Antworten und professionellen Tipps direkt von der Redaktion.
Redaktions-Hotline: **Mittwoch zwischen 15:00 und 18:00 Uhr, Tel.: 02 08/69 07 977**

Schützen Sie Ihre E-Mail-Nachrichten, Ihre E-Mail-Identität und Ihre Daten

# 7-Schritte-Lösung: So versenden und empfangen Sie sicher Ihre E-Mails

**Ihre E-Mail-Adresse kursiert womöglich schon in Hacker-Kreisen. Allein im Januar 2019 wurden fünf Hacker-Datenbanken mit insgesamt 2,2 Milliarden gestohlenen E-Mail-Adressen und Millionen gestohlener Passwörter gefunden. Warten Sie nicht, bis Sie durch Erpresser- und Banking-Trojaner schweren Schaden erleiden. Bekämpfen Sie das Übel an der Wurzel: Verschicken und empfangen Sie Ihre E-Mails ab sofort sicher.**

**Meine Lösung:** Überprüfen Sie die Sicherheit Ihres E-Mail-Anbieters (Schritt 1) und wechseln Sie bei negativem Ergebnis zu Testsieger Posteo (Schritt 2). Schicken Sie Spam-Versendern eine Wegwerfadresse (Schritt 3). So schützen Sie sich vor unerwünschten Werbe-Mails und gefährlichen Betrugs-Mails. Zusätzlichen Schutz bieten Ihnen reine Text-Mails ohne Schadprogramm-Gefahr (Schritt 7).

Doch mein Schutz geht noch weiter: Ich zeige Ihnen, wie Sie durch selbstzerstörende E-Mails (Schritt 4) und verschlüsselte E-Mail-Texte und -Anhänge (Schritt 5) auch dann noch die Kontrolle über Ihre Daten behalten, wenn sie bereits beim Empfänger angelangt sind. Das ist wichtig, denn Sie wissen ja nicht, wie sicher die PCs Ihrer E-Mail-Empfänger und deren E-Mail-Anbieter sind. Wenn Sie Ihre E-Mails außerdem als PDF-Datei drucken, gehen Ihnen keine wichtigen Daten verloren (Schritt 6).

**Machen Sie Versand und Empfang Ihrer E-Mails Schritt für Schritt sicherer:**

**Schritt 1:** Überprüfen Sie Ihren E-Mail-Anbieter (siehe Seite 2).

**Schritt 2:** Richten Sie ein Konto bei Posteo mit Zwei-Faktor-Authentifizierung und Komplett-Verschlüsselung ein (siehe Seite 3).

**Schritt 3:** Verschicken Sie anonyme E-Mails, um Ihre E-Mail-Adresse nicht preiszugeben (siehe Seite 4).

**Schritt 4:** Sichern Sie Ihren Mail-Versand wie der Geheimdienst (siehe Seite 5).

**Schritt 5:** Verschlüsseln Sie Ihre E-Mails und stoppen Sie so den Zugriff durch Kriminelle (siehe Seite 6).

**Schritt 6:** Beugen Sie Datenverlust vor und sichern Sie wichtige E-Mails als PDF-Datei (siehe Seite 7).

**Schritt 7:** Schützen Sie sich vor Skript-Angriffen und stellen Sie den E-Mail-Empfang auf Text um (siehe Seite 8).

*Wenden Sie diese 7 Schritte an und befreien Sie sich von den E-Mail-Gefahren.*

*>>> Lesen Sie bitte weiter auf Seite 2*

# Schritt 1: Überprüfen Sie Ihren E-Mail-Anbieter

**Die Sicherheit Ihrer E-Mails hängt vor allem von Ihrem E-Mail-Anbieter ab – und das ist eine schlechte Nachricht, denn es gibt nur ganz wenige sichere Anbieter. Bei den unsicheren E-Mail-Anbietern reicht die Anmeldung mit einem Passwort aus. Doch ein „sicheres Passwort" ist heute nicht mehr sicher genug. Nur wenn zusätzlich zum Passwort noch ein „Einmal-Passwort" abgefragt wird, beißen sich Hacker an Ihrem E-Mail-Konto die Zähne aus. Prüfen Sie mit meinen 7 Fragen, ob Ihr E-Mail-Anbieter sicher ist oder ob Sie besser wechseln sollten.**

1. **Reichen zur Anmeldung bei Ihrem E-Mail-Konto Ihre E-Mail-Adresse und Ihr Passwort aus?**
   - ☐ **Ja:** Ihr E-Mail-Konto ist mit diesen beiden Angaben nicht ausreichend geschützt. Aktivieren Sie zusätzlich die Zwei-Faktor-Authentifizierung. Sie erhalten dann vor jeder Anmeldung ein Einmal-Passwort auf Ihr Mobiltelefon gesendet oder erzeugen das Passwort über ein Generator-Tool. Bietet Ihr E-Mail-Anbieter keine Zwei-Faktor-Authentifizierung an, wechseln Sie so schnell wie möglich den Anbieter.
   - ☐ **Nein**

2. **Ist Ihr E-Mail-Anbieter ein amerikanisches Unternehmen?**
   - ☐ **Ja:** Aus Datenschutzgründen empfehle ich Ihnen einen deutschen Anbieter, bei einem Wohnsitz in Österreich oder der Schweiz auch einen regionalen Anbieter. Amerikanische Firmen wie Google (Gmail) oder Microsoft (Outlook.com) bieten zwar sichere E-Mail-Konten, aber es besteht die Gefahr, dass US-Geheimdienste in Ihren E-Mails herumschnüffeln.
   - ☐ **Nein**

3. **Erhalten Sie unaufgefordert Werbe-E-Mails?**
   - ☐ **Ja:** Der Spam-Filter Ihres E-Mail-Anbieters funktioniert nicht zuverlässig. Sehen Sie in den Einstellungen nach, ob sich eine stärkere Filterwirkung einstellen lässt, oder wechseln Sie den E-Mail-Anbieter.
   - ☐ **Nein**

4. **Warnt Sie Ihr Antiviren-Programm vor gefährlichen Links und Anhängen?**
   - ☐ **Ja:** Ein guter E-Mail-Anbieter filtert solche E-Mails aus (siehe auch Frage 3). Erhalten Sie durch Ihr Antiviren-Programm häufiger Warnungen vor gefährlichen E-Mails oder deren Anhang, wechseln Sie den E-Mail-Anbieter.
   - ☐ **Nein**

5. **Haben Sie nur ein E-Mail-Konto?**
   - ☐ **Ja:** Setzen Sie zu Ihrem Schutz zwei E-Mail-Konten oder E-Mail-Adressen ein. Geben Sie Ihre Haupt-E-Mail-Adresse nur an enge Freunde und für Sie wichtige und vertrauenswürdige Kontakte weiter. So vermeiden Sie Werbe- und Betrugs-Mails in Ihrem Hauptkonto.
   - ☐ **Nein**

6. **Fehlen Ihnen bei Ihrem jetzigen E-Mail-Anbieter wichtige Funktionen oder reicht der angebotene Speicherplatz nicht aus?**
   - ☐ **Ja:** Ihr E-Mail-Anbieter sollte ausreichend große E-Mail-Anhänge erlauben und ausreichend Speicherplatz zum dauerhaften Speichern Ihrer E-Mails sowie eine komfortable E-Mail-Verwaltung bieten. Sofern Sie ein Smartphone nutzen, sollte Ihr E-Mail-Dienstleister für dessen Betriebssystem (i. d. R. Android oder iOS) auch eine spezielle Mail-App anbieten. Prüfen Sie, ob Ihr E-Mail-Anbieter ein kostenpflichtiges Angebot mit ausreichend Funktionen und Leistungen bietet, und wechseln Sie ansonsten den E-Mail-Anbieter.
   - ☐ **Nein**

7. **Schickt Ihnen der E-Mail-Anbieter selbst Werbe-Mails?**
   - ☐ **Ja:** Solange Sie diese Werbe-Mails nicht stören, ist das kein Problem. Wechseln Sie ansonsten entweder zu einem werbefreien, kostenpflichtigen Angebot des Unternehmens oder wechseln Sie den E-Mail-Anbieter.
   - ☐ **Nein**

Haben Sie **Frage 1** mit **Ja** beantwortet, wechseln Sie auf jeden Fall Ihren E-Mail-Anbieter. Wechseln Sie Ihren E-Mail-Anbieter auch, wenn Sie ein E-Mail-Postfach bei AOL Mail, Google Mail (Gmail), Microsoft Outlook.com und insbesondere Yahoo Mail haben. Alle genannten E-Mail-Dienste stammen von amerikanischen Unternehmen (siehe **Frage 2**). AOL Mail und Yahoo Mail sind zudem unsicher, denn sie wurden in den letzten Jahren mehrfach gehackt.

Technisch erfüllen Gmail und Microsoft Outlook.com allerdings die Sicherheitsanforderungen, inklusive der mittlerweile unabdingbaren Zwei-Faktor-Authentifizierung. Ist Ihnen der Datenschutz nicht so wichtig, können Sie also Ihr Gmail- oder Outlook.com-Konto weiter nutzen.

**Meine Empfehlung:** Für den Wechsel empfehle ich Ihnen Posteo, den mehrfachen Testsieger der Stiftung Warentest. Posteo hat als erster E-Mail-Anbieter die Zertifizierung „Sicherer E-Mail-Transport" (BSI TR-03108) erhalten. In einem Test der Zeitschrift „Chip" antwortete der Support innerhalb von 20 Minuten. Die Hilfe von Posteo ist insbesondere zu den Sicherheitsfunktionen hervorragend. Sie werden bei Posteo zudem nicht wie etwa bei GMX oder Web.de durch Werbung belästigt. Das Konto ist zwar kostenpflichtig, aber mit 1 € pro Monat verhältnismäßig günstig.

# Schritt 2: Richten Sie ein Konto mit Zwei-Faktor-Authentifizierung und Komplett-Verschlüsselung ein

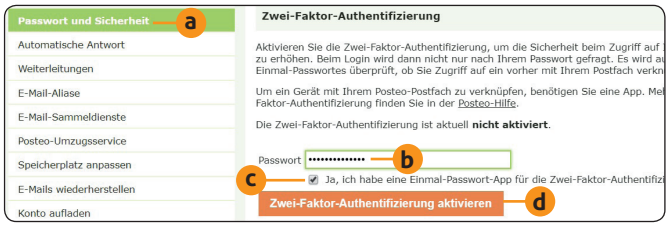
**Es gibt bei der Sicherheit große Unterschiede zwischen den E-Mail-Anbietern. Nicht alle der großen, unter „E-Mail made in Germany" werbenden Anbieter 1&1, GMX, freenet.de, Telekom und Strato bieten die sichere Zwei-Faktor-Authentifizierung an. Umfassende Sicherheit bietet Ihnen dagegen das von der Stiftung Warentest bereits mehrfach zum E-Mail-Testsieger erklärte Unternehmen Posteo. Hier erhalten Sie zwar kein kostenloses E-Mail-Konto, aber dafür Sicherheit zum kleinen Preis ab 1 € pro Monat.**

### In 7 Schritten eröffnen Sie Ihr sicheres Posteo-Konto

1. Rufen Sie zuerst über unsere sichere Service-Webseite die Internetseite von **Posteo** auf: https://posteo.de/de.
2. Geben Sie den gewünschten E-Mail-Namen ein. Erscheint „ist nicht verfügbar", ist der Name bereits vergeben. Überlegen Sie sich einen anderen Namen.
3. Denken Sie sich ein sicheres Passwort aus und geben Sie es in die Felder **Passwort** und **Passwort wiederholen** ein. Ihr Passwort sollte mindestens 14 Zeichen lang sein und aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen bestehen. Es dürfen keine Umlaute (ä, ö, ü) enthalten sein. Bewertet Posteo Ihr Passwort als sicher und korrekt, erscheint hinter dem Feld ein Haken. Klicken Sie auf **Weiter zu Schritt 2**.
4. Wählen Sie die Zahlungsart. Zur Auswahl stehen **Barzahlung**, **Gutschein**, **Kreditkarte**, **Paypal** und **Überweisung**. Klicken Sie auf **Weiter**.
5. Lesen Sie die AGB (**A**llgemeinen **G**eschäfts**b**edingungen) sowie die Datenschutzerklärung und bestätigen Sie durch Anklicken die drei Kästchen **AGB**, **Datenschutzerklärung** und **Widerrufsbelehrung**.
6. Beantworten Sie die Sicherheitsfrage und klicken Sie auf **Postfach jetzt kostenpflichtig eröffnen**.
7. Bestätigen Sie Ihre Registrierung. Danach können Sie Ihr neues Posteo-Postfach sofort nutzen. Manche Funktionen stehen Ihnen jedoch erst nach Eingang Ihrer Zahlung zur Verfügung.

### Auch schnell erledigt: So richten Sie die sichere Zwei-Faktor-Authentifizierung ein

1. Melden Sie sich bei Posteo an, wählen Sie **Einstellungen** sowie **Passwort und Sicherheit**.
2. Klicken Sie unter **Zwei-Faktor-Authentifizierung** auf **Posteo-Hilfe** und lesen Sie sich den Hilfetext durch.
3. Installieren Sie auf Ihrem Windows-PC die App, die Ihnen zukünftig das Einmal-Passwort liefert. Wie Sie die App auf Ihrem Mobiltelefon installieren, lesen Sie in der Anleitung „Mein Tipp" auf Seite 4. Den Download-Link finden Sie im Hilfetext unter **Voraussetzungen für die Zwei-Faktor-Authentifizierung**. Klicken Sie auf **WinAuth** (**Win**dows **Auth**enticator), um die App für Windows zu installieren. Sie erhalten das ZIP-Archiv **WinAuth-3.5.1.zip**. Dabei ist **3.5.1** die Versionsangabe, die sich ggf. geändert hat. Öffnen Sie das Zip-Archiv und starten Sie die App **WinAuth**.
4. Klicken Sie auf **Add** (Hinzufügen) und wählen Sie **Authenticator**.
5. Wechseln Sie zurück zu Posteo sowie **Passwort und Sicherheit** (a). Geben Sie unter **Zwei-Faktor-Authentifizierung** Ihr Posteo-Passwort ein (b). Bestätigen Sie mit einem Haken, dass Sie eine Einmal-Passwort-App installiert haben (c) (siehe Schritt 3 oben). Klicken Sie auf **Zwei-Faktor-Authentifizierung aktivieren** (d).



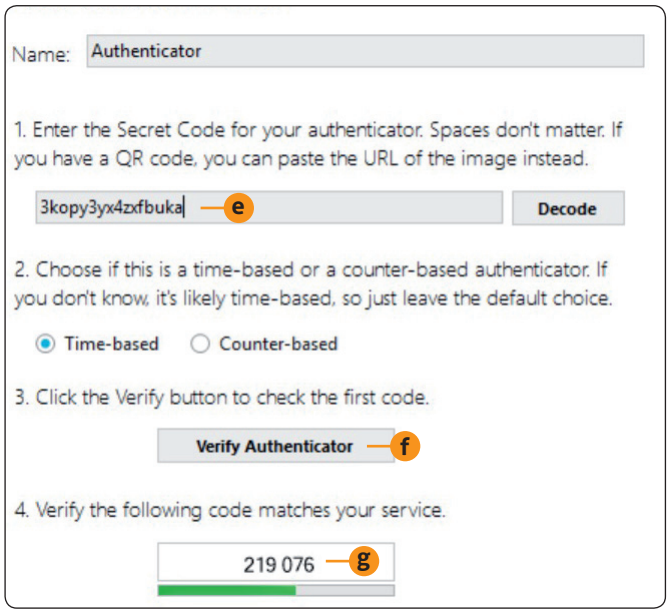

*Das Einrichten der Zwei-Faktor-Authentifizierung ist nur einmal erforderlich, danach geben Sie bei der Anmeldung nur noch Passwort und Einmal-Passwort ein.*

6. Ihnen werden ein geheimer Schlüssel wie zum Beispiel **3kopy3yx4zxfbuka** und ein QR-Code angezeigt. Geben Sie den geheimen Schlüssel im ersten Feld von WinAuth ein (e) und klicken Sie auf **Verify Authenticator** (geheimen Schlüssel überprüfen) (f).

## LESERSERVICE

**Redaktionshilfe:** Fragen Sie bei Sicherheitsbedenken immer zuerst Ihren persönlichen PC-Sicherheits-Berater Michael-Alexander Beisecker.

Melden Sie sich dazu einfach kostenlos unter **https://club.computerwissen.de** an und stellen Sie ihm dort Ihre Fragen. **Michael-Alexander Beisecker** und seine Redaktionsmitarbeiter helfen Ihnen gern weiter. Sie erhalten werktags innerhalb von 48 Stunden eine Antwort auf Ihre Frage – garantiert.




*Nach der Eingabe des geheimen Codes zeigt Ihnen WinAuth unter Punkt 4 das Einmal-Passwort an g, das alle 30 Sekunden wechselt.*

7. Geben Sie das **Einmal-Passwort** ins Feld **Aktuelles Einmal-Passwort** von Posteo ein, solange es gültig ist. Dann drücken Sie **Aktivierung bestätigen**. Waren Sie etwas zu langsam und das Einmal-Passwort ist zwischenzeitlich ungültig geworden, nehmen Sie einfach das nächste Einmal-Passwort und probieren es erneut.

**Mein Tipp:** Haben Sie ein iPhone oder Android-Mobiltelefon, können Sie die Einmal-Passwort-App auch auf Ihrem Mobiltelefon installieren. Führen Sie dazu die Schritte 1 und 2 auf Ihrem Mobiltelefon aus. Klicken Sie in Schritt 3 im Fall eines iPhones auf **FreeOTP** hinter **iOS** bzw. im Fall eines Smartphones mit Android-Betriebssystem auf **Android**. Öffnen Sie **FreeOTP** auf Ihrem Smartphone und scannen Sie den angebotenen QR-Code. Dann klicken Sie in Posteo auf **Aktivierung bestätigen**. Fertig!

### Übernehmen Sie die E-Mails aus Ihrem bisherigen E-Mail-Postfach und speichern Sie alles verschlüsselt

1. Melden Sie sich bei Posteo an. Wählen Sie für Ihren E-Mail-Umzug **Einstellungen**, **Mein Konto** und **Posteo-Umzugsservice**. Richten Sie wie in der Hilfe beschrieben den Umzugsservice ein.
2. Stellen Sie in den **Einstellungen** über **Mein Konto** und **E-Mail-Sammeldienste** den Sammeldienst ein, damit auch neu eingehende E-Mails von Ihrem alten Anbieter zum neuen übertragen werden.
3. Aktivieren Sie über die **Einstellungen** und **Verschlüsselungen** sowie **Posteo-Krypto-Mailspeicher** und **Adressbuch- und Kalenderverschlüsselung** das Verschlüsseln Ihrer E-Mails, Adressen und Kalendereinträge.

**Wichtig:** Vergessen Sie Ihr Posteo-Passwort, haben Sie nach dem Aktivieren von Zwei-Faktor-Authentifizierung und Verschlüsselung keinen Zugriff mehr auf Ihre Daten. Tragen Sie Ihr Passwort daher in Ihr Passwort-Buch oder Ihre Passwort-Liste ein. Bewahren Sie Ihre Passwort-Übersicht an einem sicheren Ort, wie zum Beispiel in Ihrem Tresor, auf.

4. Informieren Sie Ihre wichtigsten Kontakte über Ihre neue E-Mail-Adresse, damit Sie wichtige E-Mails nur noch über die neue E-Mail-Adresse erhalten.
5. Ihr vorheriges E-Mail-Konto können Sie als Zweit-Konto weiterführen, über das Sie zum Beispiel Newsletter bestellen, bei Gewinnspielen mitmachen oder kostenlose Angebote im Internet wahrnehmen.

**Meine Empfehlung:** Lesen Sie bei Posteo die Funktionsbeschreibungen in der **Hilfe** durch. Es gibt viele interessante Funktionen zu entdecken. Bei Fragen helfen Ihnen meine Redaktionsmitarbeiter und ich selbstverständlich gerne über den Computerwissen Club: https://club.computerwissen.de.

# Schritt 3: Verschicken Sie anonyme E-Mails, um Ihre E-Mail-Adresse nicht preiszugeben

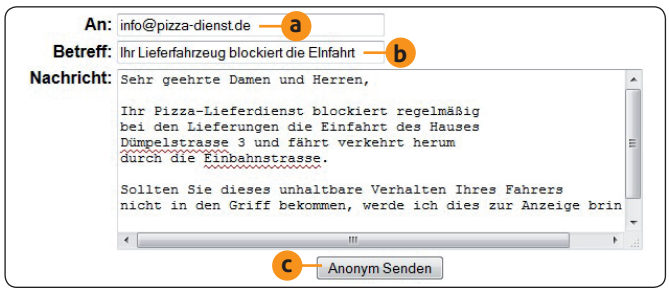
**Im Internet ist Ihre E-Mail-Adresse wertvoll wie eine Art Zahlungsmittel. Sie möchten an einem Gewinnspiel teilnehmen, ein kostenfreies eBook herunterladen oder ein Online-Programm verwenden? Dann werden Sie garantiert als Gegenleistung nach Ihrer persönlichen E-Mail-Adresse gefragt. Anschließend erhalten Sie unerwünschte Werbe-Mails und womöglich gefährliche Trojaner oder Betrugsversuche in Ihr Postfach (z. B. gefälschte E-Mails Ihrer Bank). Ihr Schutz: Geben Sie bei Gewinnspielen auf keinen Fall Ihre eigentliche E-Mail-Adresse an. Verwenden Sie ab sofort immer eine anonyme E-Mail-Adresse, wenn Sie bei kostenlosen Angeboten nach Ihrer E-Mail-Adresse gefragt werden.**

Damit der Empfänger nicht in den Besitz Ihrer E-Mail-Adresse gelangt, verschicken Sie eine anonyme E-Mail über einen speziellen Online-Dienst. Dazu ist keine Anmeldung erforderlich. Der Versender kennt somit weder Ihren Namen noch Ihre eigentliche E-Mail-Adresse. Der Absender kann Ihnen dadurch auch nicht antworten.

### So verschicken Sie anonyme E-Mails zum Einmal-Gebrauch

Für Ihren anonymen E-Mail-Versand empfehle ich Ihnen den Online-Dienst AnonEmail. Der kostenlose Dienst mit deutscher Oberfläche arbeitet seit Jahren zuverlässig und ist einfach zu bedienen:

1. Rufen Sie **AnonEmail** über den Link http://anonymouse.org/anonemail_de.html auf.
2. Geben Sie die E-Mail-Adresse des Empfängers a, den Betreff b und Ihren Text ein. Dann klicken Sie auf **Anonym Senden** c.




*Zum Versand einer anonymen E-Mail geben Sie hier Empfänger, Betreff und Text ein.*

**Ihr Schutz:** Mit anonymen E-Mails verhindern Sie, dass andere Ihnen antworten und Ihr Postfach mit Werbe-Mails oder mit anderen unerwünschten elektronischen Sendungen verstopfen. Ihre eigentliche Mail-Adresse geben Sie nicht preis. Möchten Sie bei einem Dienst, bei dem Sie einen Bestätigungslink zugeschickt bekommen, eine E-Mail-Adresse angeben? In dem Fall setzen Sie wie im Folgenden erläutert Wegwerfadressen ein.

### Mit einer Wegwerfadresse erhalten Sie anonym Antwort

Fordert Sie eine Internetseite mit einer Bestätigungs-Mail zum Anklicken eines Links auf oder schickt Ihnen einen Download-Link, brauchen Sie eine anonyme E-Mail mit Antwort-Möglichkeit – eine Wegwerfadresse. Diese steht Ihnen mindestens 24 Stunden lang zur Verfügung.

Für das Einrichten einer Wegwerfadresse empfehle ich Ihnen den kostenlosen Online-Dienst „Wegwerf E-Mail-Adresse“ mit deutscher Oberfläche:

1. Rufen Sie **Wegwerf E-Mail-Adresse** über den Link http://www.wegwerfemailadresse.com auf. Es wird Ihnen dann sofort eine Wegwerfadresse angezeigt.
2. Ändern Sie optional den vorgeschlagenen Namen, zum Beispiel von **ZWhint1962** in **Urmel1952**.
3. Wählen Sie optional den gewünschten Domänennamen. Das ist der Teil der E-Mail-Adresse, den Sie nach dem At-Zeichen @ (umgangssprachlich auch „Klammeraffe“) eintippen.
4. Notieren Sie die angezeigte E-Mail-Adresse. Oder klicken Sie auf **Kopieren**, um die Adresse in die Zwischenablage von Windows zu übernehmen und von dort in ein Anmeldeformular im Internet einzufügen.
5. Notieren Sie sich die Adresse der Webseite Ihrer „Wegwerf-E-Mail-Adresse“ oder nehmen Sie diese als Favoriten in Ihrem Browser auf.
6. Die eingehenden Antworten werden auf der Internetseite mit Ihrer Wegwerfadresse angezeigt. Im Beispiel ist das http://www.wegwerfemailadresse.com/posteingang/superrito.com/urmel1952/. Dabei steht **superrito.com** für den gewählten Domänennamen und **urmel1952** ist Ihr gewählter Name. Rufen Sie Internetseite auf, um die E-Mails zu lesen.

**Meine Empfehlung:** Nutzen Sie eine anonyme E-Mail oder eine Wegwerfadresse, wenn Sie bei einer Anmeldung im Internet unerwünschte Werbung befürchten. Aber Achtung: Verwenden Sie Wegwerfadressen nicht bei Bestellungen im Internet oder Diensten, die Sie länger als 24 Stunden nutzen möchten. Sie erhalten sonst nach Ablauf der Adresse keine für Sie wichtigen Informationen mehr. Für solche Fälle empfehle ich Ihnen eine zweite E-Mail-Adresse. Verwenden Sie also nicht Ihre Haupt-E-Mail-Adresse dazu.

# Schritt 4: Sichern Sie Ihren Mail-Versand wie der Geheimdienst

**Soll ganz sicher niemand anderer als der Empfänger Zugriff auf Ihre Nachricht erhalten, können Sie eine Geheimdienst-Technik anwenden: Sie verschicken eine Nachricht, die nach einer bestimmten Zeit automatisch gelöscht wird. Das geht mit dem Online-Dienst Privnote und seiner deutschen Oberfläche recht einfach.**

### So verschicken Sie sich selbst zerstörende E-Mails

1. Rufen Sie **Privnote** über den Link https://privnote.com/ auf.
2. Schreiben Sie Ihre Nachricht in das Notizfeld und klicken Sie anschließend auf **Nachricht erstellen**.
3. Privnote zeigt Ihnen einen Link an. Klicken Sie ihn mit der rechten Maustaste an und wählen Sie **Kopieren**.
4. Öffnen Sie in Ihrem E-Mail-Programm eine neue Nachricht. Fügen Sie mit der Tastenkombination Strg+V oder über **Bearbeiten** und **Einfügen** den Link in Ihren Text ein. Dann schicken Sie diese Nachricht ab.

Sobald der Empfänger Ihrer E-Mail auf diesen Link klickt, wird ihm Ihre Nachricht angezeigt und danach sofort gelöscht.

# Schritt 5: Verschlüsseln Sie Ihre E-Mails und stoppen Sie so den Zugriff durch Kriminelle

**Die Schritte 1 bis 4 dienen vor allem Ihrer Sicherheit. Sie werden dadurch vor Konten-Hacks sowie vor unverlangten Werbe- und Betrugs-Mails geschützt. Mit Schritt 4 haben Sie mit den sich selbst zerstörenden E-Mails eine erste Maßnahme kennengelernt, um Ihre E-Mail-Inhalte vor unbefugten Zugriffen zu schützen. Eine zweite Methode ist das Verschlüsseln wichtiger E-Mail-Texte und -Anhänge. Diese sind dann erst nach Eingabe eines Kennworts lesbar. Das gewährleistet eine hohe Sicherheit. Office-Dokumente verschlüsseln Sie mit ein paar Mausklicks, für die Mail-Texte empfehle ich Ihnen die kostenlose Version des Tools aborange Crypter.**

### Verschlüsseln von Word- und Excel-Dokumenten

Sensible Informationen befinden sich sehr häufig in Dokumenten, die mit Microsoft Word (Textverarbeitung) oder Microsoft Excel (Tabellenkalkulation) erstellt wurden. Die aktuellen Word- und Excel-Versionen enthalten eine sichere Verschlüsselung. Sie brauchen also kein Zusatz-Tool.

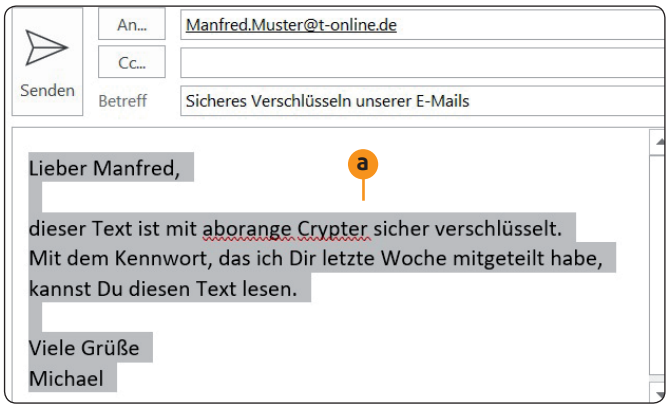
So verschlüsseln Sie Ihre Word- und Excel-Dokumente bei einem aktuellen Office 2019, 2016 oder 2013:

1. Öffnen Sie **Word** oder **Excel** und die betreffende Datei.
2. Wählen Sie **Datei**. Das Register **Information** ist geöffnet.
3. Klicken Sie auf **Dokument schützen** und **Mit Kennwort verschlüsseln**.
4. Geben Sie ein sicheres Kennwort mit einer Länge von mindestens 14 Zeichen, bestehend aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen ein, und klicken Sie auf **OK**.
5. Geben Sie das Kennwort erneut ein und klicken Sie auf **OK**.
6. Teilen Sie dem Empfänger das sichere Kennwort per Telefon oder Fax mit und versenden Sie das verschlüsselte Dokument per E-Mail.
7. Der Empfänger muss das sichere Kennwort eingeben, um das Dokument öffnen zu können. Gerät das Dokument in fremde Hände, ist der Inhalt geschützt.

**Mein Tipp:** Teilen Sie Ihren Freunden telefonisch vorab ein sicheres Kennwort für alle Ihre zukünftigen Dokumentensendungen mit. Ihre Freunde brauchen sich dann nur ein Kennwort zu merken und Sie ersparen es sich, vor jedem Dokumentenversand ein neues Kennwort mitzuteilen.

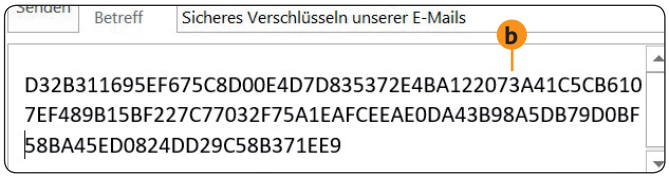
### Verschlüsseln Sie Ihre E-Mail-Texte mit dem Tool aborange Crypter

1. Laden Sie die Freeware-Version von **aborange Crypter** über den Link https://www.aborange.de/download/acrypt.exe herunter.
2. Starten Sie das heruntergeladene Installationsprogramm **acrypt.exe**. Zeigt Ihr Browser die Datei nicht sofort an, öffnen Sie mit Strg+J die Download-Liste Ihres Browsers.
3. Öffnen Sie das Tool aborange Crypter.
4. Schreiben Sie die zu verschlüsselnde E-Mail in das Textfeld oder rufen Sie diese aus den Entwürfen auf.
5. Markieren Sie den E-Mail-Text a und kopieren Sie ihn mit Strg+C in die Windows-Zwischenablage.




*Der markierte Text der noch unverschlüsselten E-Mail wird in die Zwischenablage kopiert und dort verschlüsselt.*

6. Klicken Sie in aborange Crypter auf **Zwischenablage verschlüsseln** und geben Sie zweimal Ihr sicheres Kennwort mit einer Länge von mindestens 14 Zeichen ein, bestehend aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen. Dann klicken Sie auf **OK**. Der Text in der Zwischenablage ist jetzt verschlüsselt.
7. Kopieren Sie den verschlüsselten Text mit Strg+V aus der Zwischenablage in Ihre E-Mail b und senden Sie Ihre E-Mail ab.




*Aus dem Ursprungstext ist eine Folge von Ziffern und Buchstaben geworden, die sich nur mit Ihrem Kennwort wieder in den Ursprungstext verwandeln lässt.*

### Wie der Empfänger Ihre E-Mail entschlüsselt und liest

Teilen Sie dem Empfänger Ihr Kennwort für die verschlüsselte E-Mail mit und weisen Sie ihn in die Anwendung von aborange Crypter ein. Sie können dazu die Seiten 6 und 7 dieser Ausgabe kopieren und ihm zuschicken.

1. Falls das nicht schon geschehen ist, installiert auch der Empfänger aborange Crypter.
2. Der Empfänger markiert die Ziffern- und Buchstabenfolge und überträgt diese mit Strg+C in die Windows-Zwischenablage.
3. Er ruft aborange Crypter auf und klickt auf **Entschlüsseln**, gibt das Kennwort ein und klickt auf **OK**.
4. Der Empfänger fügt den entschlüsselten Text aus der Zwischenablage in eine neue E-Mail oder ein neues Textdokument ein und kann den Text lesen. Das war schon alles!

**Meine Empfehlung:** Möchten Sie andere Dateien als Office-Dokumente verschlüsseln, verwenden Sie auch dafür aborange Crypter. Es ist ganz einfach: Sie wählen die Datei aus, klicken auf **Verschlüsseln** und geben das Kennwort zweimal ein. Der Empfänger benötigt auch hier aborange Crypter zum Entschlüsseln. Mit der für 30 € angebotenen Privatlizenz von aborange Crypter können Sie auch sich selbst entschlüsselnde Dateien erstellen. Der Empfänger benötigt dann kein aborange Crypter zum Entschlüsseln.

# Schritt 6: Beugen Sie Datenverlust vor und sichern Sie wichtige E-Mails als PDF-Datei

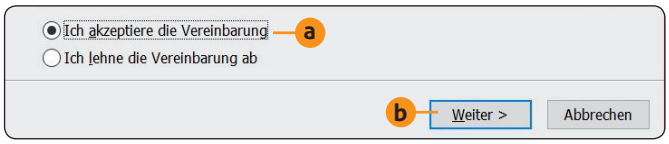
**Ihre E-Mails enthalten viele für Sie wichtige Informationen, die Sie sicher nicht verlieren möchten. Verlassen Sie sich daher nicht allein auf Ihren E-Mail-Anbieter oder Ihr E-Mail-Programm, sondern speichern Sie Ihre wichtigsten E-Mails zusätzlich in PDF-Dateien. Ihr Dreifachnutzen: Das Speichern als PDF-Datei geht so einfach wie das Ausdrucken, Ihre E-Mails sind sicher archiviert und Sie finden sie bei Bedarf immer blitzschnell wieder.**

Ist auf Ihrem PC das aktuelle Windows 10 installiert, haben Sie auch den PDF-Druckertreiber „Microsoft Print to PDF“ zur Verfügung. Drucken Sie Ihre E-Mails damit in eine PDF-Datei.

### Vor der E-Mail-Sicherung: Installieren Sie einen PDF-Drucker bei Windows 7

Windows 7 enthält keinen PDF-Druckertreiber. Haben Sie Windows 7 noch im Einsatz, installieren Sie daher PDF24 Creator. Das kostenlose Tool wurde mehrfach ausgezeichnet und ist frei von Schadprogrammen.

1. Laden Sie **PDF24 Creator** über den Link https://de.pdf24.org/pdf-creator-download.html herunter.
2. Starten Sie das heruntergeladene Installationsprogramm **pdf24-creator-8.9.1.exe**. Die Angabe **8.9.1** steht für die aktuelle Version und kann bei Ihnen daher anders lauten. Zeigt Ihr Browser die Datei nicht sofort an, öffnen Sie über die Tastenkombination Strg+J die Download-Liste Ihres Browsers.
3. Stimmen Sie den Lizenzbedingungen (a) zu, klicken Sie auf **Weiter** (b) und folgen Sie dem Assistenten mit dem freundlich dreinblickenden Schaf. Klicken Sie beim letzten Bildschirm auf **Fertigstellen**.




*Bitte beachten Sie, dass PDF24 Creator laut Lizenzbedingungen nur in der Europäischen Union genutzt werden darf; die Nutzung ist sowohl privat als auch gewerblich kostenlos.*

**Mein Tipp:** Das angebotene und kostenfreie PDF24-Konto müssen Sie nicht einrichten, um PDF-Dateien drucken zu können. Lassen Sie die Felder einfach leer, wenn Sie anonym bleiben möchten.

Nach der Installation von PDF24 Creator finden Sie bei allen druckfähigen Windows-Programmen im Drucken-Dialog den neuen Drucker **PDF 24 PDF**, mit dem Sie die PDF-Datei erstellen.

### So archivieren Sie Ihre E-Mails als PDF

Das Drucken in eine PDF-Datei unterscheidet sich nur wenig vom Drucken auf Papier. Es gibt nur zwei Unterschiede: Sie wählen statt Ihres Tintenstrahl- oder Laserdruckers einen virtuellen PDF-Drucker aus und legen fest, in welchem Ordner Ihr Windows 10 oder 7 die PDF-Datei abspeichern soll. So geht's:

**Impressum**

Ihr PC-Sicherheits-Berater, ISSN 2196-9299

Dieses monothematische Supplement „Ihr Leitfaden für Ihren sicheren E-Mail-Verkehr“ gehört zu dem Titel „Ihr PC-Sicherheits-Berater“.

Computerwissen, ein Verlagsbereich der VNR Verlag für die Deutsche Wirtschaft AG

Vorstand: Richard Rentrop

Chefredakteur: Michael-Alexander Beisecker (V.i.S.d.P.), Oberhausen

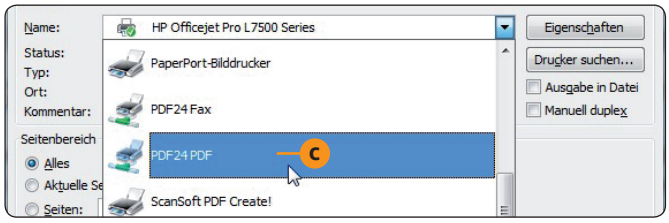
Herausgeberin: Patricia Sparacio

Adresse: Verlag für die Deutsche Wirtschaft AG, Theodor-Heuss-Str. 2-4, 53177 Bonn

Telefon: 0228/9550190, Fax: 0228/3696350

Eingetragen: Amtsgericht Bonn HRB 8165

1. Rufen Sie Ihr E-Mail-Programm, wie zum Beispiel Outlook, oder die Internetseite Ihres E-Mail-Anbieters, wie zum Beispiel Web.de, auf und melden Sie sich bei Ihrem E-Mail-Konto an.
2. Öffnen Sie die gewünschte E-Mail und klicken Sie das Symbol zum Drucken an. Oder Sie wählen den entsprechenden Befehl wie **Datei** und **Drucken**. Häufig lässt sich die Druckfunktion auch per Strg+P aufrufen.
3. Wählen Sie im Feld **Name** den PDF-Drucker aus (C) und klicken Sie auf **OK**. Es öffnet sich der Assistent des PDF-Druckers. Klicken Sie dort auf **Als PDF speichern** und wählen Sie den Ordner zum Speichern.




*Zum Drucken als PDF-Datei wählen Sie **PDF24PDF** aus.*

### Speichern Sie Ihre E-Mails in den PDF-Dateien geordnet und systematisch ab

Speichern Sie die erstellten PDF-Dateien nach Themen/Absendern in verschiedenen Ordnern. Zum Anlegen dieser Ordner verwenden Sie den Windows-Explorer.

Anschließend finden Sie die gerade benötigten E-Mails über die Windows-Suche sekundenschnell wieder. Sie sind also nicht auf Ihr E-Mail-Programm und dessen anfällige Datenbank angewiesen.

**Meine Empfehlung:** Durch das Speichern auf Ihrer Festplatte sind Sie vor Datenverlust geschützt, selbst wenn Ihr E-Mail-Anbieter Probleme haben sollte. Vergessen Sie aber nicht, die PDF-Dateien zusammen mit allen anderen wichtigen Daten auf Ihrer Festplatte regelmäßig auf einer externen USB-Festplatte zu sichern. Haben Sie Fragen zur Datensicherung, beraten meine Mitarbeiter aus der Redaktion und ich Sie gern über den Computerwissen Club: https://club.computerwissen.de.

# Schritt 7: Schützen Sie sich vor Skript-Angriffen und stellen Sie den E-Mail-Empfang auf Text um

**E-Mails lassen sich durch Hintergründe, Bilder, unterschiedliche Schriftarten und Formatierung wie gedruckte Texte oder professionelle Webseiten gestalten. Das ist sehr schön anzusehen, birgt aber eine große Gefahr: Die E-Mails sind in der Seitenbeschreibungssprache HTML programmiert, über die sich Skripte, also Programme, ausführen lassen. Eine Sicherheitslücke in Ihrem E-Mail-Programm oder bei Windows 10 oder 7 reicht aus und Ihr PC ist infiziert. Empfangen Sie Ihre E-Mails daher zu Ihrem Schutz voreingestellt immer im Text- und nicht im HTML-Format. Wie Sie hierfür vorgehen, zeige ich Ihnen in diesem Beitrag.**

So stellen Sie bei den aktuellen Outlook-Versionen 2019, 2016 und 2013 das Text-Format für Ihre eingehenden E-Mails ein:

1. Öffnen Sie das Menü **Datei**, wählen Sie **Optionen** und klicken Sie links unten auf **Trust Center**.

**Mein Sicherheits-Tipp:** Der erweiterte Support für Office 2010 und damit auch für Outlook 2010 endet am 13.10.2020. Danach erhalten Sie keine Sicherheitsupdates mehr. Arbeiten Sie noch mit Office 2010, führen Sie daher schnellstmöglich ein Update auf Office 2019 durch.

2. Klicken Sie auf **Einstellungen für das Trust Center**.
3. Wählen Sie links **E-Mail-Sicherheit** und aktivieren Sie rechts unter **Als Nur-Text lesen** die Option **Standardnachrichten im Nur-Text-Format lesen**.
4. Der Missbrauch digitaler Signaturen ist selten, aber wenn Sie keinerlei Risiko eingehen möchten, aktivieren Sie zusätzlich die Option **Digital signierte Nachrichten im Nur-Text-Format lesen**.

Im reinen Text-Format werden keine Bilder angezeigt und die Texte sind bei Werbe-Mails und Newslettern teilweise schwer lesbar. So wechseln Sie ins HTML-Format:

- Vertrauen Sie einer eingehenden E-Mail, klicken Sie zum Wechsel in das HTML-Format in die Infoleiste dieser E-Mail und wählen **Bilder herunterladen**.
- Sie können in der Infoleiste zur HTML-Darstellung je nach Ihrer Outlook-Version auch **Ansicht im Browser** oder **Als HTML anzeigen** wählen.

**Meine Empfehlung:** Verwenden Sie ein anderes E-Mail-Programm als Outlook, nehmen Sie die Umstellung auf das Text-Format in den dortigen E-Mail-Optionen vor. Sie finden diese zum Beispiel bei Thunderbird im Menü **Ansicht** unter **Nachrichteninhalt**. Dort stellen Sie **Reiner Text** oder **Vereinfachtes HTML (nicht so sicher)** ein. Haben Sie Fragen zum sicheren Einstellen Ihres E-Mail-Programms, beraten meine Mitarbeiter aus der Redaktion und ich Sie gern über den Computerwissen Club: https://club.computerwissen.