



digitaleseniorInnen
Servicestelle für Bildungseinrichtungen

Internetkriminalität

Schritt für Schritt Anleitungen



Workshop

Informationen, Tipps und Übungen für den Unterricht

Schutz vor Internetkriminalität

Schritt für Schritt Anleitungen

- Betrügerische Werbung melden
- Phishing-Schutz einschalten
- Dateien auf Viren überprüfen



Quelle: pixabay.com

Betrügerische Werbung melden

Facebook – Google - Instagram



Google



Betrügerische Werbung melden

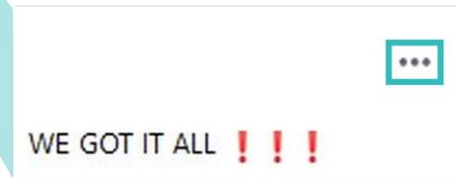
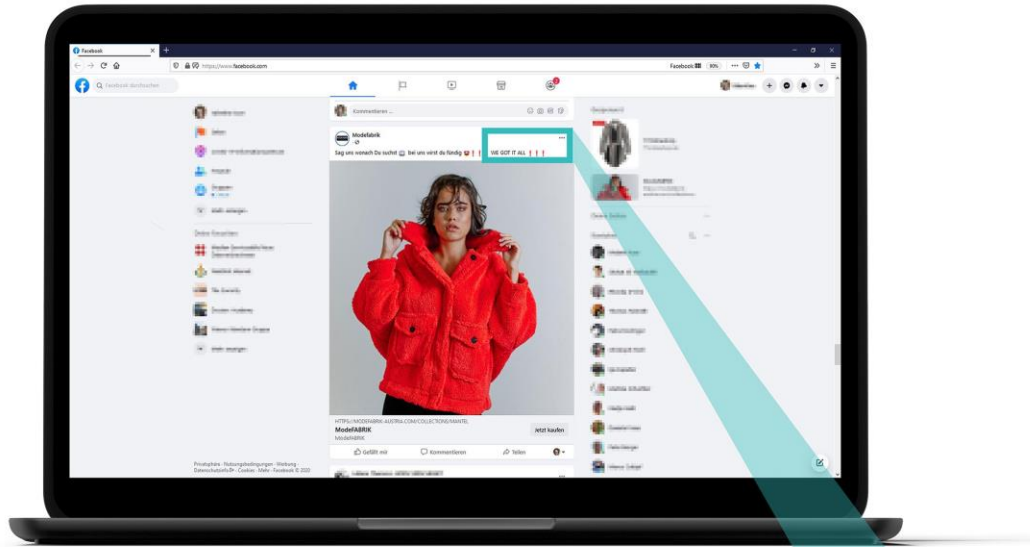
Facebook



Google



Betrügerische Werbung melden (Facebook)



Schritt 1:

Klicken Sie auf die drei Punkte.



Betrügerische Werbung melden (Facebook)



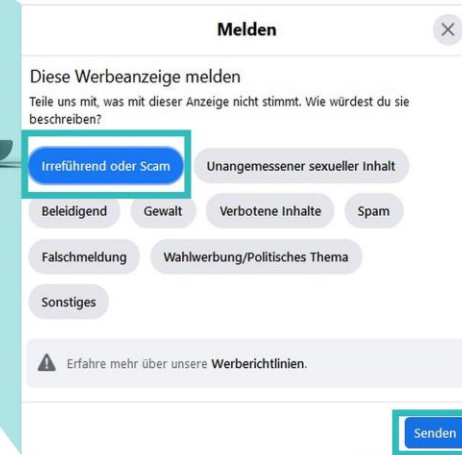
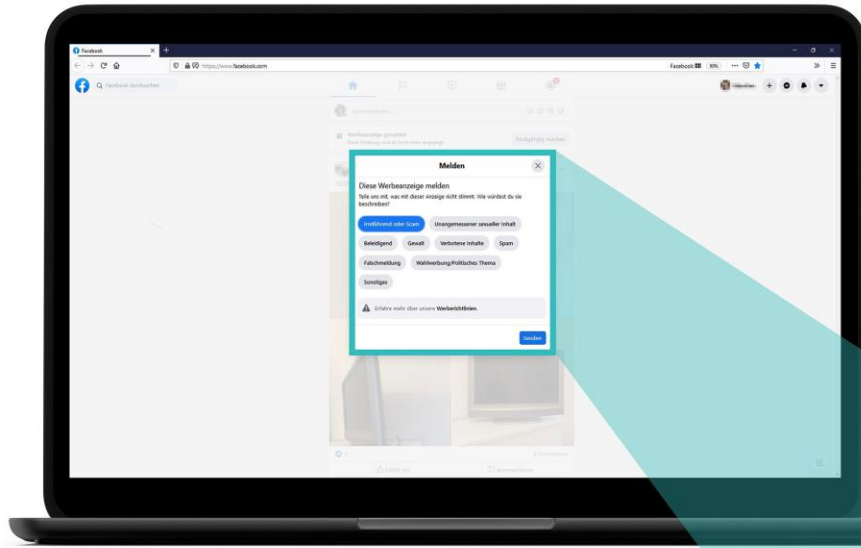
- Werbeanzeige verbergen
Diese Werbeanzeige wird nicht mehr angezeigt
- Werbeanzeige melden**
Teile uns ein Problem mit dieser Anzeige mit
- Link speichern
Zu deinen gespeicherten Objekten hinzufügen
- Benachrichtigungen zu diesem Beitrag aktivieren
- Warum sehe ich diese Werbeanzeige?
- Einbetten

Schritt 2:

Klicken Sie auf „Werbeanzeige melden“.



Betrügerische Werbung melden (Facebook)

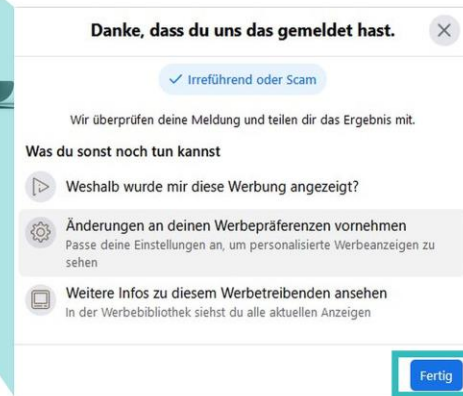
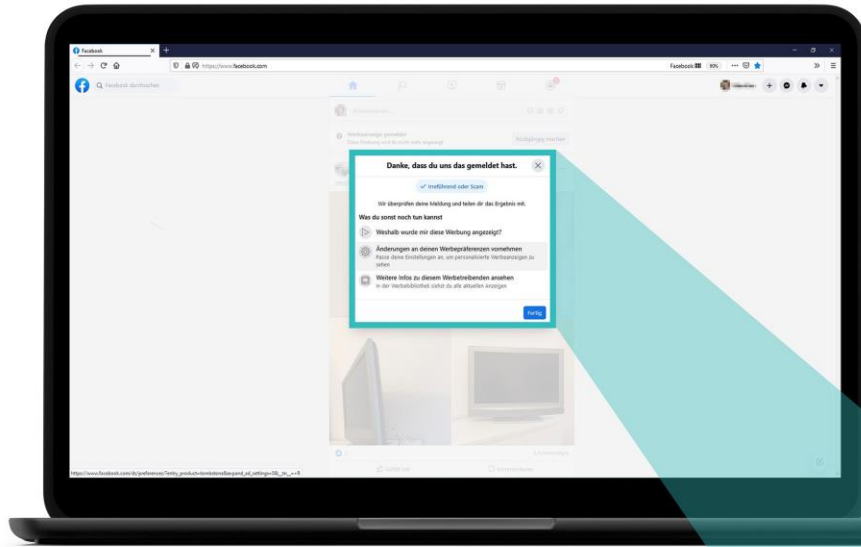


Schritt 3:

Klicken Sie auf „Irreführend oder Scam“
und anschließend auf „Senden“.



Betrügerische Werbung melden (Facebook)



Schritt 4:

Klicken Sie auf „Fertig“,
um den Vorgang abzuschließen.



Betrügerische Werbung melden

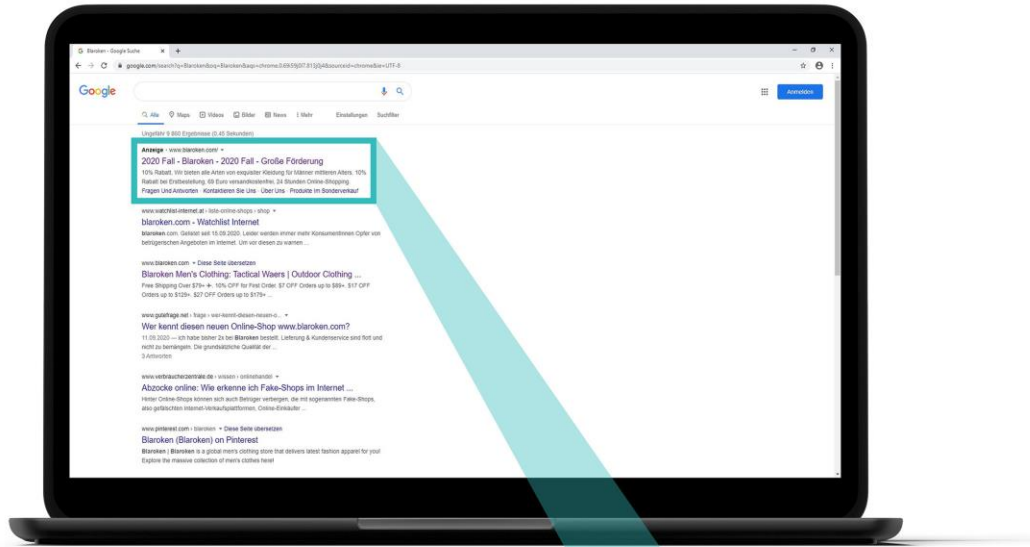
Google



Google



Betrügerische Werbung melden (Google)



Schritt 1:

Klicken Sie auf den Pfeil.

Anzeige · www.blaroken.com

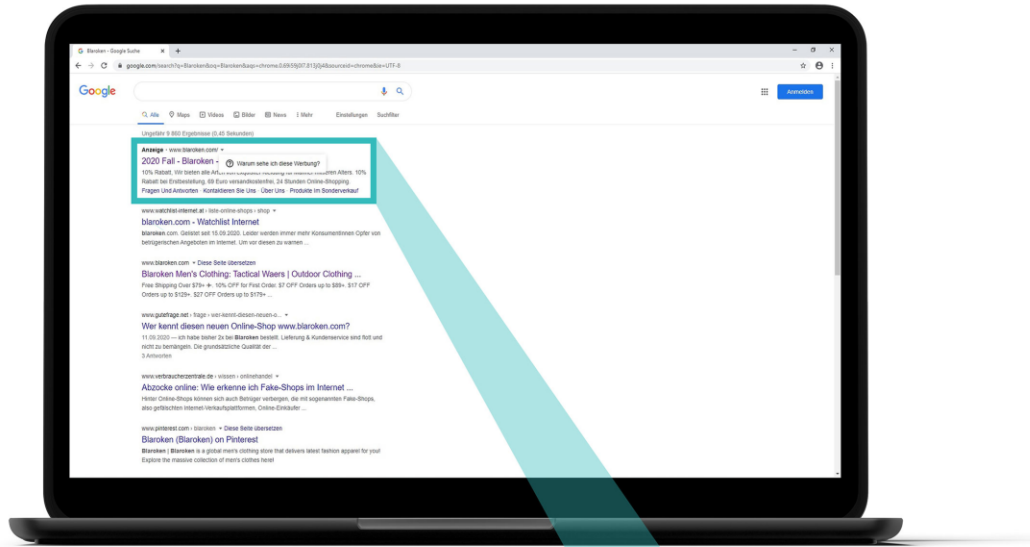
2020 Fall - Blaroken - 2020 Fall - Große Förderung

10% Rabatt, Wir bieten alle Arten von exquisiter Kleidung für Männer mittleren Alters. 10% Rabatt bei Erstbestellung, 69 Euro versandkostenfrei, 24 Stunden Online-Shopping.

Fragen Und Antworten · Kontaktieren Sie Uns · Über Uns · Produkte Im Sonderverkauf



Betrügerische Werbung melden (Google)



Anzeige · www.blaroken.com/ ▾

2020 Fall - Blaroken - Warum sehe ich diese Werbung?

10% Rabatt, Wir bieten alle Arten von exquisiter Kleidung für männer mittleren Alters. 10% Rabatt bei Erstbestellung, 69 Euro versandkostenfrei, 24 Stunden Online-Shopping.

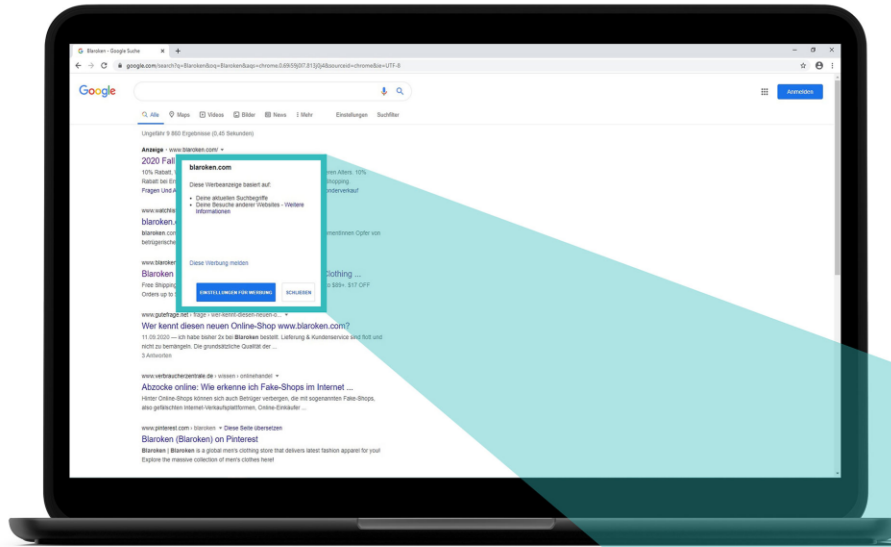
Fragen Und Antworten · Kontaktieren Sie Uns · Über Uns · Produkte Im Sonderverkauf

Schritt 2:

Klicken Sie auf „Warum sehe ich diese Werbung?“.



Betrügerische Werbung melden (Google)



blaroken.com

Diese Werbeanzeige basiert auf:

- Deine aktuellen Suchbegriffe
- Deine Besuche anderer Websites - Weitere Informationen

Diese Werbung melden

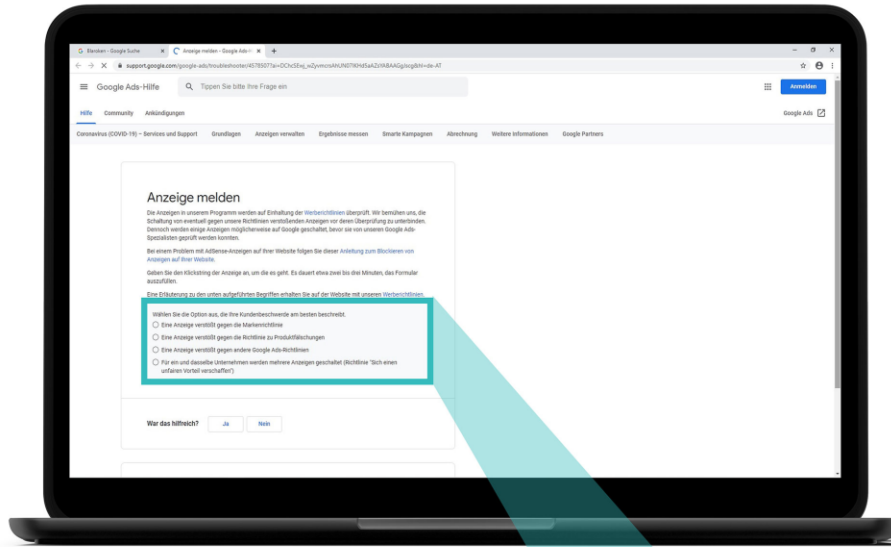
EINSTELLUNGEN FÜR WERBUNG

SCHLIEßEN

Schritt 3:

Klicken Sie auf „Diese Werbung melden“.





Schritt 4:

Klicken Sie auf „Eine Anzeige verstößt gegen die Richtlinie zu Produktfälschungen“.

Wählen Sie die Option aus, die Ihre Kundenbeschwerde am besten beschreibt.

- Eine Anzeige verstößt gegen die Markenrichtlinie
- Eine Anzeige verstößt gegen die Richtlinie zu Produktfälschungen
- Eine Anzeige verstößt gegen andere Google Ads-Richtlinien
- Für ein und dasselbe Unternehmen werden mehrere Anzeigen geschaltet (Richtlinie "Sich einen unfairen Vorteil verschaffen")

Betrügerische Werbung melden

Instagram



Google





Betrügerische Werbung melden (Instagram)

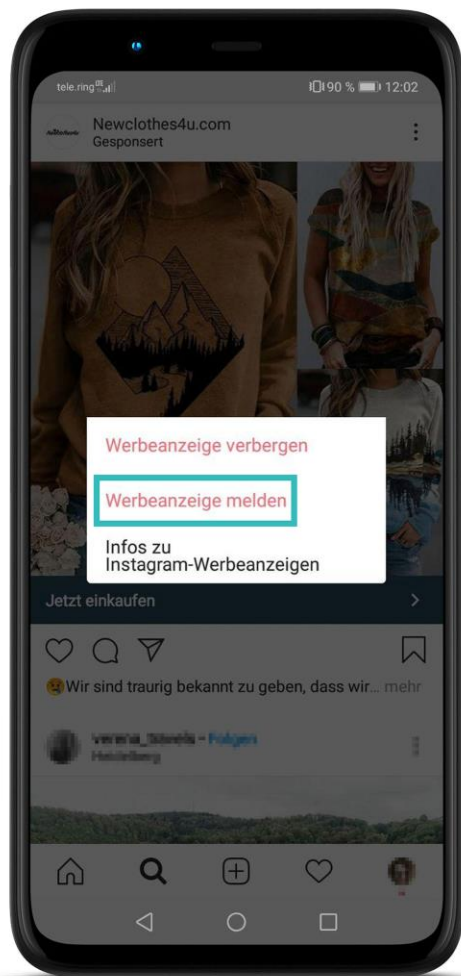


Schritt 1:

Klicken Sie auf die drei Punkte.



Betrügerische Werbung melden (Instagram)

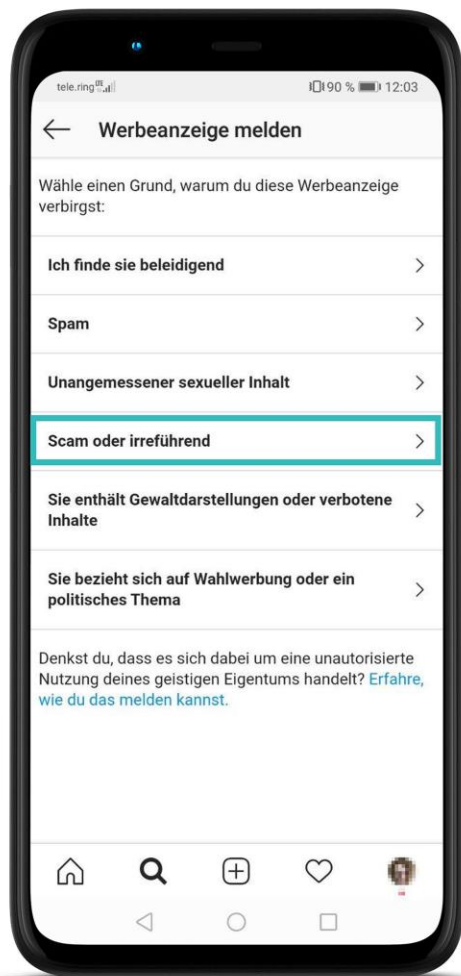


Schritt 2:

Klicken Sie auf
„Werbeanzeige melden“.



Betrügerische Werbung melden (Instagram)



Schritt 3:

Klicken Sie auf
„Scam oder irreführend“. Scam
bedeutet auf Deutsch „Betrug“.



Phishing-Schutz einschalten

Chrome - Firefox

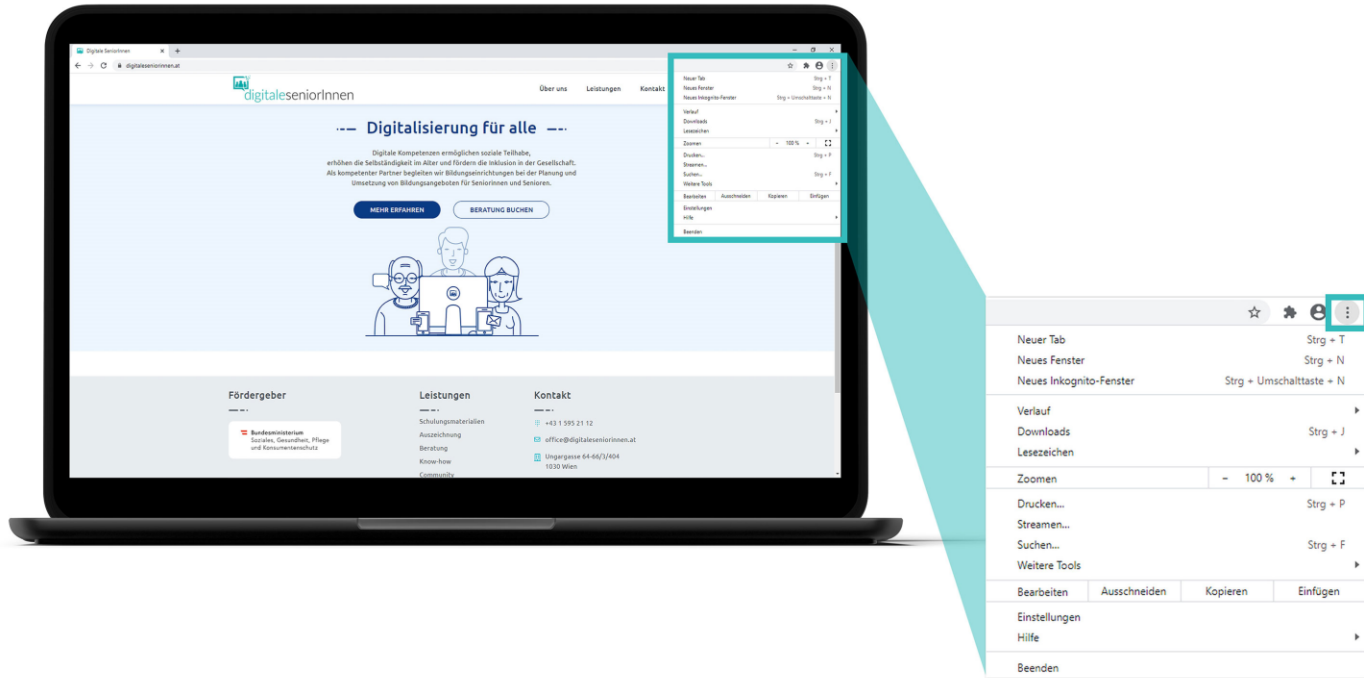


Phishing-Schutz einschalten

Chrome



Schutz vor Phishing-Webseiten einschalten (Chrome)



Schritt 1:

Öffnen Sie Chrome und klicken Sie rechts oben auf die drei Punkte.



Schutz vor Phishing-Webseiten einschalten (Chrome)



The image shows a laptop screen displaying the website 'digitalesenioren.at'. The website content includes the title 'Digitalisierung für alle' and a call to action 'BERATUNG BUCHEN'. A Chrome menu is overlaid on the right side of the screen, with the 'Einstellungen' (Settings) option highlighted in a red box. The menu items are as follows:

Neuer Tab	Strg + T		
Neues Fenster	Strg + N		
Neues Inkognito-Fenster	Strg + Umschalttaste + N		
Verlauf	→		
Downloads	Strg + J		
Lesezeichen	→		
Zoomen	- 100% +		
Drucken...	Strg + P		
Streamen...	→		
Suchen...	Strg + F		
Weitere Tools	→		
Bearbeiten	Ausschneiden	Kopieren	Einfügen
Einstellungen			
Hilfe			→
Beenden			

Schritt 2:

Klicken Sie auf „Einstellungen“.



Schutz vor Phishing-Webseiten einschalten (Chrome)



The image shows a laptop displaying the Chrome settings page. A callout menu is open, highlighting the 'Datenschutz und Sicherheit' (Privacy and Security) option. The menu items are:

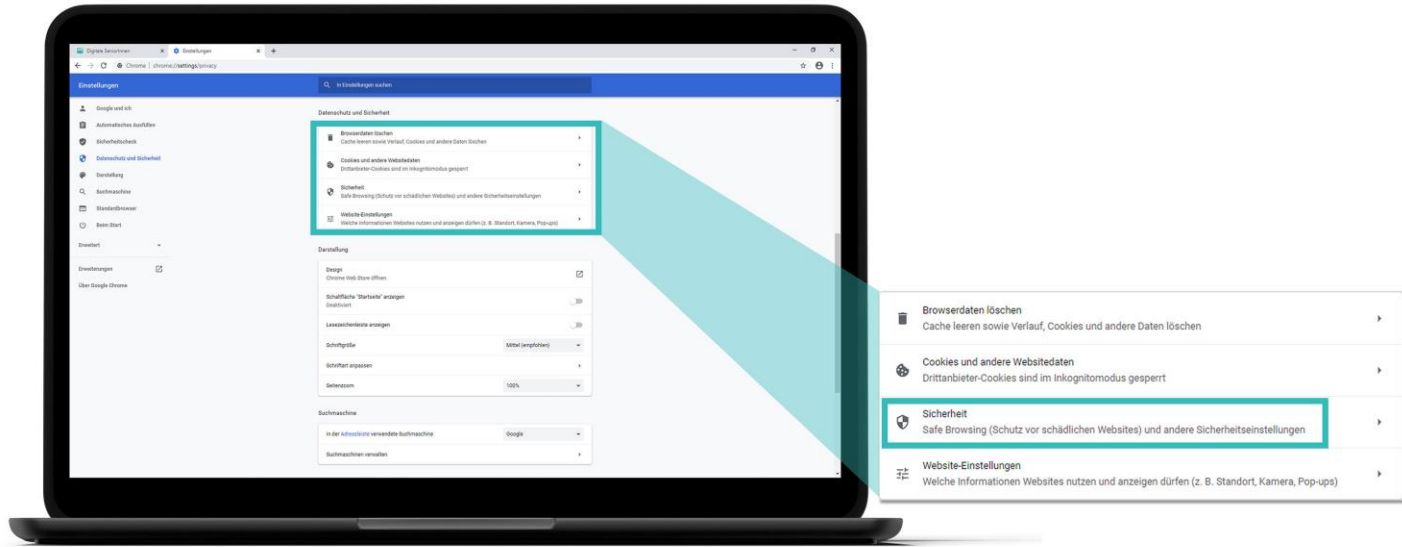
- Google und ich
- Automatisches Ausfüllen
- Sicherheitscheck
- Datenschutz und Sicherheit**
- Darstellung
- Suchmaschine
- Standardbrowser
- Beim Start
- Erweitert
- Erweiterungen
- Über Google Chrome

Schritt 3:

Es öffnet sich eine neue Seite. Klicken Sie dort auf „Datenschutz & Sicherheit“.



Schutz vor Phishing-Webseiten einschalten (Chrome)

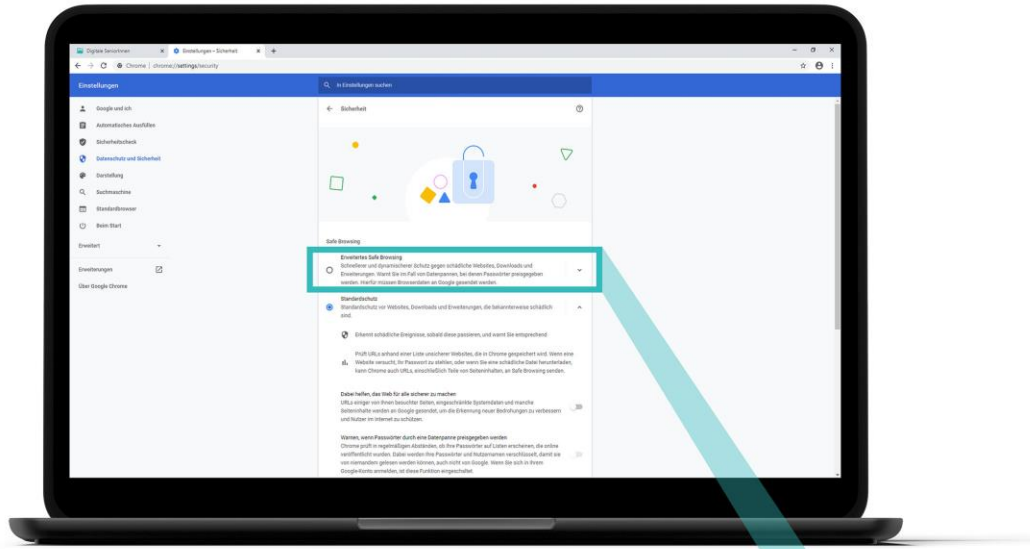


Schritt 4:

Klicken Sie auf „Sicherheit“.



Schutz vor Phishing-Webseiten einschalten (Chrome)



Erweitertes Safe Browsing

Schnellerer und dynamischer Schutz gegen schädliche Websites, Downloads und Erweiterungen. Warnt Sie im Fall von Datenpannen, bei denen Passwörter preisgegeben werden. Hierfür müssen Browserdaten an Google gesendet werden.

Schritt 5:

Klicken Sie auf „Erweitertes Safe Browsing“.

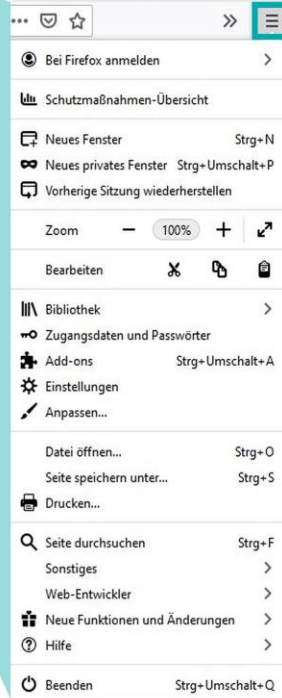
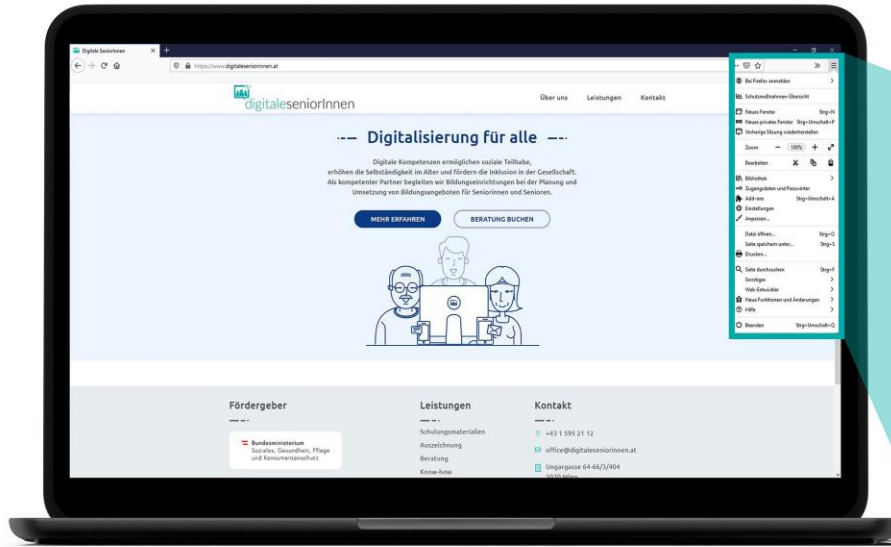


Phishing-Schutz einschalten

Firefox



Schutz vor Phishing-Webseiten einschalten (Firefox)

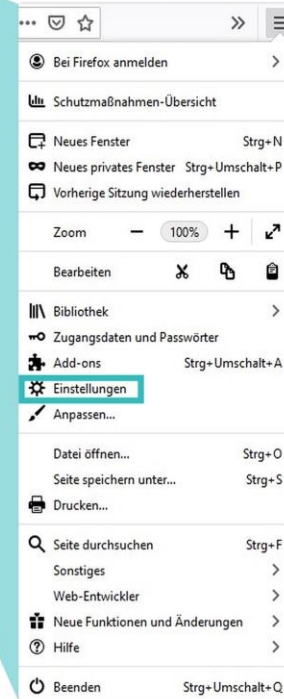
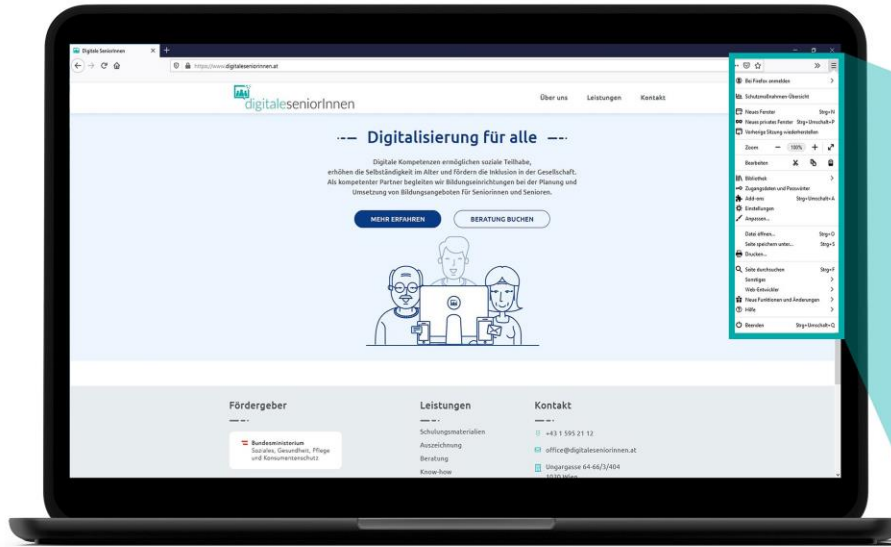


Schritt 1:

Öffnen Sie Firefox und klicken Sie rechts oben auf die drei Striche.



Schutz vor Phishing-Webseiten einschalten (Firefox)



Schritt 2:

Klicken Sie auf „Einstellungen“.



Schutz vor Phishing-Webseiten einschalten (Firefox)

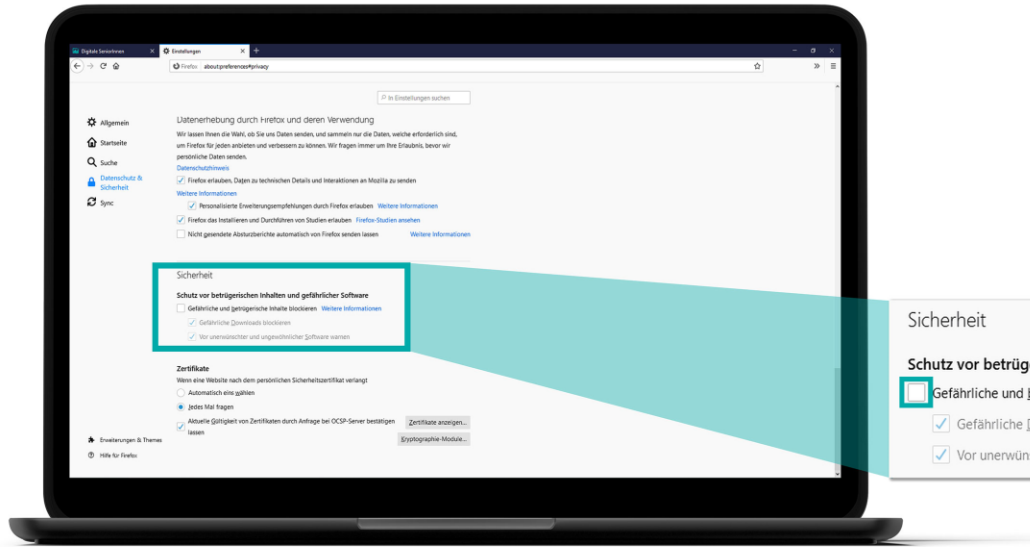
A laptop screen displays the Firefox Settings page. The 'Allgemein' (General) section is highlighted with a teal box. A callout menu on the right side of the screen lists the settings categories: 'Allgemein', 'Startseite', 'Suche', 'Datenschutz & Sicherheit', and 'Sync'. The 'Datenschutz & Sicherheit' option is highlighted with a teal border. The laptop screen shows the 'Einstellungen' (Settings) page with the 'Allgemein' section selected. The 'Start' section includes options for 'Vorherige Sitzung wiederherstellen' and 'Immer überprüfen, ob Firefox der Standardbrowser ist'. The 'Tabs' section has options for 'Rechtliches Tab die Tab nach letzter Nutzung in absteigender Reihenfolge anzeigen', 'Links in Tabs neuzeit in neuen Fenstern öffnen', 'Tabs im Vordergrund öffnen', and 'Tab-Vorschau in der Windows-Taskleiste anzeigen'. The 'Erweiterung' section shows 'Die Erweiterung Facebook Container verwaltet die Tab-Umgebungen' and 'Tab-Umgebungen aktivieren'. The 'Sprache und Erscheinungsbild' section shows 'Standard-Schriftart' and 'Größe'.

Schritt 3:

Es öffnet sich eine neue Seite. Klicken Sie dort auf „Datenschutz & Sicherheit“.



Schutz vor Phishing-Webseiten einschalten (Firefox)



Sicherheit

Schutz vor betrügerischen Inhalten und gefährlicher Software

- Gefährliche und betrügerische Inhalte blockieren [Weitere Informationen](#)
- Gefährliche Downloads blockieren
- Vor unerwünschter und ungewöhnlicher Software warnen

Schritt 4:

Klicken Sie unter dem Punkt „Sicherheit“ auf „Gefährliche und betrügerische Inhalte blockieren“.

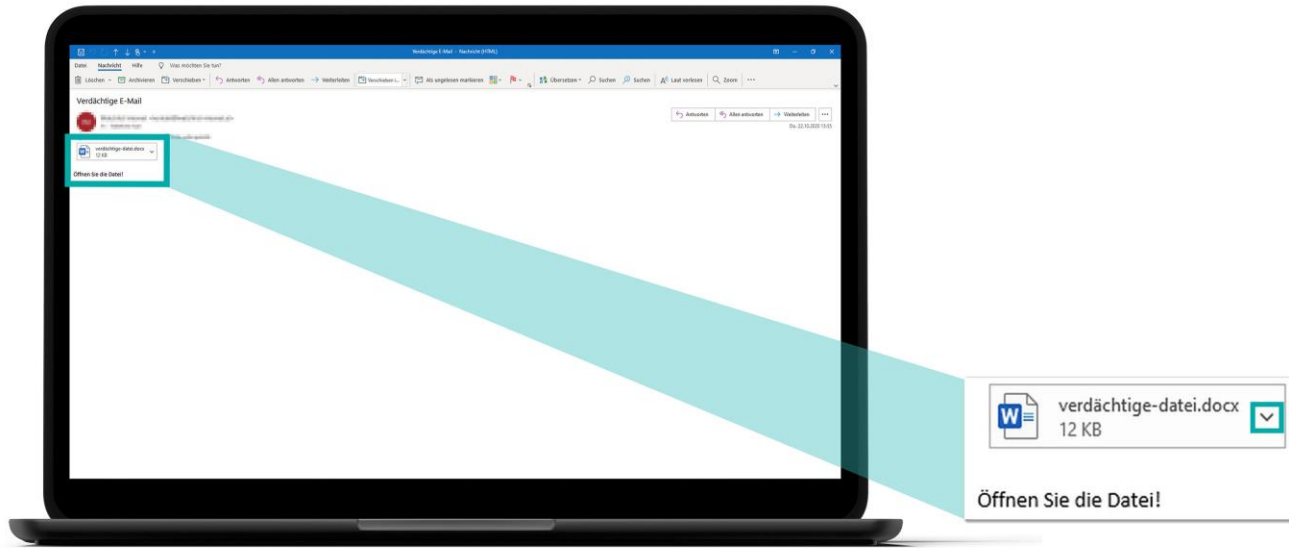


Dateien auf Viren überprüfen

Virustotal - <https://www.virustotal.com>



Überprüfung verdächtiger E-Mail-Anhänge

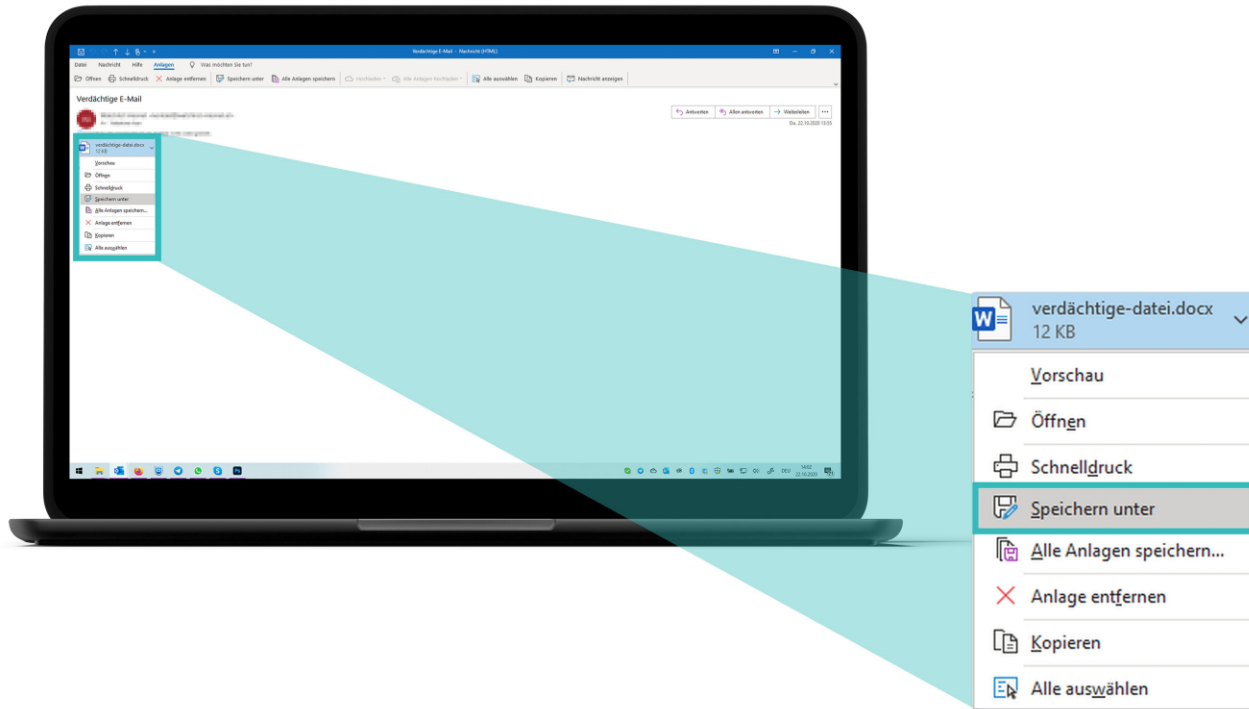


Schritt 1:

Klicken Sie neben der verdächtigen Datei auf den Pfeil oder klicken Sie mit rechts direkt auf die Datei. **WICHTIG:** Klicken Sie nicht doppelt auf die Datei!



Überprüfung verdächtiger E-Mail-Anhänge

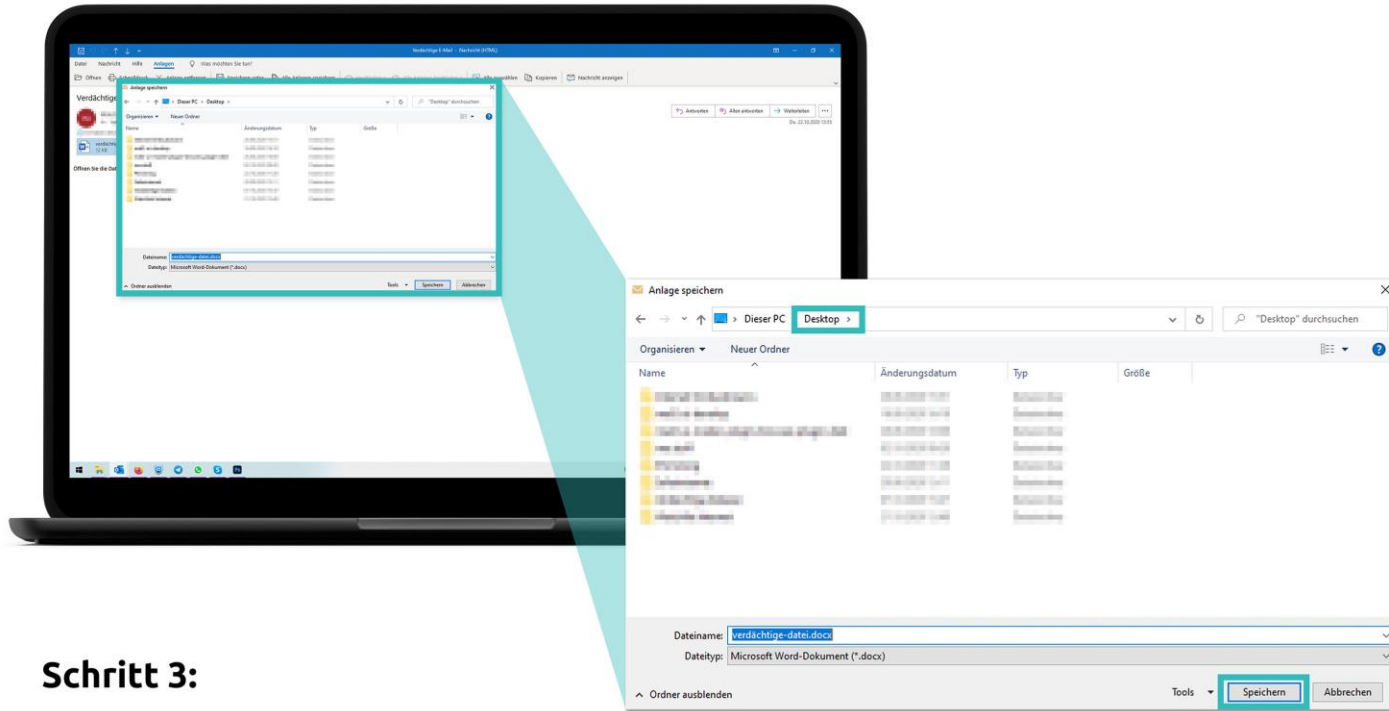


Schritt 2:

Klicken Sie auf „Speichern unter“.



Überprüfung verdächtiger E-Mail-Anhänge

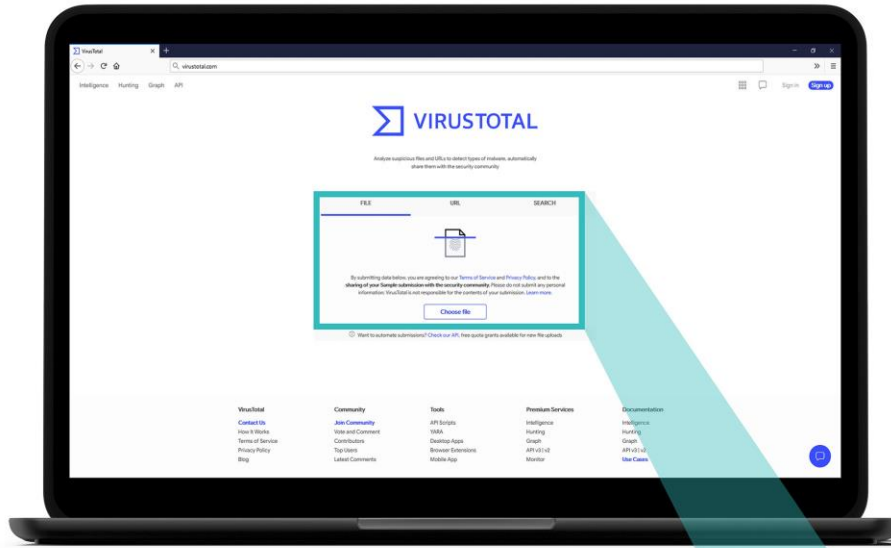


Schritt 3:

Wählen Sie einen Ort, an dem Sie die Datei leicht wiederfinden (zum Beispiel „Desktop“). Klicken Sie auf „Speichern“.

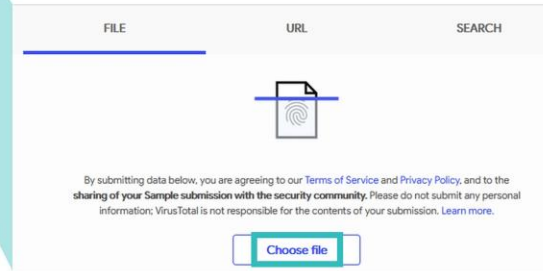


Überprüfung verdächtiger E-Mail-Anhänge

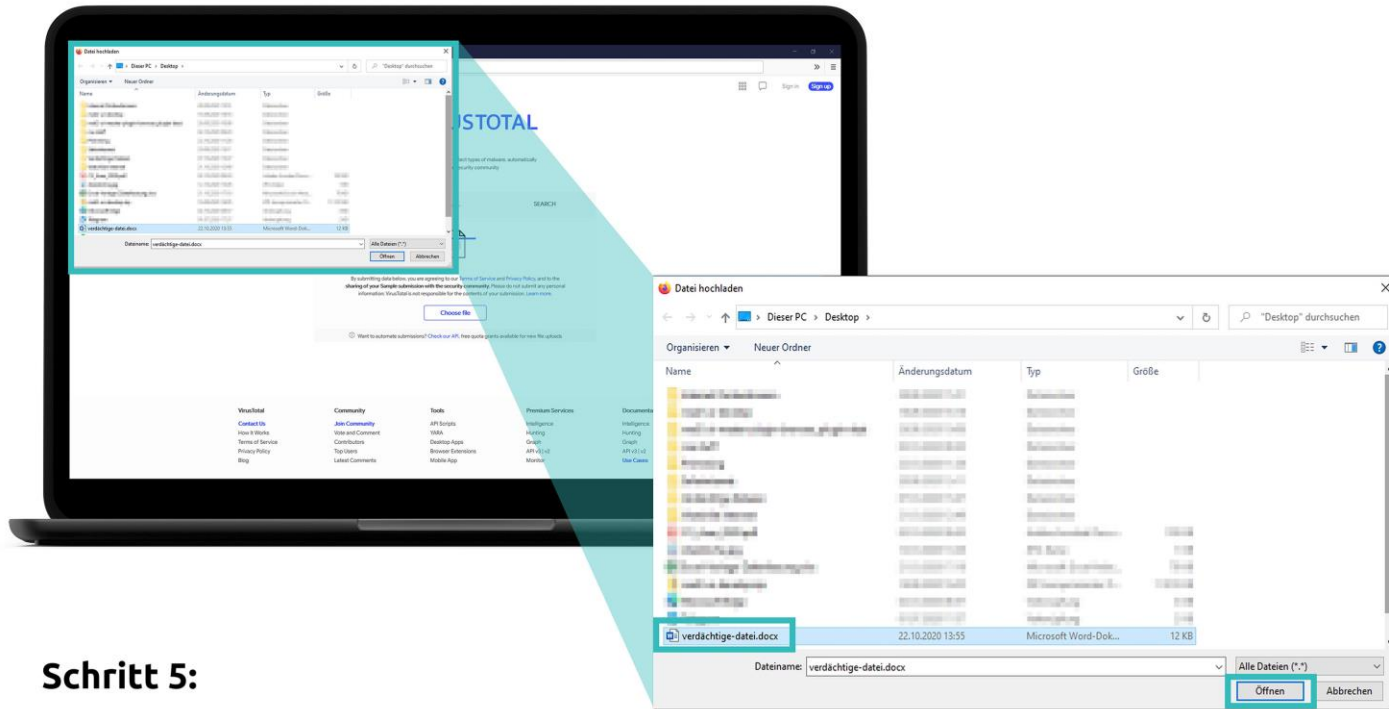


Schritt 4:

Öffnen Sie in Ihrem Browser die Webseite „virustotal.com“. Klicken Sie auf „Choose File“ („Datei wählen“).



Überprüfung verdächtiger E-Mail-Anhänge



Schritt 5:

Es öffnet sich ein neues Fenster.
Klicken Sie auf die verdächtige Datei. Klicken Sie auf „Öffnen“.



Überprüfung verdächtiger E-Mail-Anhänge



0 / 63

✓ No engines detected this file

90a928f92a574b18a2f6f5280c5ec5

DETECTION	DETAILS	RELATIONS	COMMENTARY
Ad-Aware	undetected	AviraLab	undetected
Anti-Lee-VE	undetected	BitDefender	undetected
AVe	undetected	Avast	undetected
Avast	undetected	Avast	undetected
Avast-Mobile	undetected	Avast	undetected
Avira-Cloud	undetected	Avira	undetected
BitDefender	undetected	BitDefenderThreat	undetected
BitDefender	undetected	BitDefenderThreat	undetected
Blau	undetected	BitDefenderThreat	undetected
ClamAV	undetected	ClamAV	undetected
Comodo	undetected	Comodo	undetected
Cyren	undetected	Cyren	undetected
Emsisoft	undetected	Emsisoft	undetected
ESET-NOD32	undetected	ESET-NOD32	undetected
F-Secure	undetected	F-Secure	undetected
FreeEye	undetected	FreeEye	undetected

Erhalten Sie ein grünes Ergebnis, wurde die Datei nicht als gefährlich erkannt. Seien Sie trotzdem vorsichtig! Das Ergebnis gibt Ihnen nur eine erste Einschätzung.



Überprüfung verdächtiger E-Mail-Anhänge



The screenshot shows the VirusShare interface for a file analysis. A callout box highlights a red alert: "2 engines detected this file". The interface includes a table with the following columns: DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COGNATE. The table lists various engines and their detection results for the file.

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COGNATE
MailScan	Signatures/MS/Phishing	Network/Dns/Hosts	Network/Dns/Hosts	Phishing
Ad-Aware	undetected	undetected	undetected	undetected
AhnLab-V3	undetected	undetected	undetected	undetected
Antiy-AVL	undetected	undetected	undetected	undetected
Avast	undetected	undetected	undetected	undetected
Avira (cloud)	undetected	undetected	undetected	undetected
Baidu	undetected	undetected	undetected	undetected
BitDefender	undetected	undetected	undetected	undetected
Blav	undetected	undetected	undetected	undetected
ClamAV	undetected	undetected	undetected	undetected
Comodo	undetected	undetected	undetected	undetected
Cyren	undetected	undetected	undetected	undetected
DnWeb	undetected	undetected	undetected	undetected
eScan	undetected	undetected	undetected	undetected
F-Secure	undetected	undetected	undetected	undetected

Callout box content: 2 engines detected this file. 01ce1724f620e47dbb0ceb0921f8c

Erhalten Sie ein rotes Ergebnis, wurde die Datei als gefährlich erkannt. Löschen Sie die E-Mail und die Datei.





DANKE FÜR IHRE
AUFMERKSAMKEIT!

