

Wer liest in meinen E-Mails?

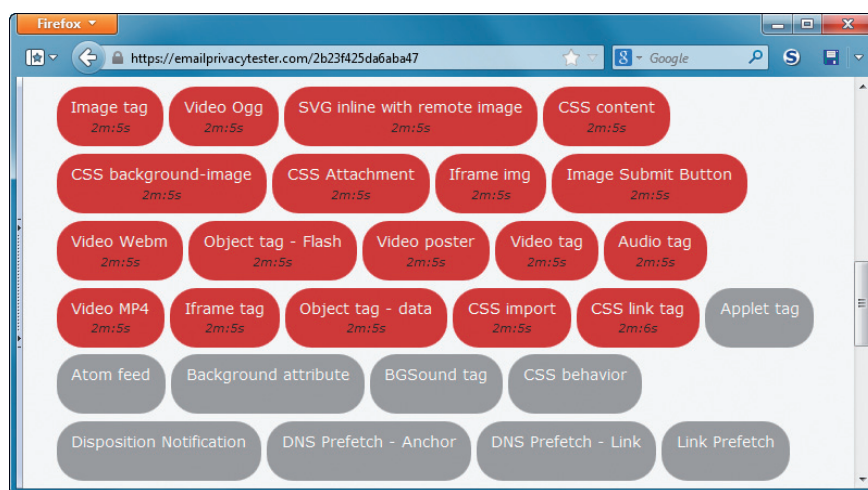
Versteckte Tracking-Elemente in E-Mails verraten dem Absender einer Nachricht, wann, wo und womit Sie Ihre E-Mails lesen – auch dann, wenn Sie bewusst keine Lesebestätigung versendet haben.

E-Mails lassen sich problemlos so manipulieren, dass der Absender auch gegen Ihren Willen erfährt, dass Sie die Mail geöffnet haben. Das funktioniert auch, wenn Sie keine Lesebestätigung senden.

Um herauszufinden, ob und wann Sie beispielsweise einen Newsletter geöffnet haben, betten manche Absender versteckte Tracking-Elemente in die Nachricht ein. Ein solches Tracking-Element kann etwa bewirken, dass beim Öffnen der Nachricht automatisch ein kleines Bild von einem Server des Absenders heruntergeladen wird.

So erfährt er, dass die E-Mail geöffnet wurde. Außerdem erfährt der Absender die genaue Uhrzeit und Ihre IP-Adresse. Mit Hilfe der IP-Adresse kann er dann sogar per Geolocation Ihren Aufenthaltsort ermitteln. Diese Daten lassen sich leicht sammeln und zu Empfänger-Profilen zusammensetzen.

Der Artikel zeigt, wie Sie Ihr eigenes E-Mail-Programm prüfen und herausfinden, welche Tracking-Elemente es ohne Ihr Wissen ausführt. Einige der



Tracking-Elemente: Die Webseite [www.emailprivacytester.com](https://emailprivacytester.com/2b23f425da6aba47) zeigt in Rot an, welche Tracking-Elemente ein Webmail-Dienst oder ein E-Mail-Client zulässt (Bild B)

beliebtesten Mail-Programme und Webmail-Clients haben wir bereits getestet und die Ergebnisse in zwei Tabellen zusammengefasst.

Verstecktes Tracking

Ein typisches Tracking-Element ist das Image tag. Dabei handelt es sich um das bereits erwähnte Bild, das meist aus wenigen unsichtbaren Pixeln besteht. Das Bild selbst ist auf dem Server des Absenders gespeichert.

Wenn der Empfänger die E-Mail öffnet, lädt der Webmail-Dienst beziehungsweise der E-Mail-Client das Bild vom Server des Absenders herunter. Dadurch kennt der Server die Uhrzeit des E-Mail-Abrufs und die IP-Adresse des Empfängers. Diese Vorgehensweise nennt sich E-Mail-Tracking. Sie ist

besonders für Werbetreibende interessant und wird daher in erster Linie im Marketing genutzt, um herauszufinden, ob Empfänger die versendeten E-Mails anklicken und welche Inhalte sie interessieren.

Ähnliche Tracking-Elemente lassen sich auch in Anhängen oder Links der E-Mail einbauen, sodass der Absender weiß, wann und wo der Empfänger Anhänge geöffnet hat und welche Links sein Interesse geweckt haben.

Allerdings verhalten sich Webmail-Dienste und E-Mail-Clients unterschiedlich bei der automatischen Weiterleitung von Tracking-Informationen.

Auf Seite 125 und 126 finden Sie zwei Übersichten mit Webmail-Diensten beziehungsweise E-Mail-Clients. Sie zeigen, welche Tracking-Elemente zum

Inhalt

Wer liest in meinen E-Mails?

■ Webmailer und E-Mail-Clients	S. 125
GMX, Google Mail, Yahoo und Co.	S. 126
Outlook, Thunderbird und Co.	S. 127
■ Fazit	S. 127
■ Zusatz-Infos	
Webmail-Dienste: Tracking-Elemente	S. 125
E-Mail-Clients: Tracking-Elemente	S. 126

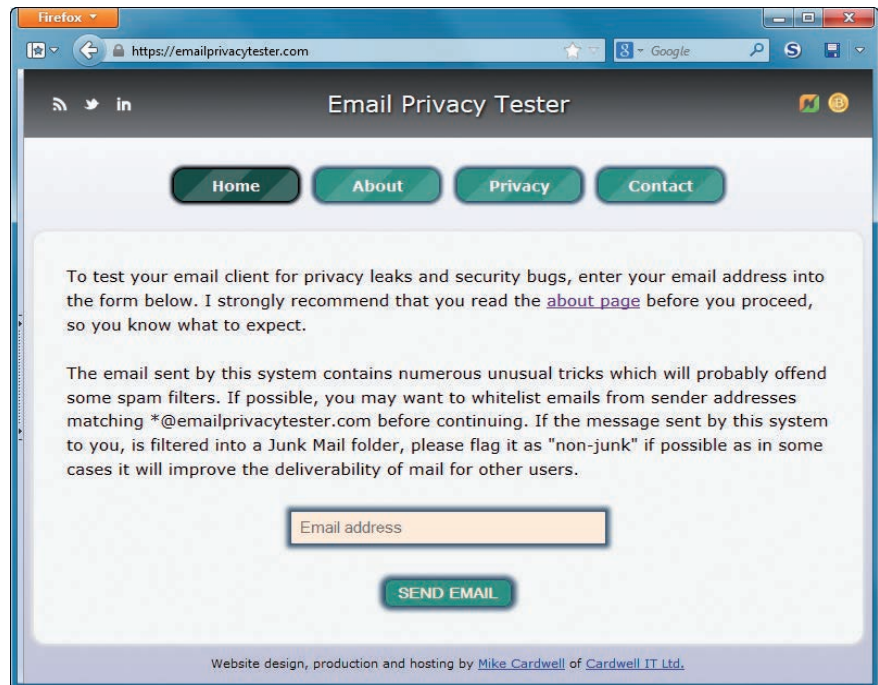
Einsatz kommen, wenn Sie eine E-Mail anklicken oder den Abruf externer Inhalte erlauben.

Webmailer und E-Mail-Clients

Die Webseite Email Privacy Tester ermittelt mit Hilfe einer Test-E-Mail, ob Webmail-Dienste und E-Mail-Clients automatisch die Tracking-Elemente der E-Mail abrufen und damit Informationen über den E-Mail-Empfänger an den Absender schicken.

Um eine eigene E-Mail-Adresse zu testen, öffnen Sie die Webseite www.emailprivacytester.com und tippen die Adresse in das Eingabefeld ein (Bild A). Nach einem Klick auf „SEND EMAIL“ verschickt die Webseite eine E-Mail mit einer PNG- und einer SVG-Datei im Anhang. Erstere hat eine doppelte Dateiendung, letztere enthält ausführbaren Code in Form von Javascript.

Nachdem die E-Mail versendet wurde, zeigt Email Privacy Tester eine Liste aller 39 Tracking-Elemente an, die in der Test-E-Mail enthalten sind, darun-



Email Privacy Tester: Geben Sie hier Ihre E-Mail-Adresse ein, um zu prüfen, ob Ihr Mail-Programm heimlich Daten übermittelt (Bild A)

ter auch die bekannte gewöhnliche Le-sebestätigung. Zunächst sind alle Elemente grau hinterlegt.

Wenn Sie nun in Ihrem Webmail-Dienst oder E-Mail-Client auf die Mail

klicken und die Elemente grau bleiben, dann sind keine Daten an den Absender gegangen. Ändert sich die Farbe in Rot, dann haben der Webmail-Dienst oder E-Mail-Client das Tracking- ▶

Webmail-Dienste: Ausgelöste Tracking-Elemente

Die Tabelle zeigt in der ersten Zeile, welche Tracking-Elemente übermittelt werden, wenn Sie in Ihrem Postfach auf eine E-Mail klicken. In der zweiten Zeile steht, welche Tracking-Elemente aktiviert werden, wenn Sie das Nachladen externer Inhalte erlauben.

	Freenet	GMX	Google Mail	Outlook.de	T-Online	Web.de	Yahoo
E-Mail angeklickt	–	<ul style="list-style-type: none"> • Background attribute • CSS back-ground-image • Image tag 	<ul style="list-style-type: none"> • CSS back-ground-image • Image Submit Button • Image tag 	<ul style="list-style-type: none"> • DNS Prefetch – Achor • DNS Prefetch – Link • SVG inline with remote image 	<ul style="list-style-type: none"> • Audio tag • Image Submit Button • Image tag • Video Ogg • Video MP4 • Video poster • Video tag • Video Webm 	<ul style="list-style-type: none"> • Background attribute • CSS back-ground-image • Image tag 	–
Externe Inhalte erlaubt	<ul style="list-style-type: none"> • CSS back-ground-image • Image tag 	¹⁾	¹⁾	<ul style="list-style-type: none"> • Autio tag • Image Submit Button • Image tag • Video mp4 • Video Ogg • Video poster • Video tag • Video Webm 	¹⁾	¹⁾	<ul style="list-style-type: none"> • CSS back-ground-image • Image Submit Button • Image tag

¹⁾ Option nicht angezeigt; es wurden die Standardeinstellungen der Webmail-Dienste verwendet

Element geladen und damit Informationen an den Absender geschickt (Bild B).

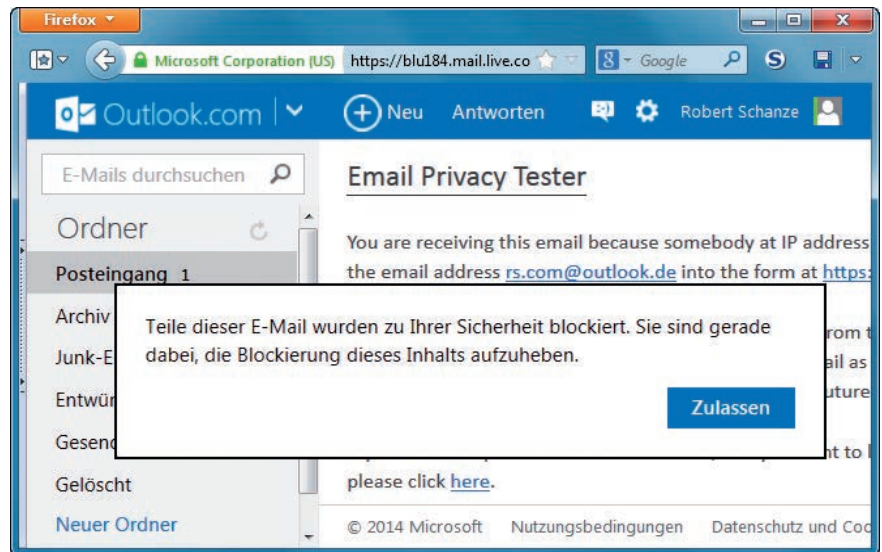
Einige Webmail-Dienste und viele E-Mail-Clients zeigen innerhalb einer E-Mail zudem an, ob die E-Mail möchte, dass Sie externe Inhalte nachladen lassen (Bild C). Spätestens wenn Sie das zulassen, nehmen einige Tracking-Elemente auf Email Privacy Tester die Farbe Rot an.

Hinweis: Wenn Sie die E-Mail von Email Privacy Tester nicht in Ihrem Posteingang finden sollten, hat Ihr Webmail-Dienst oder E-Mail-Client sie vermutlich als Spam aussortiert. Verschieben Sie die E-Mail dann für den Test aus Ihrem Spam-Ordner in Ihren Posteingang.

GMX, Google Mail, Yahoo und Co.

Bei dem Check der Webmailer Freenet, GMX, Google Mail, Outlook.de, T-Online, Web.de und Yahoo wurden die Standardeinstellungen verwendet.

Freenet und Yahoo lösten im Test keine Tracking-Elemente von Email Privacy Tester aus. GMX, Google Mail, T-Online und Web.de sendeten hingen



Schutz vor externen Inhalten: Einige Webmailer und viele E-Mail-Clients unterbinden das Nachladen externer Inhalte durch E-Mails, außer der Nutzer stimmt dem ausdrücklich zu (Bild C)

gen Tracking-Informationen an den E-Mail-Absender. Outlook.de – ehemals Hotmail – lud sogar zwei Tracking-Elemente im Voraus, noch bevor die E-Mail angeklickt wurde. Ein weiteres Element kam hinzu, nachdem die E-Mail geöffnet wurde. Die meisten Tracking-Elemente löste T-Online aus.

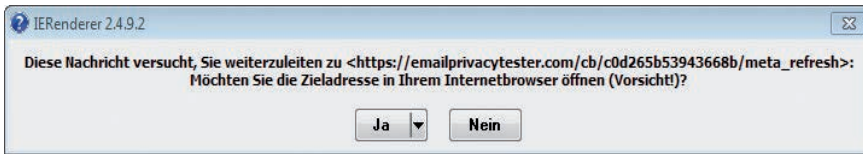
Freenet, Outlook.de und Yahoo boten an, den Abruf blockierter externer Inhalte zu erlauben, und zeigten dafür eine Schaltfläche innerhalb der E-Mail an. Nach einem Klick darauf lud Freenet nur zwei Tracking-Elemente nach. Bei Yahoo waren es drei, bei Outlook.de acht. Noch strikter waren die anderen

E-Mail-Clients: Ausgelöste Tracking-Elemente

Diese Tabelle zeigt in der ersten Zeile, dass lokal installierte E-Mail-Programme deutlich weniger Tracking-Elemente übermitteln als Webmailer. Wenn Sie aber das Nachladen externer Inhalte erlauben, führen sie sehr viele Tracking-Elemente aus.

	Outlook 2010	Pegasus Mail 4.70	The Bat 6.3.2	Thunderbird 24.4	Windows Live Mail 2012
E-Mail angeklickt	–	• Object tag – Flash	–	–	–
Externe Inhalte erlaubt	<ul style="list-style-type: none"> • Background attribute • CSS Import • CSS link tag • Image tag • Image Submit Button 	<ul style="list-style-type: none"> • Atom feed • Background attribute • BGSound tag • CSS Attachment • CSS background-image • CSS link tag • DNS Prefetch – Link • Image Submit Button • Image tag • Link Prefetch • OpenSearch • RSS feed • Script tag (javascript) 	<ul style="list-style-type: none"> • Background attribute • CSS background-image • Image Submit Button • Image tag 	<ul style="list-style-type: none"> • Audio tag • CSS Attachment • CSS background-image • CSS content • CSS import • CSS link tag • IFrame img • IFrame tag • Image tag • Image Submit Button • Object tag – data • Object tag – Flash • SVG inline with remote image • Video MP4 • Video Ogg • Video poster • Video tag • Video Webm 	<ul style="list-style-type: none"> • GSound tag • CSS Attachment • CSS background-image • CSS import • CSS link tag • Image tag • Image Submit Button • Object tag – Flash • Link Prefetch

Es wurden die Standardeinstellungen der E-Mail-Clients verwendet



Automatische Weiterleitung: Pegasus Mail 4.70 zeigt einen Weiterleitungsversuch der Tracking-E-Mail an. Ein Klick auf „Ja“ löst hier das Übermitteln von Tracking-Elementen aus (Bild D)

E-Mail-Dienste: Sie boten in den Standardeinstellungen das Nachladen externer Inhalte gar nicht erst an.

Die gewöhnliche Lesebestätigung zeigten die Webmail-Dienste außer GMX und Web.de ebenfalls nicht an. Sie ist offenbar durch Tracking-Elemente überflüssig geworden.

Outlook, Thunderbird und Co.

Neben den am weitesten verbreiteten Webmail-Diensten wurden auch mehrere E-Mail-Clients getestet: Outlook 2010, Pegasus Mail 4.70, The Bat 6.3.2, Thunderbird 24.4 und Windows Live Mail 2012. Auch diese Tests wurden mit den Standardeinstellungen der Programme durchgeführt.

Anders als die Webmail-Dienste laden nahezu alle E-Mail-Clients zunächst keine Tracking-Elemente. Das liegt daran, dass sie meist standardmäßig Skripts und Tags in E-Mails blockieren, die auf externe Inhalte verweisen.

Eine Ausnahme war Pegasus Mail 4.70. Dieser Mail-Client lud ein Tracking-Element beim Öffnen der E-Mail. Dazu zeigte Pegasus Mail eine Meldung an, die besagte, dass die E-Mail versucht, den Empfänger auf eine Webseite weiterzuleiten (Bild D).

Ein Klick auf „Ja“ leitet auf eine Unterseite von Email Privacy Tester weiter, die den Empfänger warnt, dass der E-Mail-Client Meta-Refresh-Tags akzeptiert. Diese Tags können dazu verwendet werden, Anwender auf eine andere, möglicherweise manipulierte und infizierte Webseite weiterzuleiten.

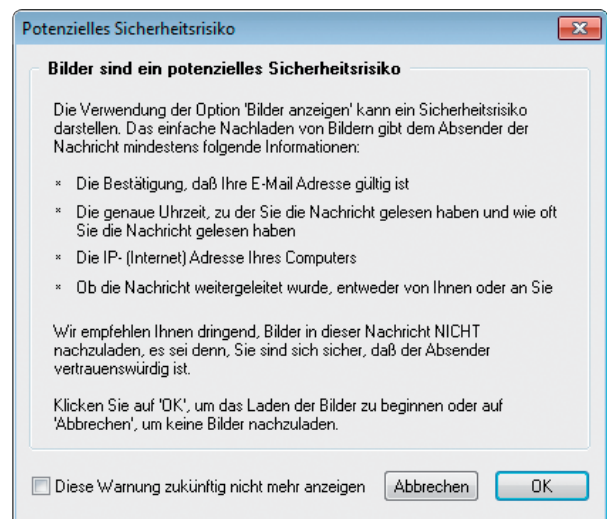
Blockierte externe Inhalte lassen sich mit allen E-Mail-Clients nachladen. Die meisten externen Inhalte lädt Thunderbird 24.4 nach. Das liegt daran, dass das Open-Source-Programm viele Web- und Mail-Techniken unterstützt, und ist nicht direkt ein Sicherheitsproblem. Immerhin muss das Nachladen ja vom Anwender selbst ausgelöst werden.

Pegasus Mail zeigt als einziges Programm einen ausführlichen Hinweis an, der den Empfänger über die Gefahren des Nachladens informiert (Bild E).

Als wir versuchten, die Dateien des Anhangs der Test-E-Mail zu öffnen, hat das Microsoft-Programm Outlook 2010 die PNG-Datei gar nicht angezeigt.

The Bat 6.3.2 meldete als einziger E-Mail-Client, dass die PNG-Datei eine doppelte Dateieindung hat und deshalb vor dem Öffnen überprüft werden sollte (Bild F).

Dieser E-Mail-Client war auch der einzige, bei dem es nicht möglich war, eine offizielle Lesebestätigung zu versenden.



Warnhinweis: Pegasus Mail 4.70 informiert ausführlich darüber, welche Folgen das Nachladen externer Inhalte haben kann (Bild E)

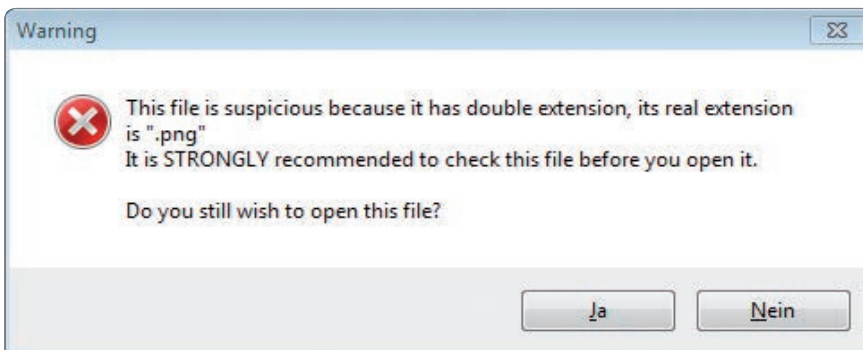
Fazit

Wer E-Mail-Tracking umgehen und seine Privatsphäre schützen will, nutzt am besten E-Mail-Clients wie Thunderbird oder Outlook und lässt E-Mails nicht im HTML-Format darstellen. Bereits in den Standardeinstellungen sind sie weitgehend sicher konfiguriert. Bei Webmailern sollten Sie das automatische Nachladen externer Inhalte deaktivieren, um E-Mail-Tracking einzuschränken. ■

Robert Schanze
internet@com-magazin.de

Weitere Infos

■ www.mailhilfe.de
Informationen zu E-Mail-Programmen



Doppelte Dateieindung: Der E-Mail-Client The Bat 6.3.2 warnte als einziger, dass die PNG-Datei im Anhang der Test-E-Mail eine doppelte Dateieindung hat, was oft ein Hinweis auf Viren ist (Bild F)