

@ E-Mail



# Computer- Stammtisch



# @ E-Mail



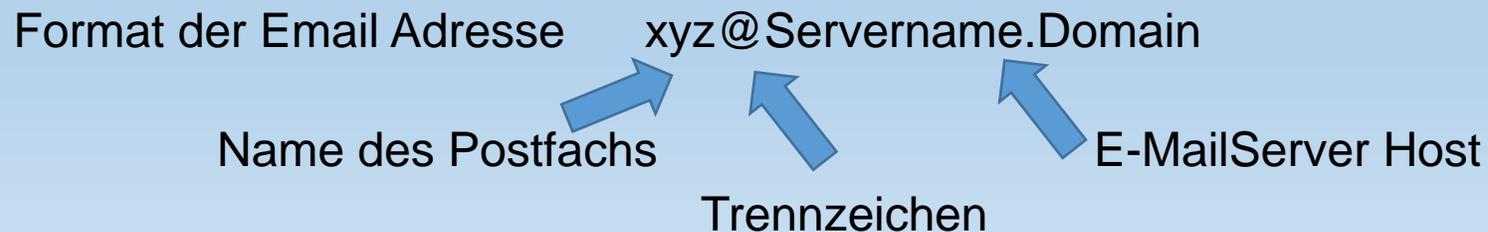
Der Name E-Mail ist ein Kurzform für den englischen Begriff electronic mail das heißt elektronische Post.

E-Mail ist auch heute noch ein viel benutzter Internetdienst um Informationen, Bilder, Dateien und Links zu versenden.

E-Mail ist ein asynchroner Nachrichtendienst, der Empfänger und der Sender einer Information müssen nicht zur selben Zeit im Internet angemeldet sein.

Die erste E-Mail wurde 1971 versandt, da war das Internet noch ein Netzwerk von Universitätsrechnern, und hieß ArpaNet.

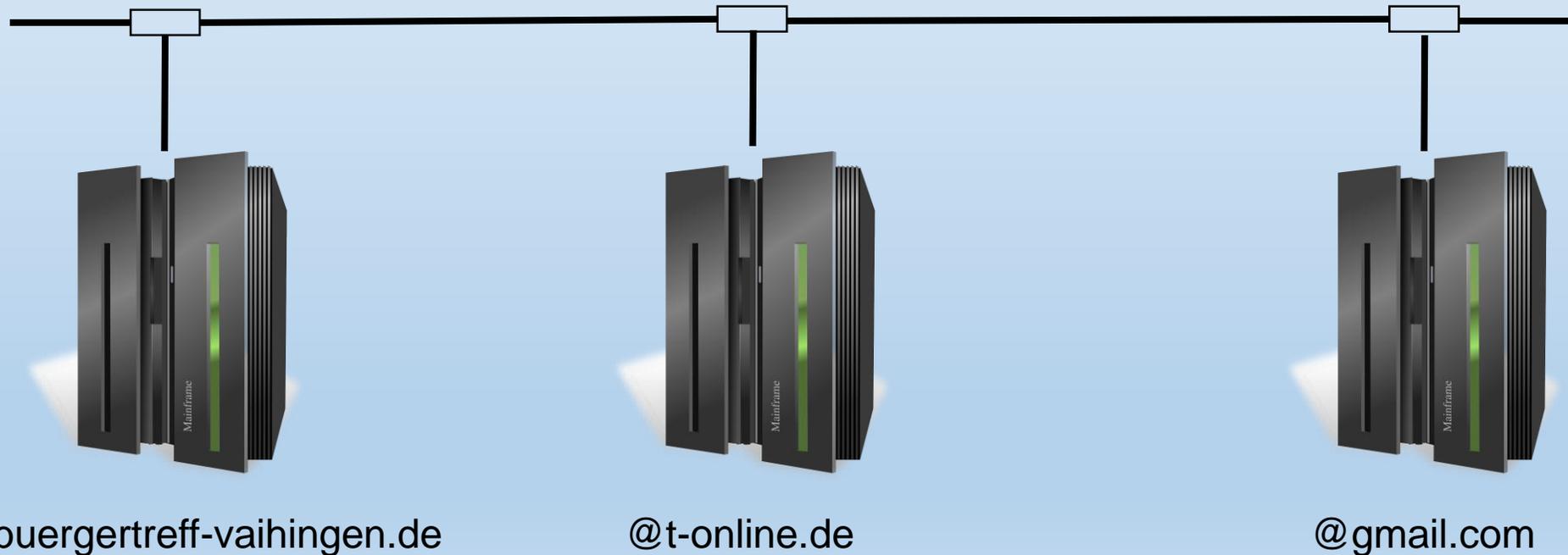
E-Mail war viele Jahre der Dienst auf dem ArpaNet, der die meisten Daten übertragen hat.



# @ E-Mail



E-Mails sind Nachrichten, die in einem definierten Format mit dem Protokoll SMTP **S**imple **M**ail **T**ransfer **P**rotocol über das Internet zwischen Servern ausgetauscht werden.



# @ E-Mail

Um ein Mail zu schreiben und in den Startserver zu laden, gibt's zwei Möglichkeiten:

1. Mailprogramm auf dem eigenen Computer.



SMTP

HTTPS

2. Browser auf dem eigenen Computer und Mailprogramm auf dem Mailserver.



## @ E-Mail



Beim E-Mail-Schreiben gibt es, außer der Benutzerfreundlichkeit der unterschiedlichen Programme, keine grundsätzlichen Vor- oder Nachteile der zwei Möglichkeiten.

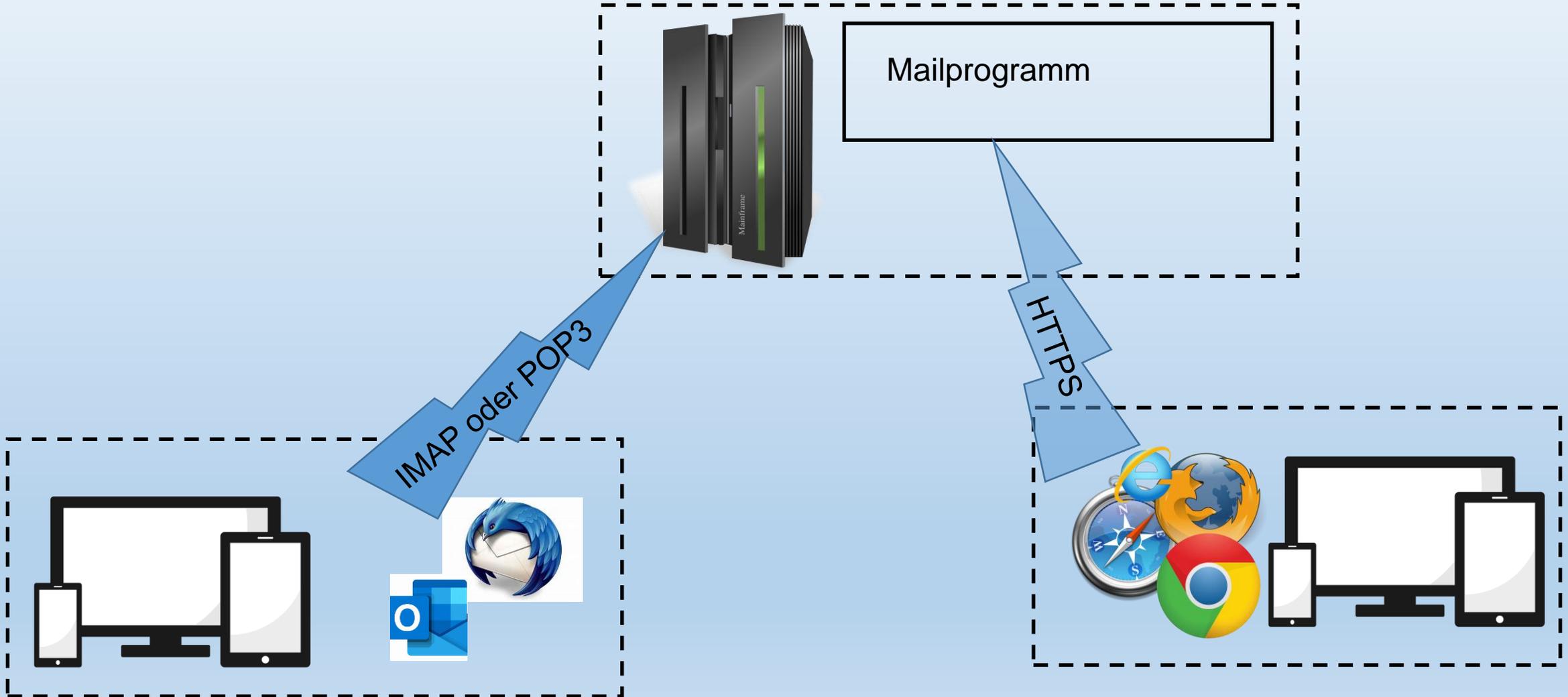
Bei Möglichkeit 2, Verwendung des E-Mailprogrammes, oder besser der Oberfläche, auf dem Server, ist während der kompletten Erstellung der E-Mail eine Internetverbindung erforderlich.

Bei Verwendung eines Mailprogramms auf dem eigene PC können E-Mails auch offline geschrieben werden. Sie werden dann nach Herstellung der Internetverbindung auf einmal an den Mailserver übertragen.

# @ E-Mail



Um ein E-Mail zu empfangen, gibt es drei Möglichkeiten:



## @ E-Mail



Zum Empfang von E-Mails mit dem E-Mail-Programm des eigenen Rechners werden hauptsächlich zwei Protokolle angewendet.

**1. IMAP.** Hier verbleiben die E-Mails - nach der Übertragung auf den eigenen Rechner - auf dem Mailserver, sie können also beliebig oft und von beliebig vielen Geräten heruntergeladen werden.

Der Speicherplatz auf dem Mailserver muss beobachtet und bei Bedarf Mails manuell gelöscht werden.

**2. POP3** ist das ältere Protokoll, es ist so ausgelegt, dass der Server die E-Mails zur Übertragung an den eigenen Rechner zur Verfügung stellt und nach der positiven Rückmeldung, dass die E-Mails auf dem eigenen Rechner gespeichert sind, löscht. Es gibt inzwischen Server, die mit einem abgewandelten POP 3 Protokoll arbeiten und die E-Mails nach einer POP3 Übertragung auf dem Mailserver belassen.

Werden die E-Mails mit dem Browser über die E-Mail-Oberfläche des Mailservers gelesen, verbleiben sie auf dem Server und müssen bei Bedarf auf den eigenen Rechner heruntergeladen werden.

**IMAP** = Internet Message Access Protocol; **POP3** = Post Office Protocol

# @ E-Mail



	IMAP	POP3	Mail mit Browser lesen
Postfachgröße auf Mailserver managen.	✗	✓	✗
Mails mit mehreren Geräten lesen	✓	✗	✓
Sicherheit gegen Computerviren	-	-	+

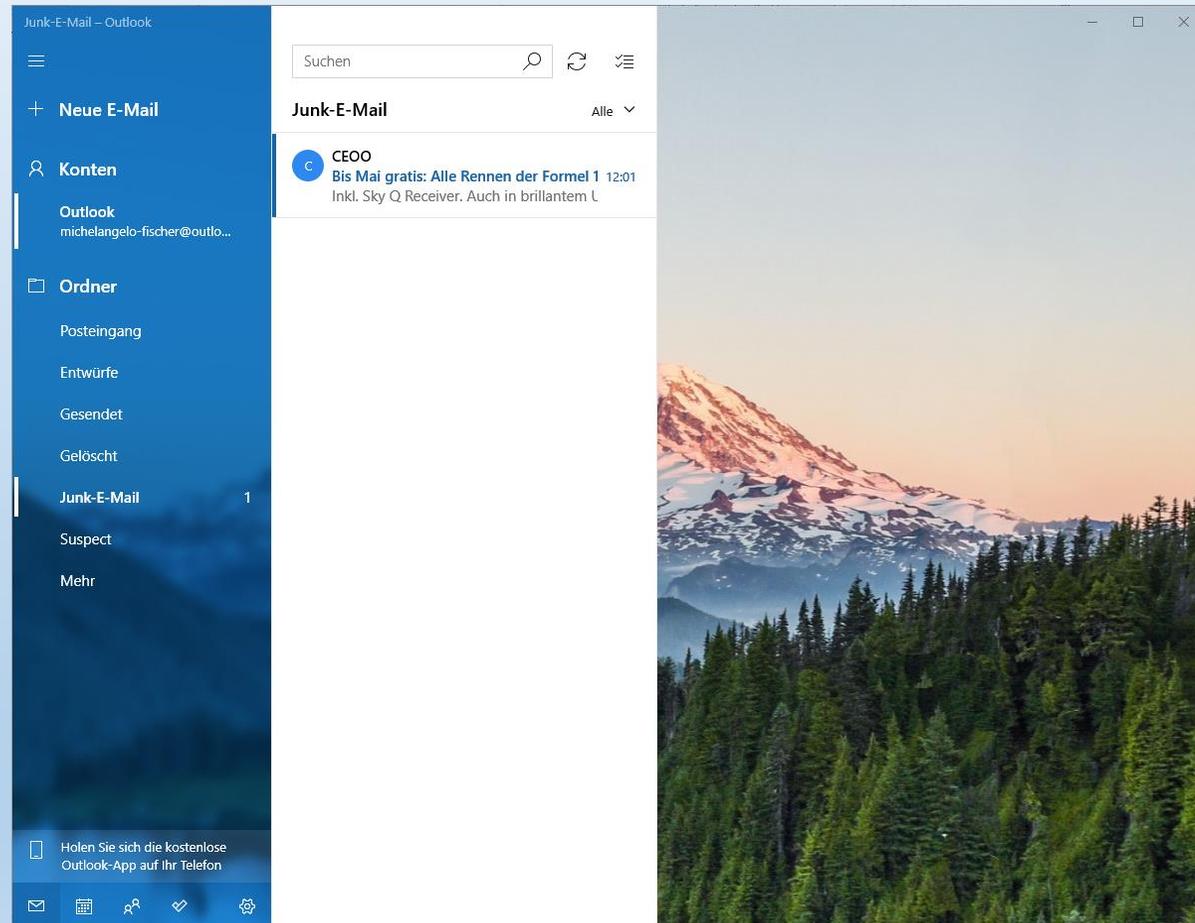
# @ E-Mail



Das **Windows Mailprogramm** gehört zum Standardumfang von Windows.

Es bringt neben der Möglichkeit, ein E-Mail-Archiv anzulegen, einen Kalender und ein Kontakte-Verzeichnis mit.

Es können mehrere E-Mail-Konten integriert werden.



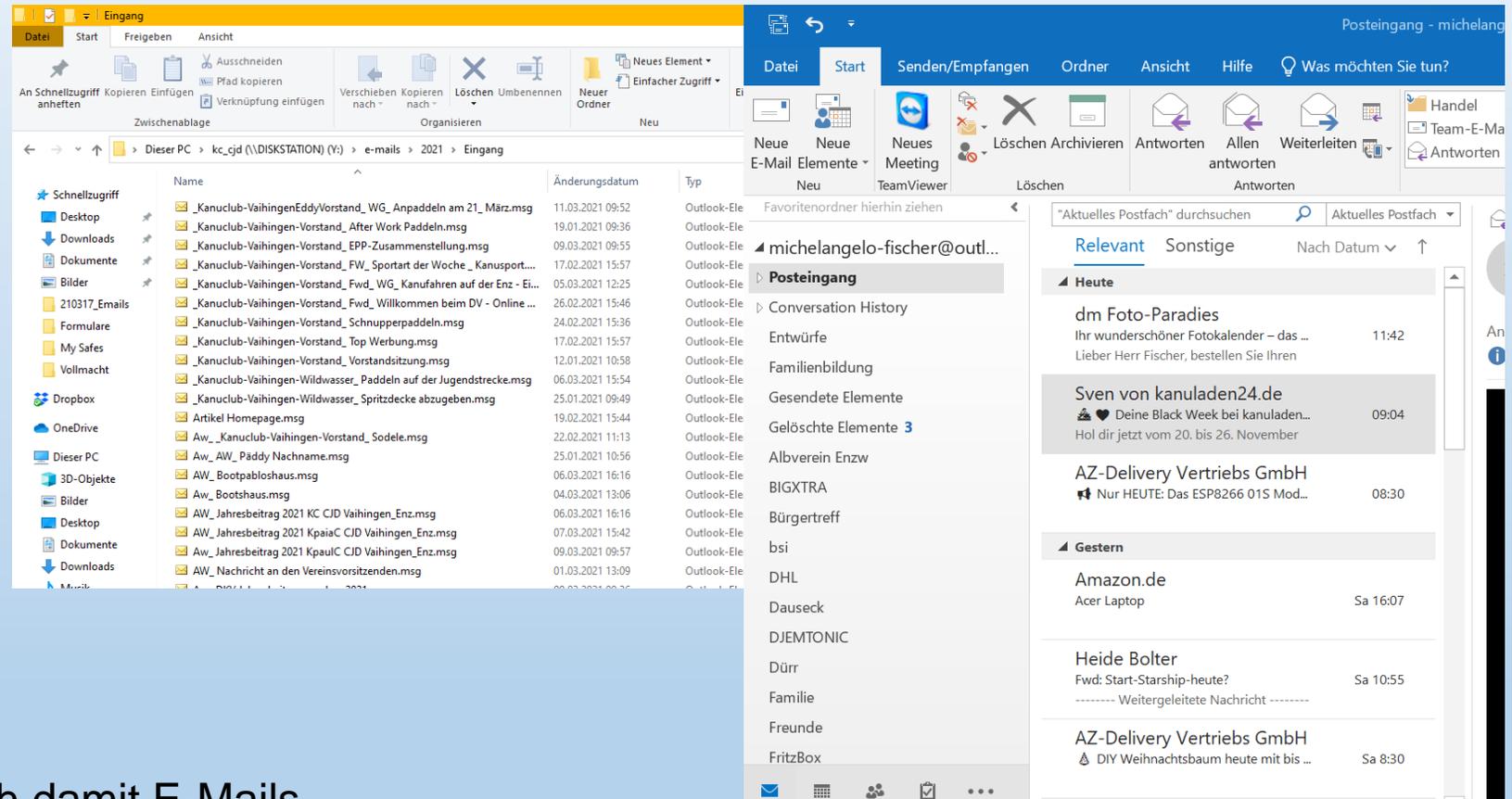
# @ E-Mail



Microsoft Outlook muss man kaufen.

Es kann alles, was ein Mailprogramm können muss, inklusive Kalender und Kontakte-Verzeichnis.

E-Mails können aus dem Mailprogramm direkt ins Dateiverzeichnis abgelegt werden. Outlook verwendet dazu ein firmenspezifisches Datenformat. Dateierweiterung .msg.



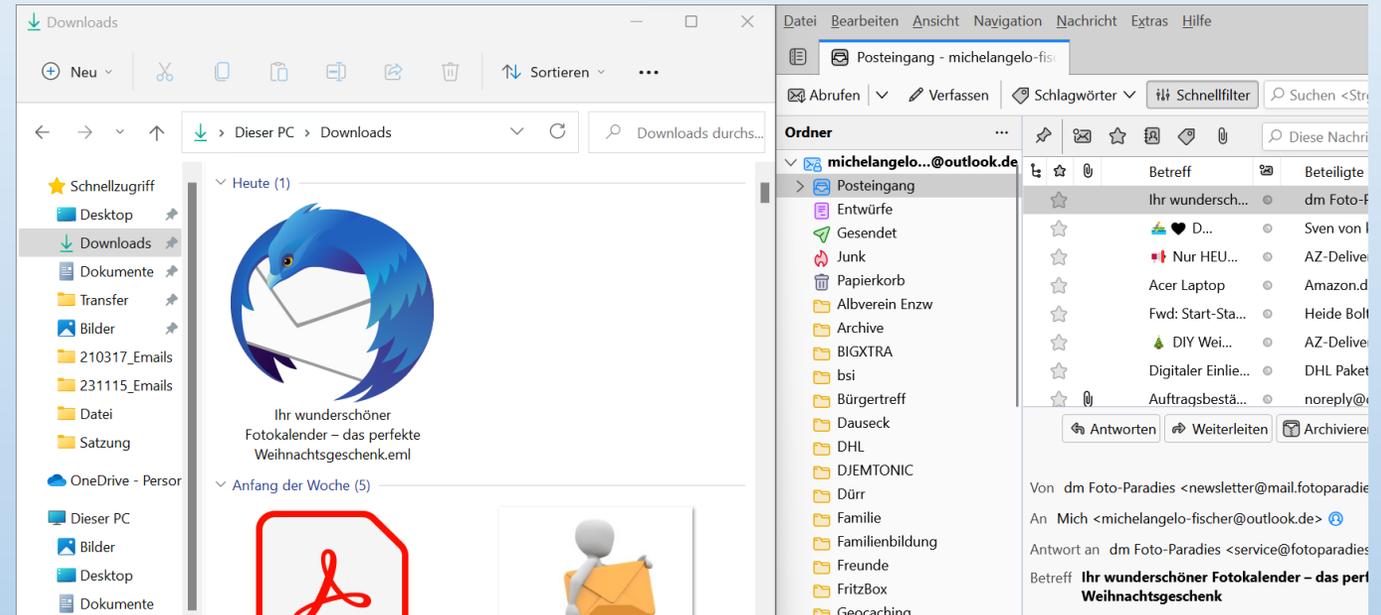
Für mich ein wichtiges Feature, da ich damit E-Mails in themenbezogenen Ordnern unterbringen kann.

# @ E-Mail



**Modzilla Thunderbird** unter GNU Lizenz ist kostenlos für Privatnutzer.

Auch hier funktioniert die direkte Mailablage im Windows Dateisystem. Das verwendete Datenformat wird auch von anderen Mailprogrammen unterstützt. Dateiendung **.eml**.



@ E-Mail



Wie sicher sind E-Mails?

Unverschlüsselte Mails sind so sicher wie eine Postkarte, die aus Gründen der Übertragung übers Internet bei jeder Menge Leuten zum Weitertransport vorbei geschickt wird.

Das unverschlüsselte Mail kann an jeder Zwischenstation komplett gelesen und gespeichert werden.

Verschlüsselte Mails sind so sicher wie ein Brief, der bei jeder Menge Leute vorbei geschickt wird.

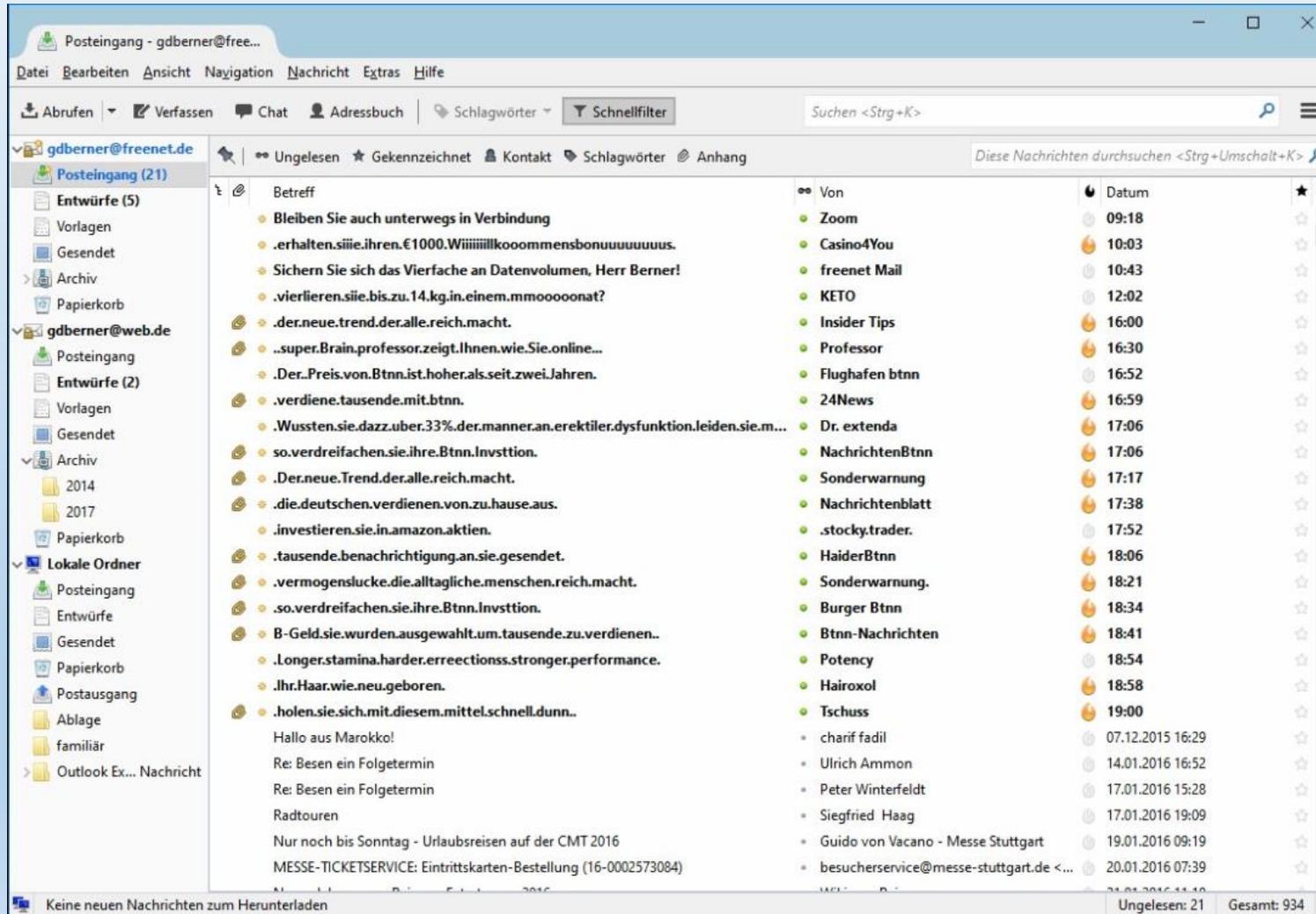
Bei der verschlüsselten Mail kann an jeder Zwischenstation der Absender und alle Empfänger gelesen werden.

Der Inhalt ist nicht lesbar.

# @ E-Mail



## SPAM die Geißel des Mailverkehrs



Im Jahr 2007 waren 90% der weltweit verschickten E-Mails SPAM.

## @ E-Mail



### AntiSPAM-Massnahmen:

Handelt es sich beim SPAM um aus Versehen oder aus Unachtsamkeit bestellte Newsletter, kann man diese über den Link in der Mail abbestellen. Aber bitte wirklich nur dann.

SPAM-Mails nie beantworten, der Absender erhält mit jeder Antwort die Bestätigung, dass er eine gültige und in Betrieb befindliche E-Mail-Adresse als Ziel gewählt hat.

Mailadressen nicht unnötig veröffentlichen, speziell das Internet wird nach Mailadressen abgescannt.

SPAM-Filter oder Zusatzsoftware können nicht wirklich alle SPAM E-Mails ausfiltern und filtern häufig auch E-Mails aus, auf die man dringend wartet.

Der empfangende Mailprovider wendet im Normalfall AntiSPAM-Maßnahmen an und kennzeichnet SPAM-Mails, die von seinen Filtern und Algorithmen erkannt werden.

## @ E-Mail



Gefährliche E-Mails:

Die aktuell beliebtesten Angriffe sind

**Mails mit verseuchtem Anhang**, Viren und Trojanern, die beim Öffnen des Anhangs auf den Rechner installiert werden.

Schutzmaßnahme: nur Anhänge von Mails öffnen, die einem vertrauenswürdig erscheinen.  
Absender ist bekannt, Mail wird erwartet etc.

**Mails mit gefährlichen Links**, Links die auf Webseiten führen, von denen Daten abgegriffen werden, oder Viren oder Trojaner auf dem Rechner installieren.

Schutzmaßnahme: nur auf Links in Mails klicken, die einem vertrauenswürdig erscheinen,  
Absender ist bekannt oder die E-Mail wird erwartet.

## @ E-Mail



Möglichst E-Mail im Nur-Text-Modus verwenden, sicherheitshalber zum Lesen aber auch zum Senden.

Die E-Mails sehen zwar nicht mehr so attraktiv aus, dafür ist aber nur noch Text drin, keine Bilder und keine Formatierungen, aber auch keine versteckten Programme die heruntergeladen werden, wenn man das Mail liest.

Links sind noch aktiv, wenn man drauf klickt, man sieht aber, wo der Link hinführt.

Keine vertrauenswürdige Bank wird Ihnen eine E-Mail schicken, um Kontodaten oder noch schlimmer TANs abzufragen.

Gewinnversprechen sind immer falsch, um bei einer Lotterie gewonnen haben, müssen sie wenigstens dran teilgenommen haben.

Es gibt keinen Multimillionär, der Ihnen größere Teile seines Vermögens überschreiben will.

## @ E-Mail



Sind Sie Funktionsträger in einem Verein?

Ich bekomme Mails, in denen ich aufgefordert werde, Zahlungen zu tätigen, unterschrieben vom ersten Vorsitzenden des Kanuclubs mit dessen Mailadresse als Absender.

Diese Methode wird vornehmlich gegenüber Firmenmitarbeitern angewendet, Privatleute sind aber auch nicht sicher davor.

Machen Sie in Ihrem Umfeld aus, dass auf solche Mails hin nichts passiert, fragen Sie bevor sie Zahlungen ausführen beim Auftraggeber telefonisch nach, bitte nicht per Mail.

Diese Masche hat schon Millionen eingebracht.

Der Austausch der Absender-Mailadresse um eine falsche Identität vor zu gaukeln ist überhaupt kein Problem, das kann man mit jedem Mailprogramm machen.

# @ E-Mail



The screenshot shows a Gmail interface in a browser. The browser's address bar displays the URL `https://mail.google.com/mail/u/0/#inbox/FMfcgxlswFwrWCFMcLkbWLSNRdQJgZr`. The Gmail header includes the search bar "In E-Mails suchen" and the "Keine Synchronisierung" status. The left sidebar shows navigation options: "Schreiben", "Posteingang", "Markiert", "Zurückgestellt", "Gesendet", "Entwürfe", "Mehr", "Meet", and "Hangouts". The main content area displays an email from "Angela@bundeskanzlerin.de" with the subject "Schönen Gruß aus Berlin". The email body contains the text: "Ein Hallo an den Bürgertreff Weiter so", "Mit freundlichen Grüßen Angela Merkel", and "Bundeskanzlein". A "[Message clipped]" notice is present with a link to "Vollständige Nachricht ansehen". At the bottom of the email, there are buttons for "Antworten" and "Weiterleiten".

# @ E-Mail

Wenn Sie mithelfen wollen, die Polizei über aktuell im Umlauf befindliche, gefährliche E-Mails zu informieren, senden Sie die verdächtigen Mails an [trojaner@polizeilabor.de](mailto:trojaner@polizeilabor.de)



The screenshot shows a web browser window with the URL <https://www.polizei-praevention.de/themen-und-tipps/serviceangebot/spammails-zur-polizei>. The page header includes the logo of the Landeskriminalamt Niedersachsen and navigation links for 'Aktuelles', 'Themen und Tipps', 'Mediathek', and 'Ihre persönliche Frage'. A 'Nach oben' button is visible in the top right.

**SERVICEANGEBOT**

- Datencheck
- Ihr Weg zur Strafanzeige
- Spammails zur Polizei**
- ZAC

**AKTUELLES NACH THEMEN**

- Amazon, Android, Apple, App Store
- Betrug, Bewerbung, Corona
- Cyberpolizei, ebay, Emotet, Einzeltrick
- Erpressung, Facebook, Fakeshops
- Falscher Polizeibeamter, Finanzagent
- Gandcrab, Geldwäsche, Identitätsdiebstahl
- Jobangebote, Kettenbrief, Mail

**Anleitung für Ihre Spamweiterleitung an uns**

Die Polizei Niedersachsen bietet Ihnen im Bereich Cybercrime einen Service an. Jeder Internetnutzer, der auffällige/betrügerische Spammails bekommt, die möglicherweise auch Schadsoftware enthalten, kann dazu beitragen, die Polizei darüber zu informieren (KEINE ANZEIGENERSTATTUNG!).

Leiten Sie einfach die verdächtige Mail unkommentiert und ohne Veränderungen an die Mailadresse **trojaner(at)polizeilabor(dot)de**

(Die bisherige Mailadresse trojaner@polizei-praevention.de sollte nicht mehr benutzt werden, da eine Weiterleitung aufgrund diverser Filter beim Provider, die wir leider nicht beeinflussen können, nicht garantiert werden kann.)

Achten Sie bitte darauf, dass persönliche, automatische Signaturen, z.B. eigener Firmenname, innerhalb des Mailtextes von Ihnen vor dem Versenden entfernt werden, damit dies nicht zu Fehleinschätzungen bei der Auswertung kommt. Fügen Sie bitte auch keine Kommentare oder Veränderungen hinzu. Dies ist besonders wichtig, da diese Mails u.a. automatisiert ausgewertet werden.

Wenn Sie jedoch den Original-Header (erweiterter Briefkopf) auslesen können, können Sie diesen gern der Mail hinzufügen.

Lesen Sie auch aufmerksam die weiteren Infos für diesen Dienst durch.

Sollten Sie allerdings persönliche Fragen zu Cybercrime haben, so stellen Sie Ihre persönliche Frage an uns über das Formular **→ hier**.

## Wichtig! Generelle Sicherheitshinweise

- Beachten Sie weiterhin folgende wichtige Verhaltenshinweise:
- Öffnen Sie keine Anhänge/Links von unbekanntem Versendern!
- Nutzen Sie eine aktuelle Antivirensoftware, die auch Ihren ein- und ausgehenden Postverkehr überwacht!
- Nutzen Sie die Möglichkeit, Mails online bei Ihrem Provider über den Browser zu lesen? Auf dortige Mailanhänge hat Ihr lokales Antivirenprogramm keinen Zugriff. Dort prüfen ggf. nur die Provider.
- Nicht jede Schadsoftware in einer Mail wird sofort durch Antivirenprogramme erkannt. Auch diese müssen erst mit Updates versorgt werden. Ggf. zeigt eine erneute Prüfung z.B. 24 Stunden später ein anderes Ergebnis.
- Halten Sie Ihr Betriebssystem und Ihre Software auf einem aktuellen Stand.
- Sollten Sie unbekannte Anhänge aus einer Mail z.B. für eine Überprüfung mittels Antivirensoftware oder über [www.virustotal.com](https://www.virustotal.com) auf Ihrem Desktop oder an anderer Stelle zwischengespeichert haben, so vergessen Sie nicht, diese Datei im Anschluss zu löschen, damit sie nicht später versehentlich geöffnet wird! Löschen Sie auch den Papierkorbinhalt im Anschluss.

# @ E-Mail



Wer noch mehr nachlesen möchte, hier ein [Link zu einem Artikel](#) beim BSI (Bundesamt für Sicherheit in der Informationstechnik), der sich mit diesem Thema beschäftigt.

← ↻ 🔒 https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen... 🗖️ 🔊 📄 ☆ ⚙️ | 📄 ☆ 🔍

 Das BSI Themen IT-Sicherheitsvorfall Karriere

Hinweis zur Verwendung von Cookies

Das BSI speichert keine personenbezogenen Daten der Webseitenbesucher. Details in unserer [Datenschutzerklärung](#)

## Nutzen Sie die E-Mail wirklich sicher?

Für die sichere Nutzung von E-Mails ist es nicht erforderlich, zusätzliche Software zu installieren. Viele E-Mail-Provider bieten Webmail-Zugänge an, die Sie über den Internet-Zugang mit Ihrem Browser nutzen können. Wichtig ist, auf eine verschlüsselte Verbindung (HTTPS) zum Postfach zu achten, um von den Schutzmechanismen Ihres Browsers zu