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

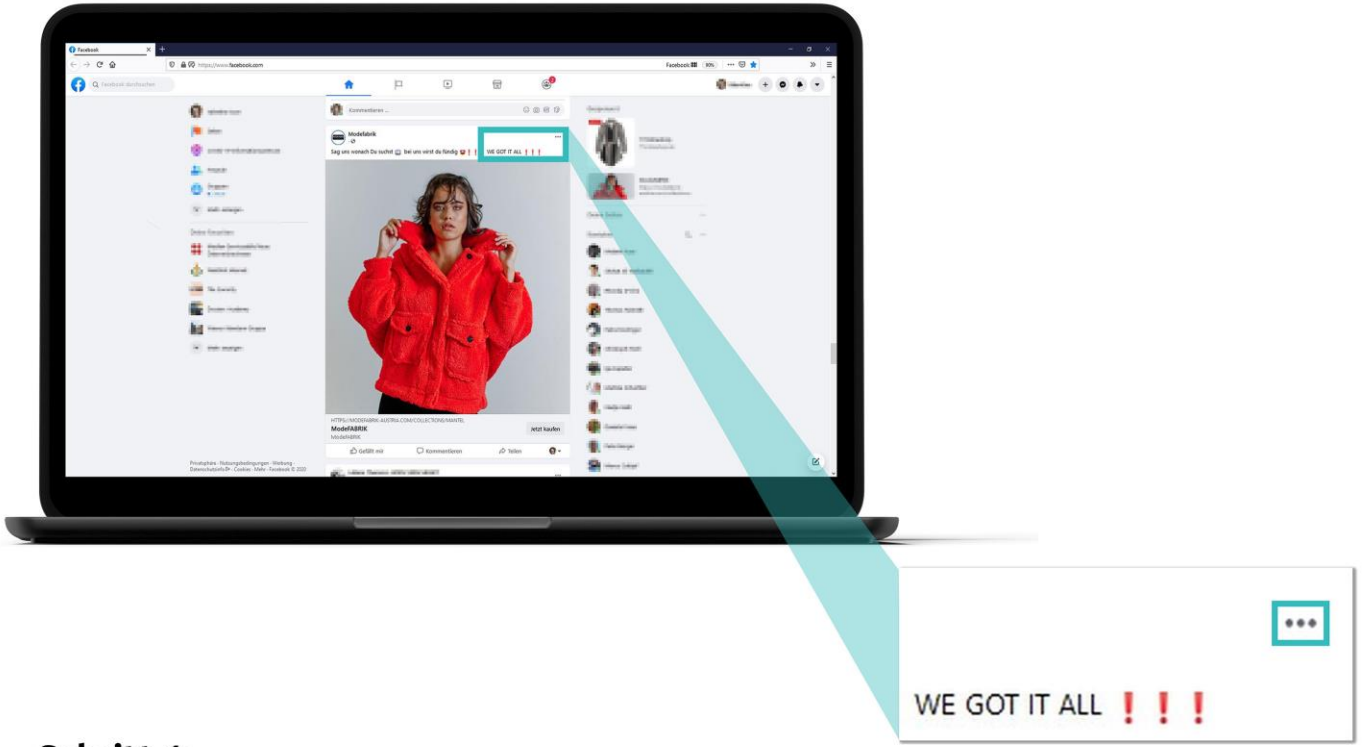
Quelle: pixabay.com

Betrügerische Werbung melden

Facebook

Quelle: pixabay.com

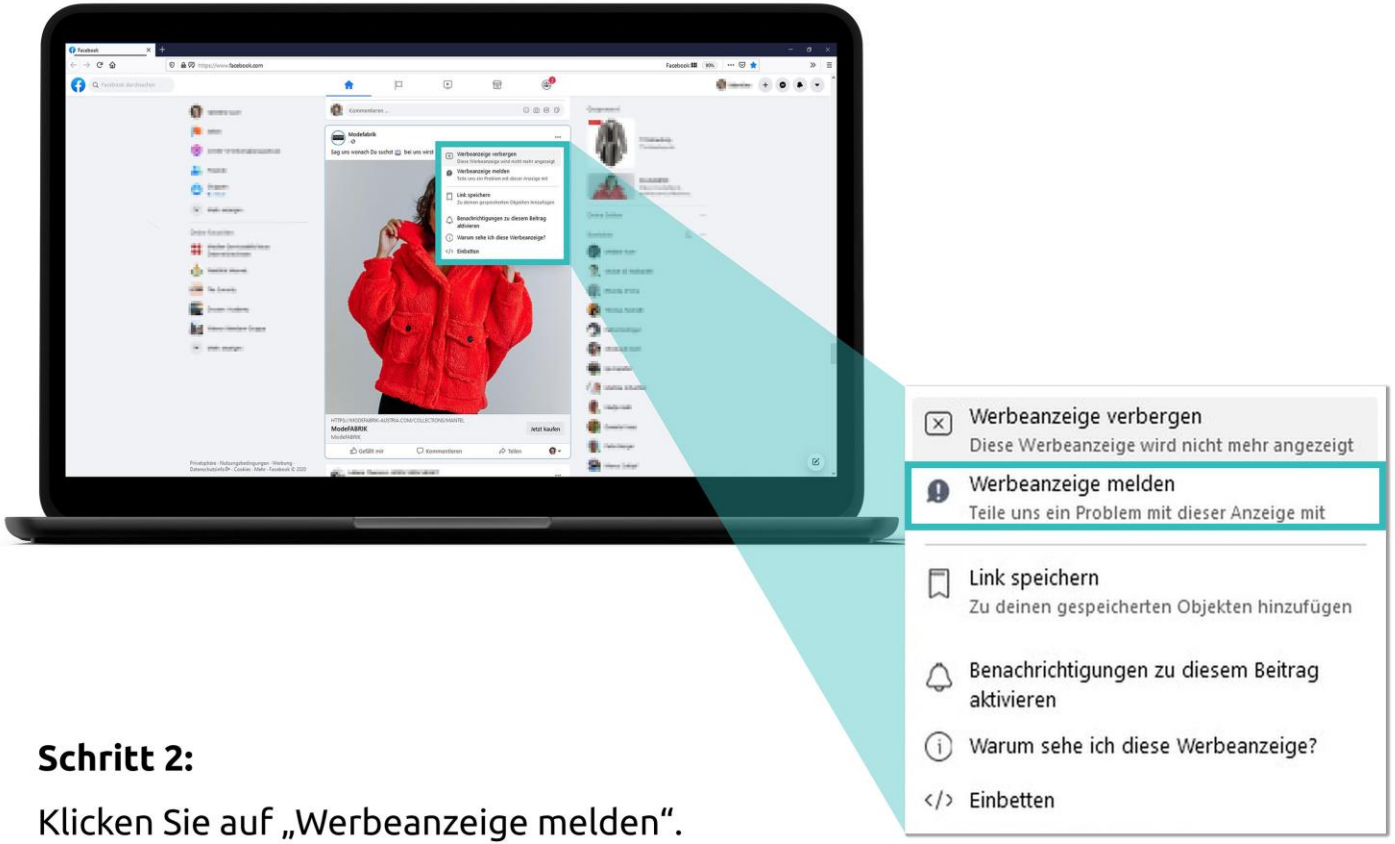
Betrügerische Werbung melden (Facebook)



Schritt 1:

Klicken Sie auf die drei Punkte.

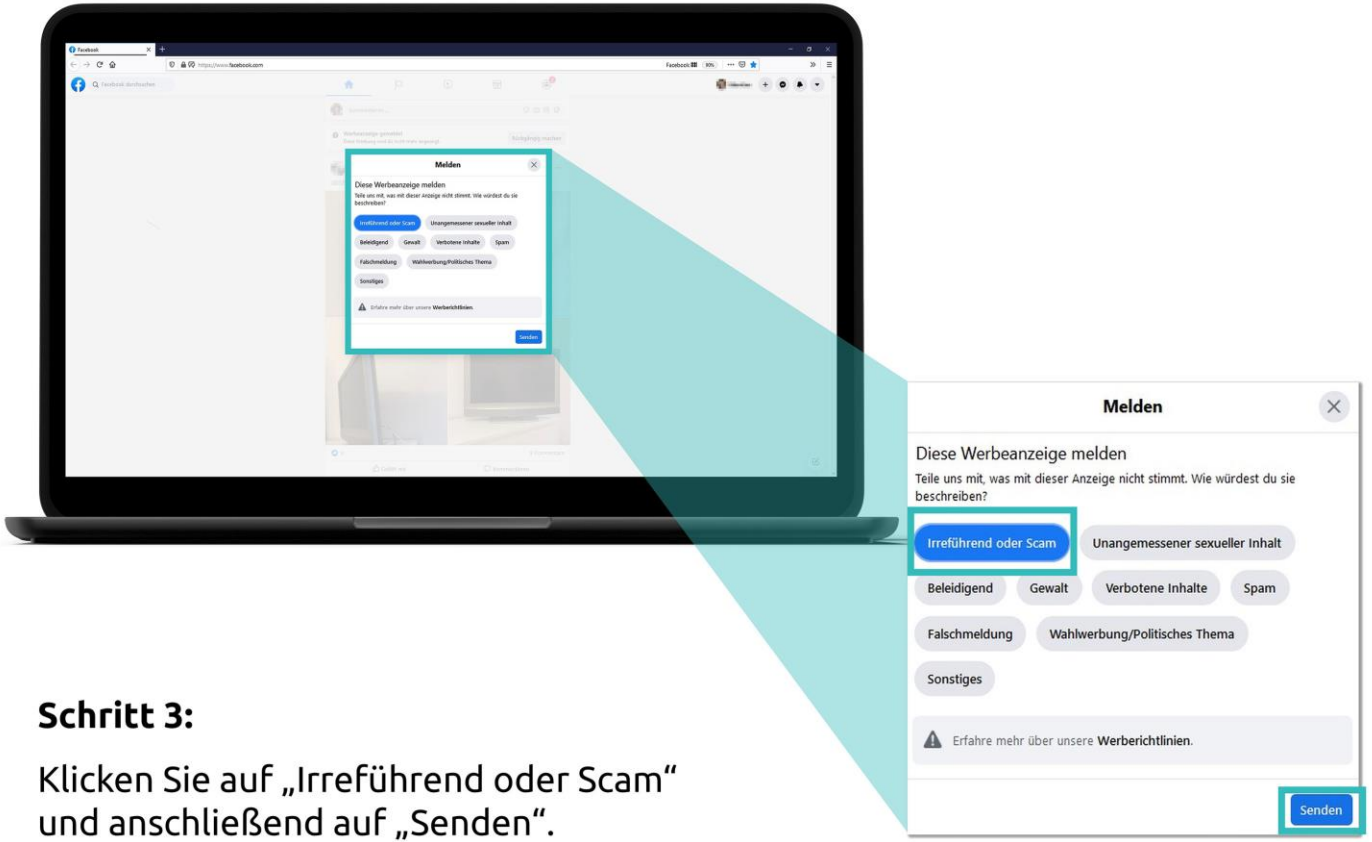
Betrügerische Werbung melden (Facebook)



Schritt 2:

Klicken Sie auf „Werbeanzeige melden“.

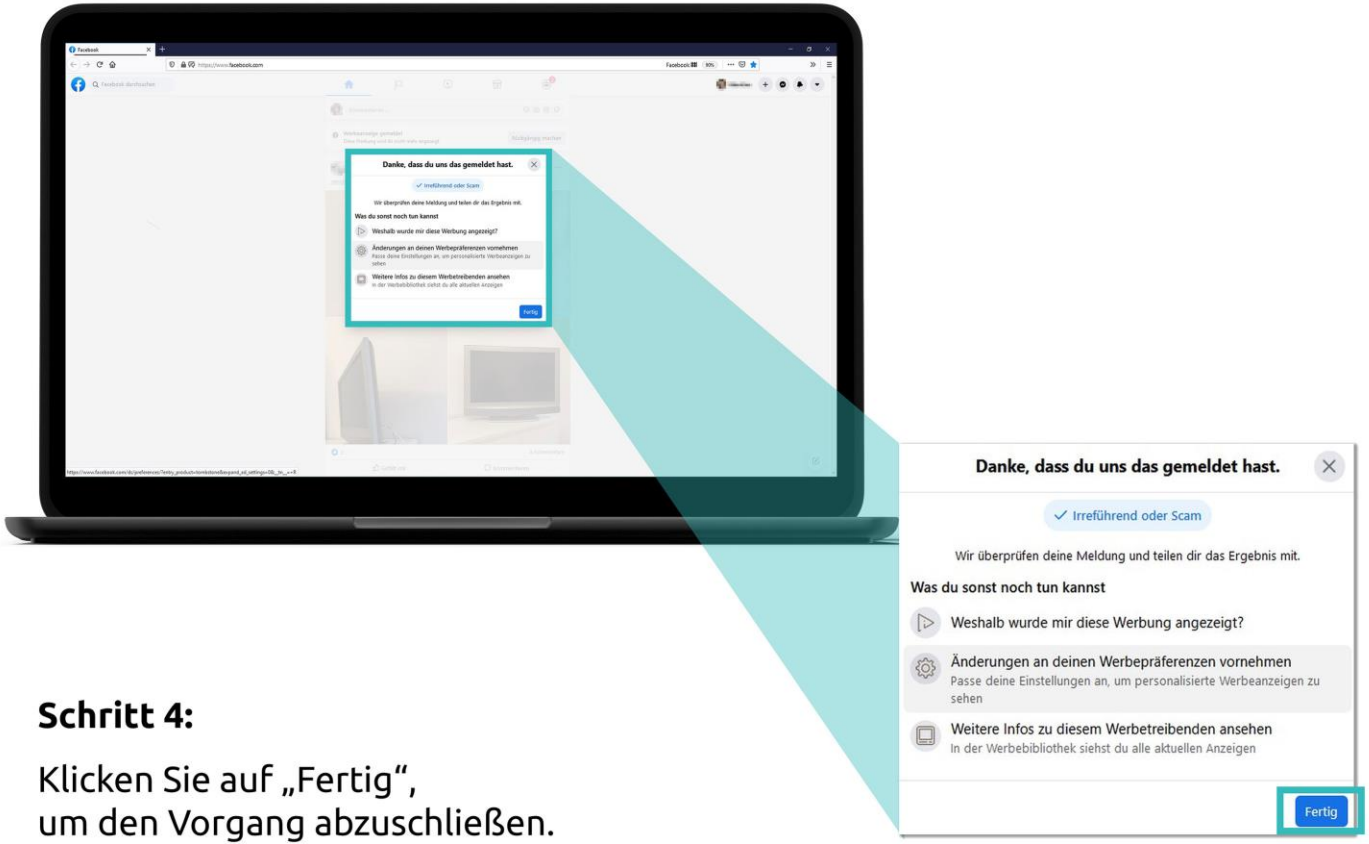
Betrügerische Werbung melden (Facebook)



Schritt 3:

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

Betrügerische Werbung melden (Facebook)



Schritt 4:

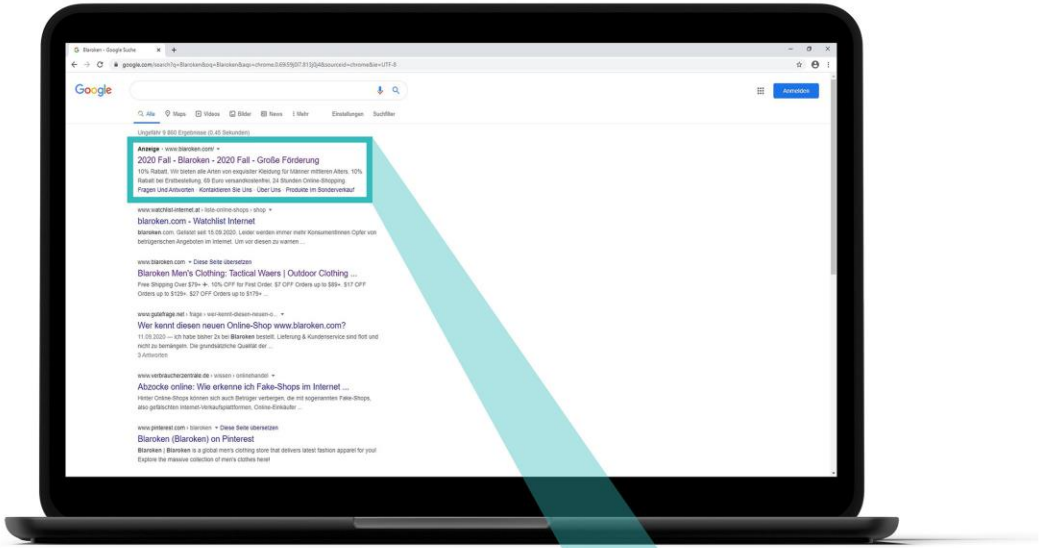
Klicken Sie auf „Fertig“,
um den Vorgang abzuschließen.

Betrügerische Werbung melden

Google

Quelle: pixabay.com

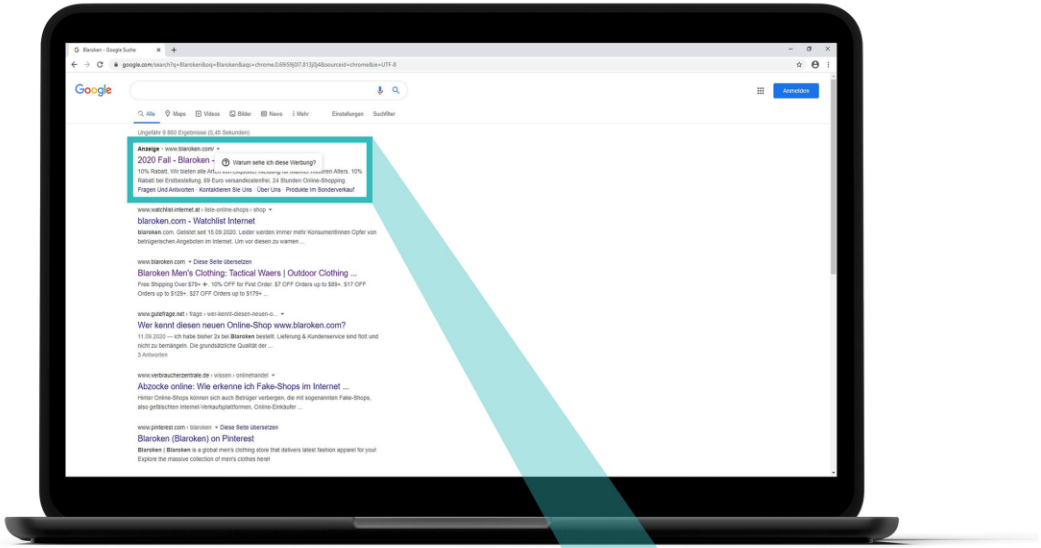
Betrügerische Werbung melden (Google)



Schritt 1:

Klicken Sie auf den Pfeil.

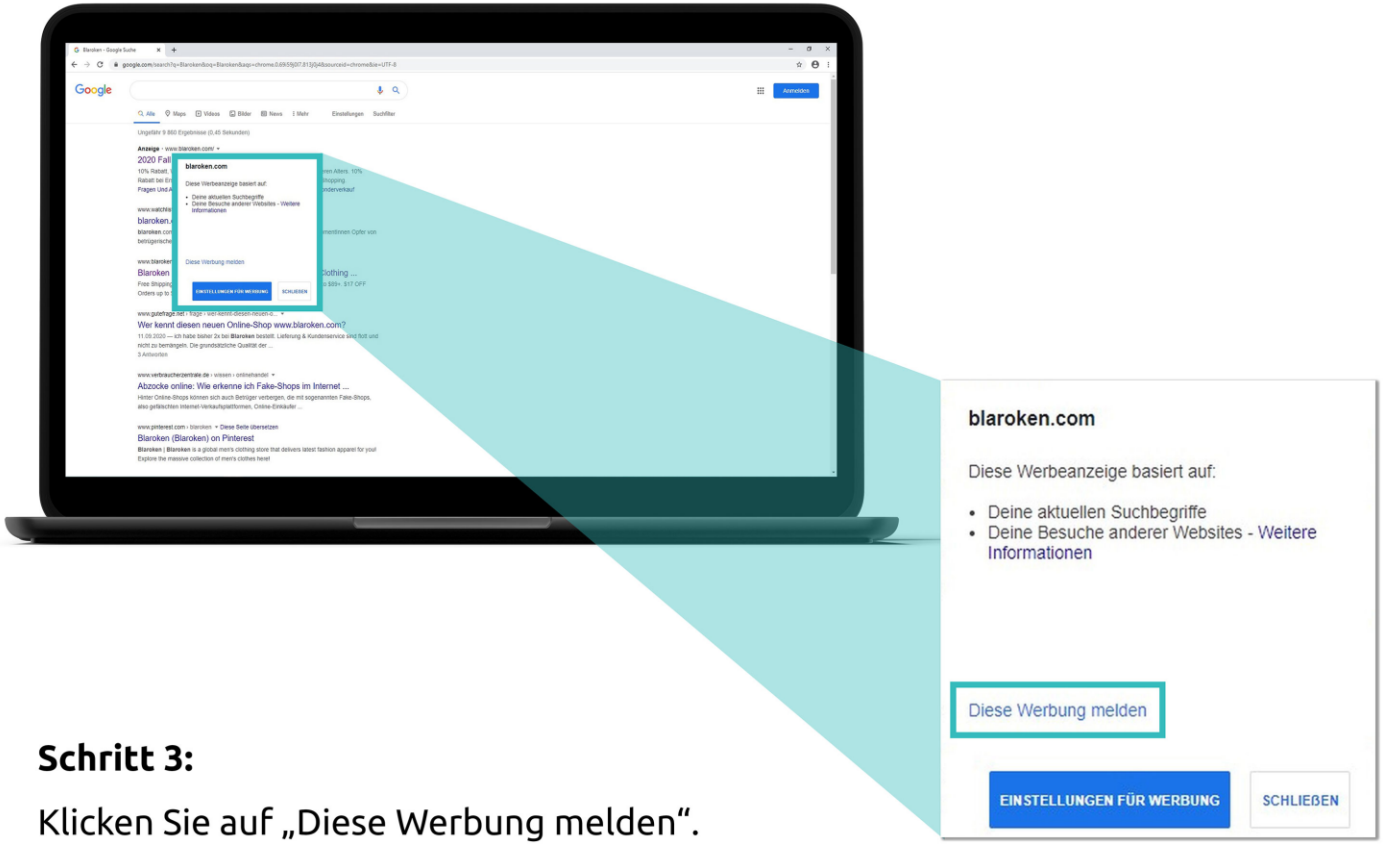
Betrügerische Werbung melden (Google)



Schritt 2:

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

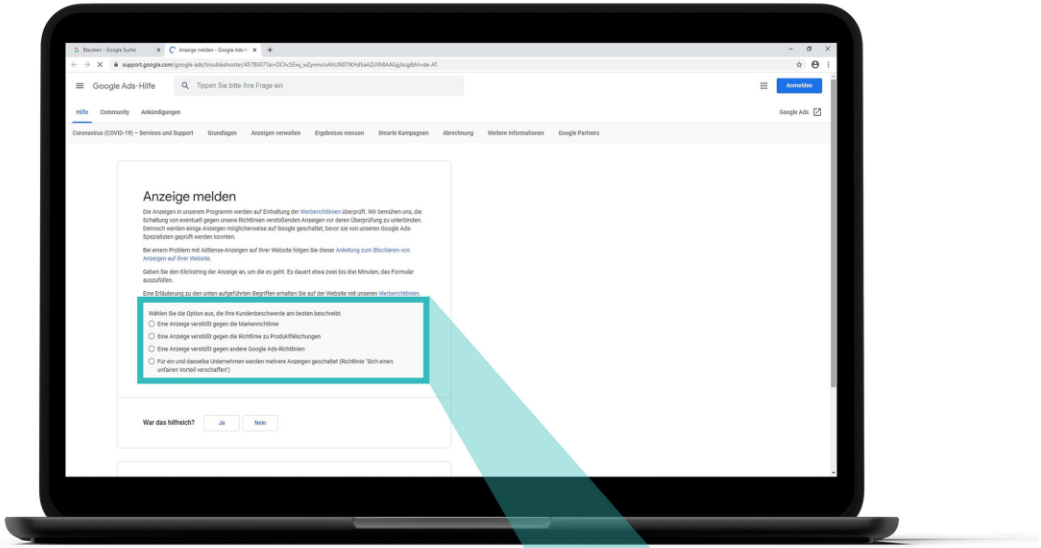
Betrügerische Werbung melden (Google)



Schritt 3:

Klicken Sie auf „Diese Werbung melden“.

Betrügerische Werbung melden (Google)



Schritt 4:

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

Betrügerische Werbung melden

Instagram

Quelle: pixabay.com

Betrügerische Werbung melden (Instagram)

Schritt 1:

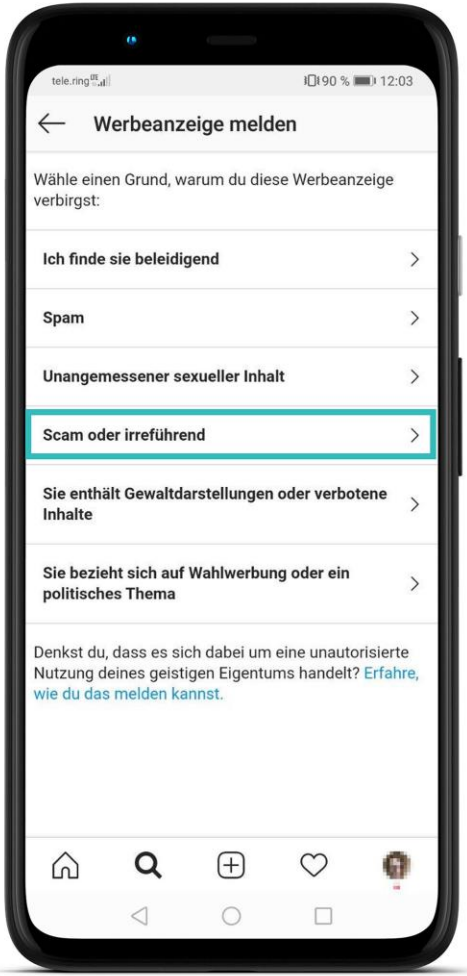
Klicken Sie auf die drei Punkte.

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

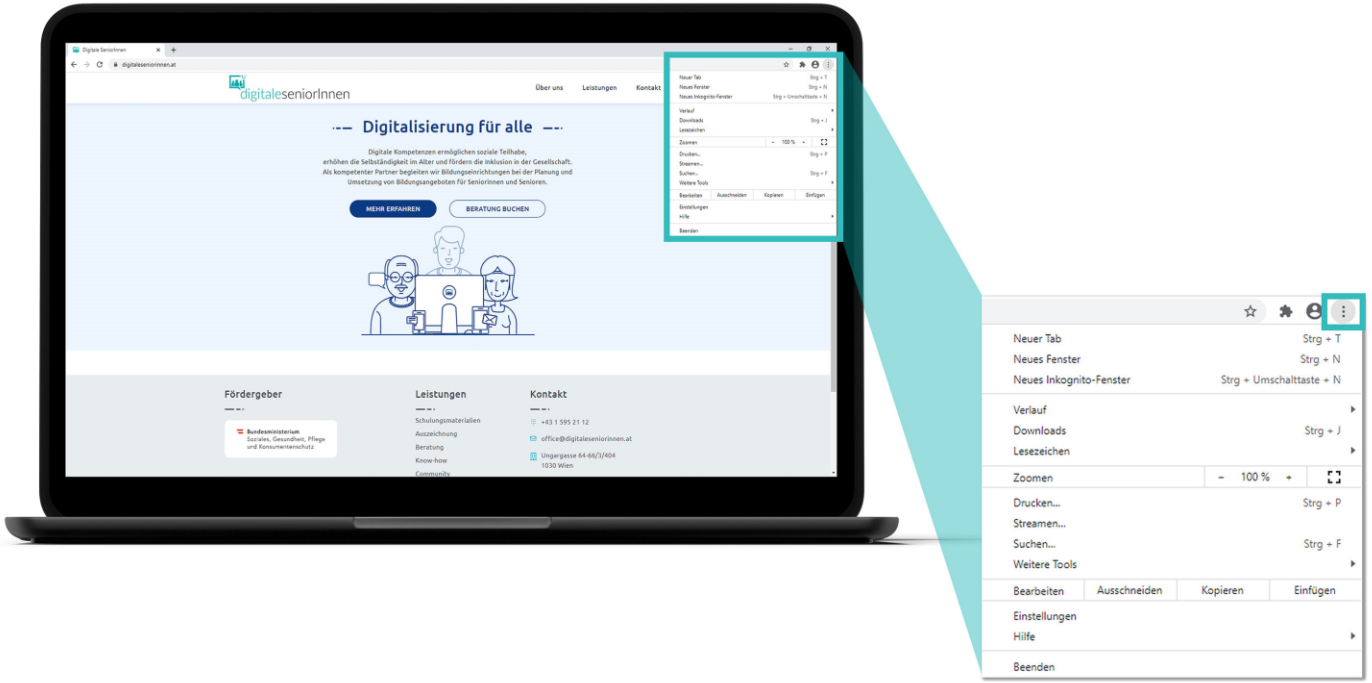
Quelle: pixabay.com

Phishing-Schutz einschalten

Chrome

Quelle: pixabay.com

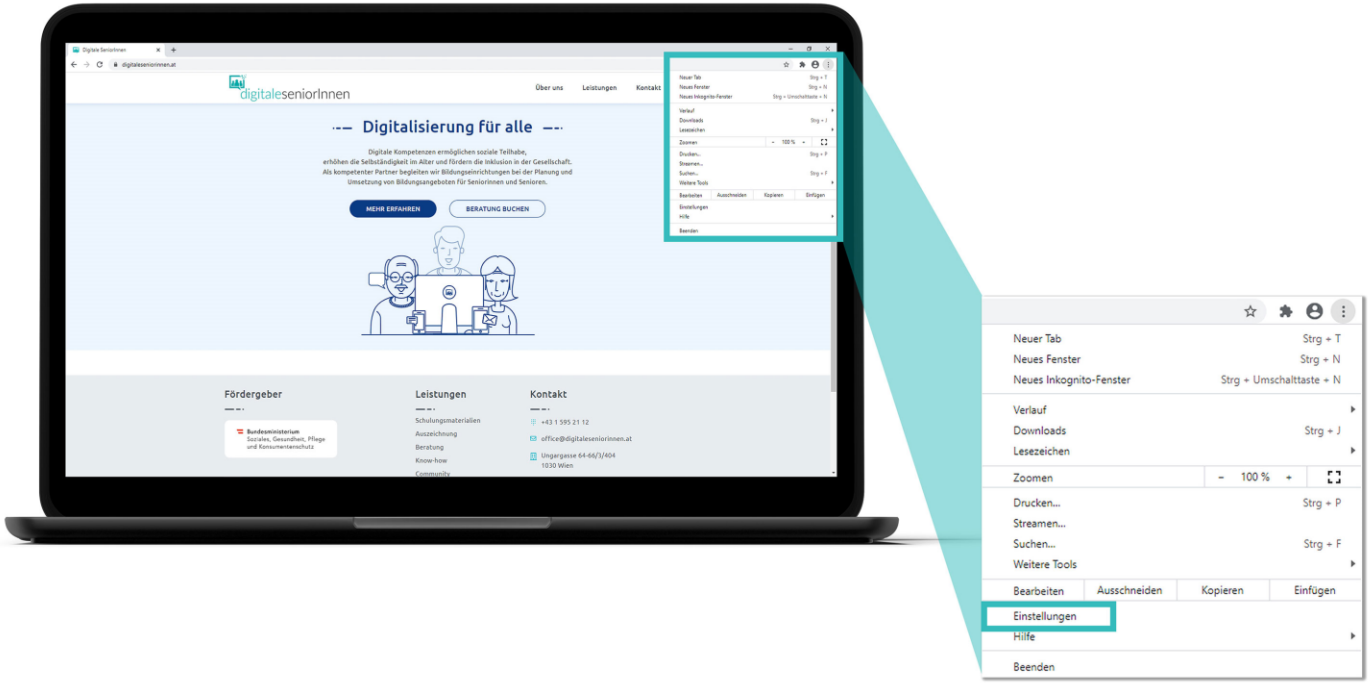
Schutz vor Phishing-Webseiten einschalten (Chrome)



Schritt 1:

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

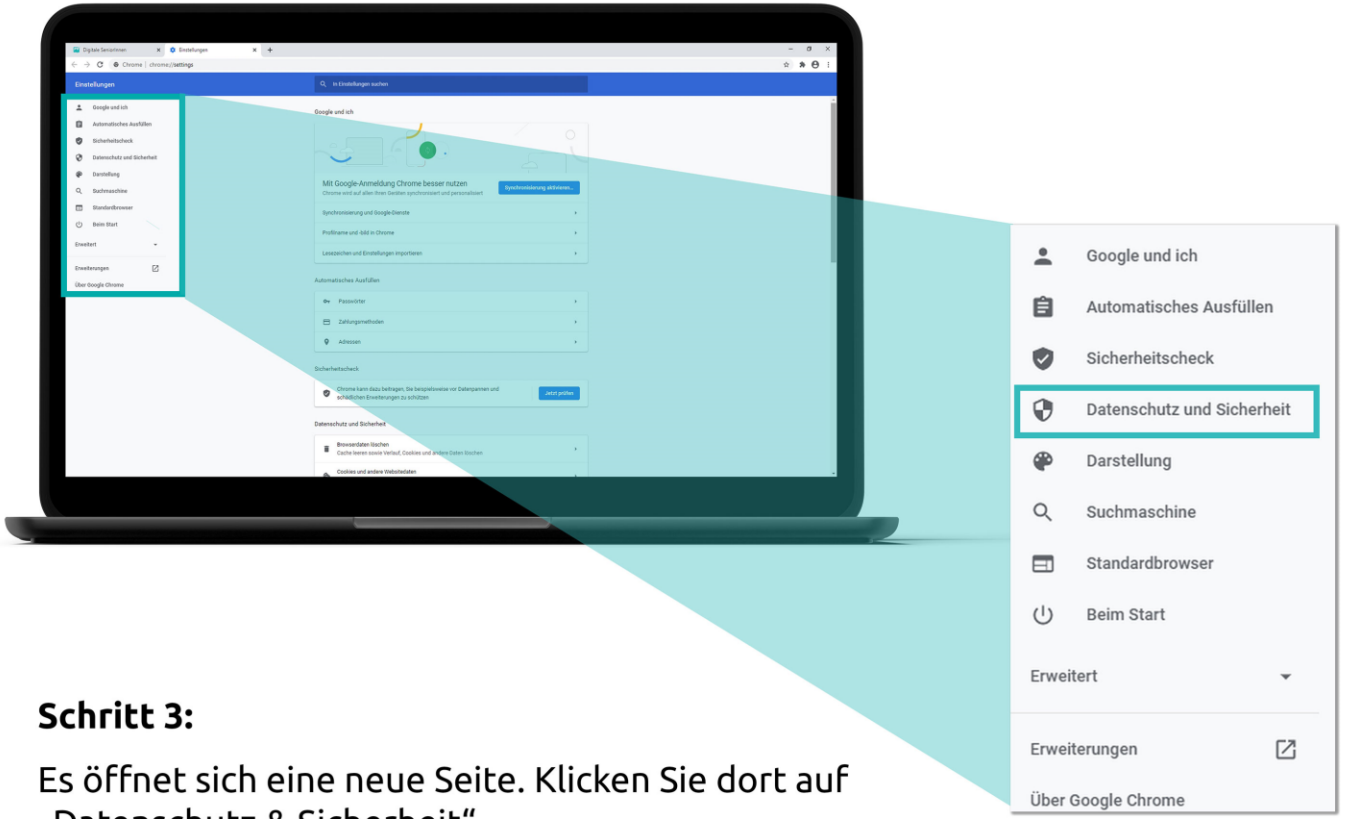
Schutz vor Phishing-Webseiten einschalten (Chrome)



Schritt 2:

Klicken Sie auf „Einstellungen“.

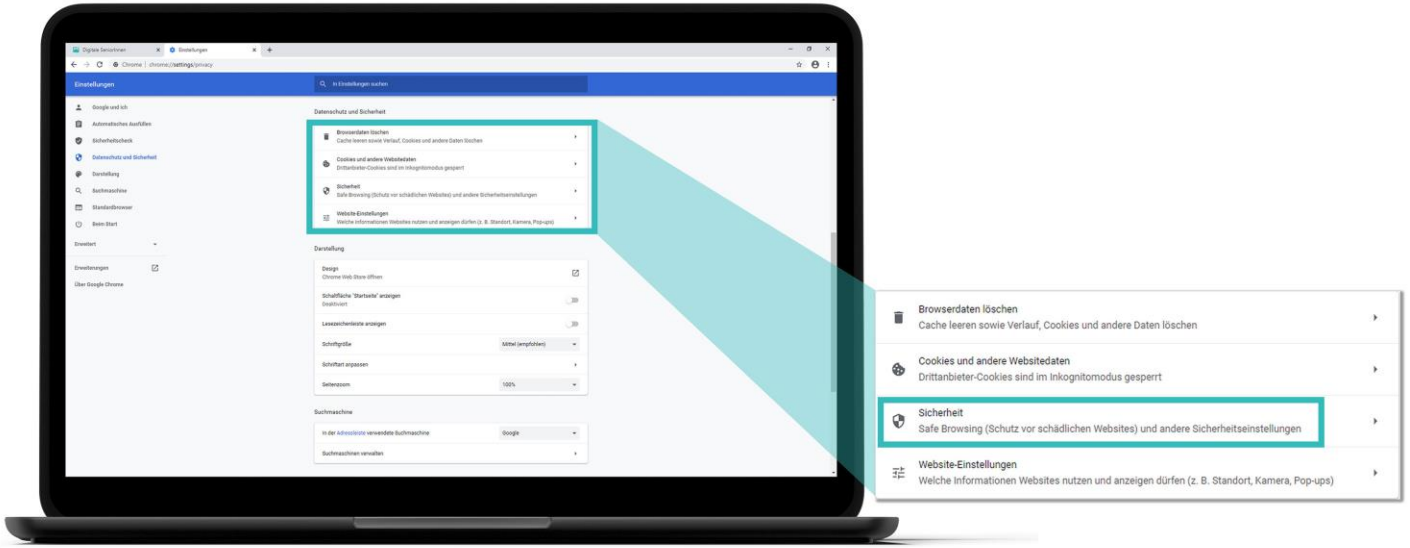
Schutz vor Phishing-Webseiten einschalten (Chrome)



Schritt 3:

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

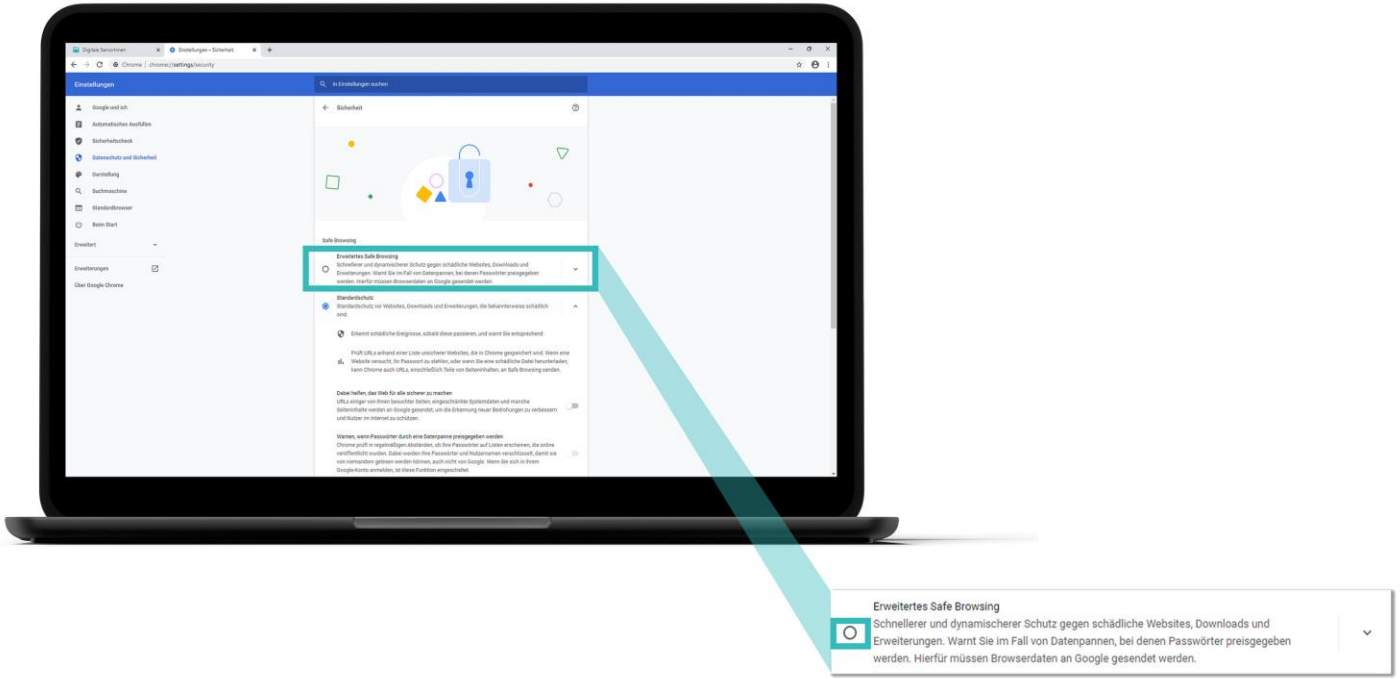
Schutz vor Phishing-Webseiten einschalten (Chrome)



Schritt 4:

Klicken Sie auf „Sicherheit“.

Schutz vor Phishing-Webseiten einschalten (Chrome)



Schritt 5:

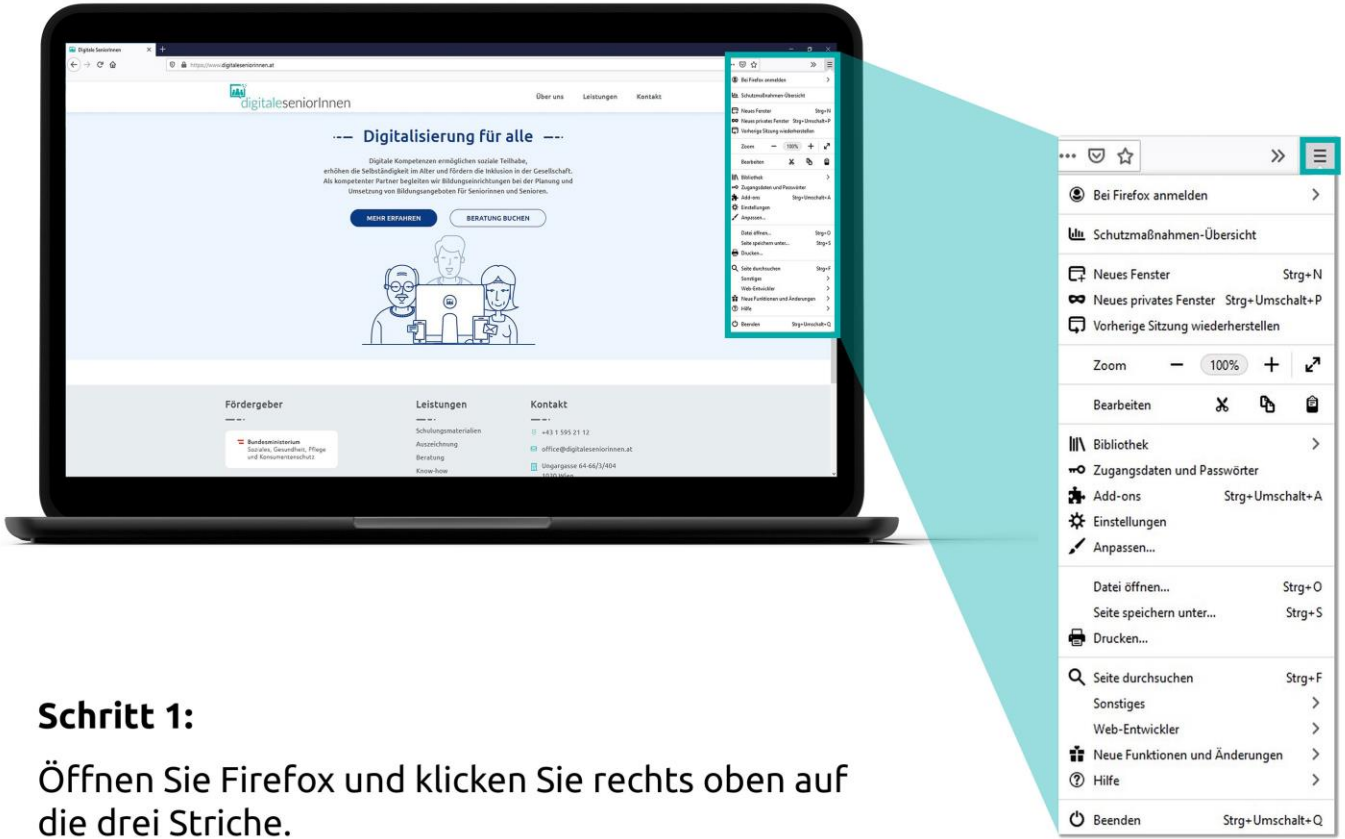
Klicken Sie auf „Erweitertes Safe Browsing“.

Phishing-Schutz einschalten

Firefox

Quelle: pixabay.com

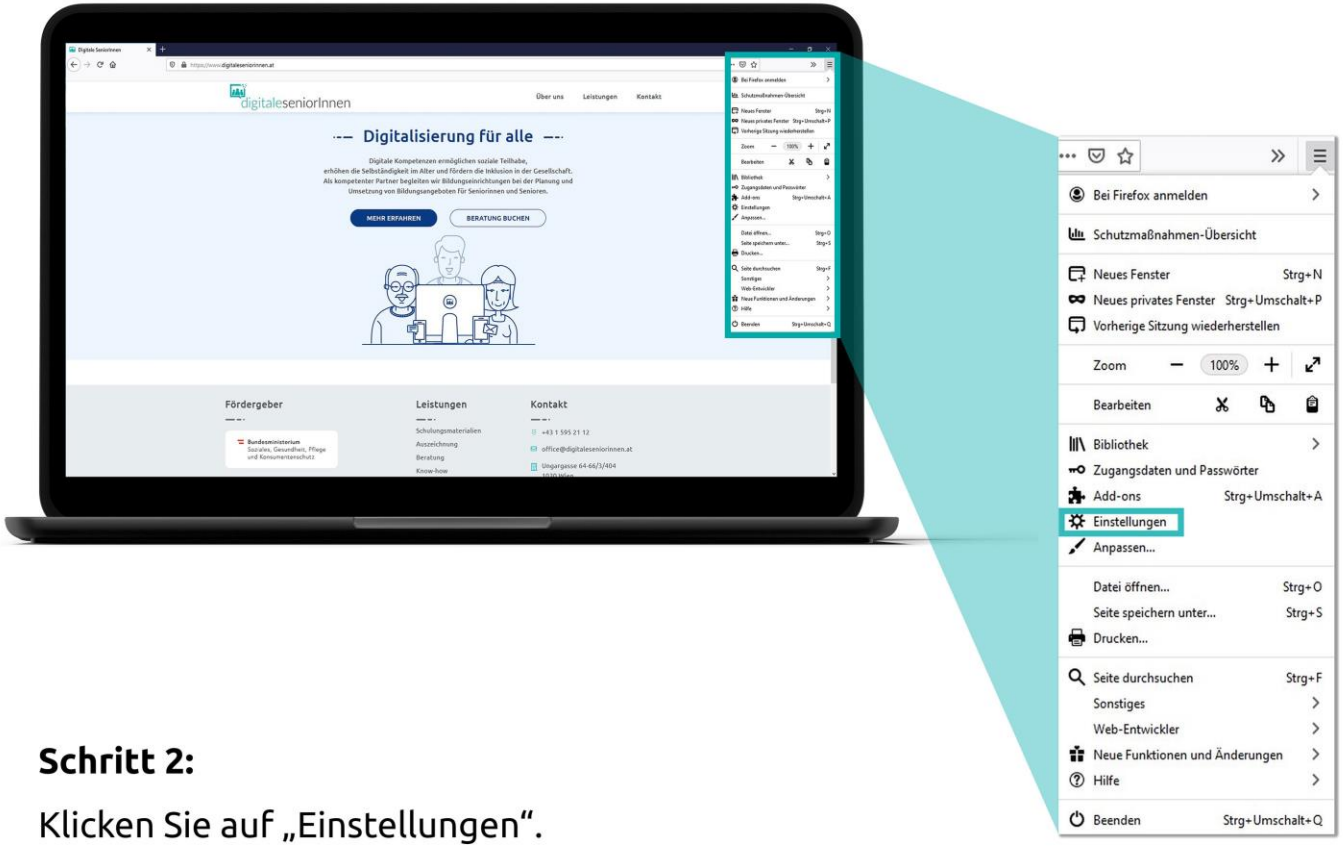
Schutz vor Phishing-Webseiten einschalten (Firefox)



Schritt 1:

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

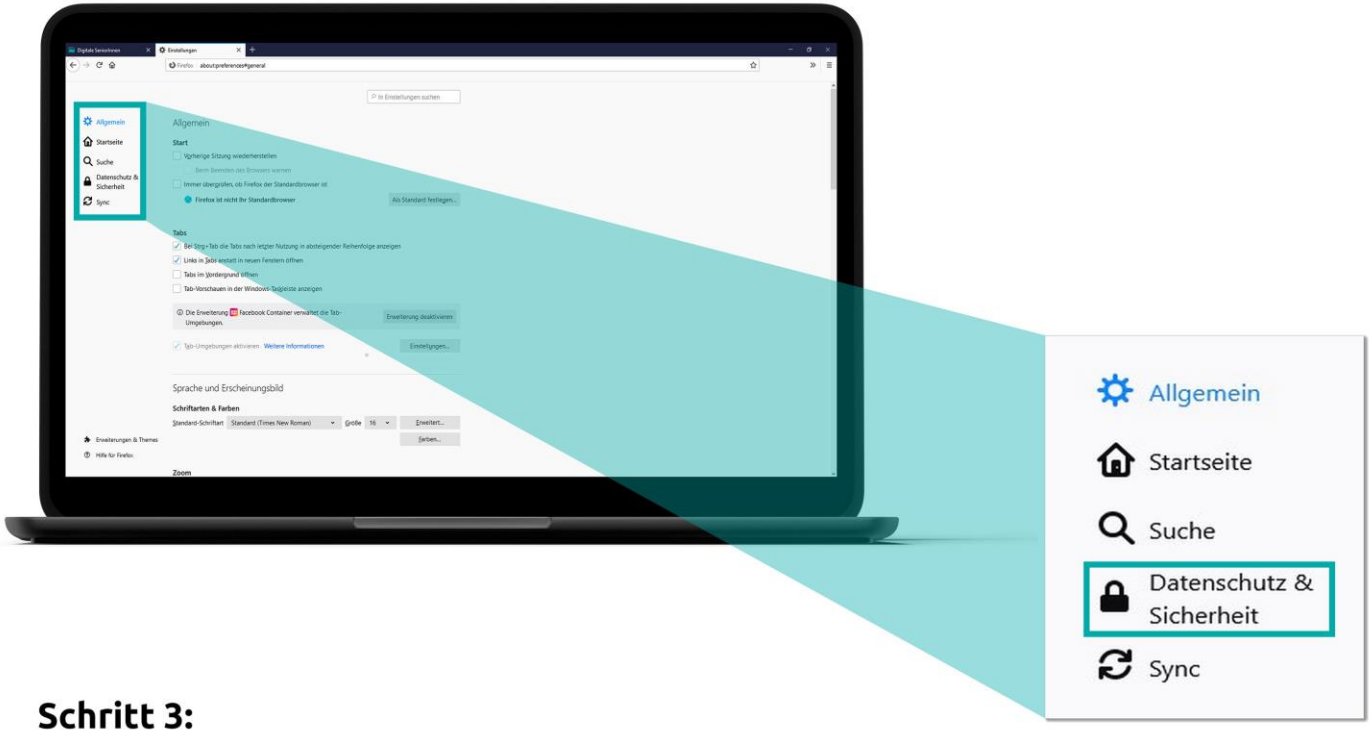
Schutz vor Phishing-Webseiten einschalten (Firefox)



Schritt 2:

Klicken Sie auf „Einstellungen“.

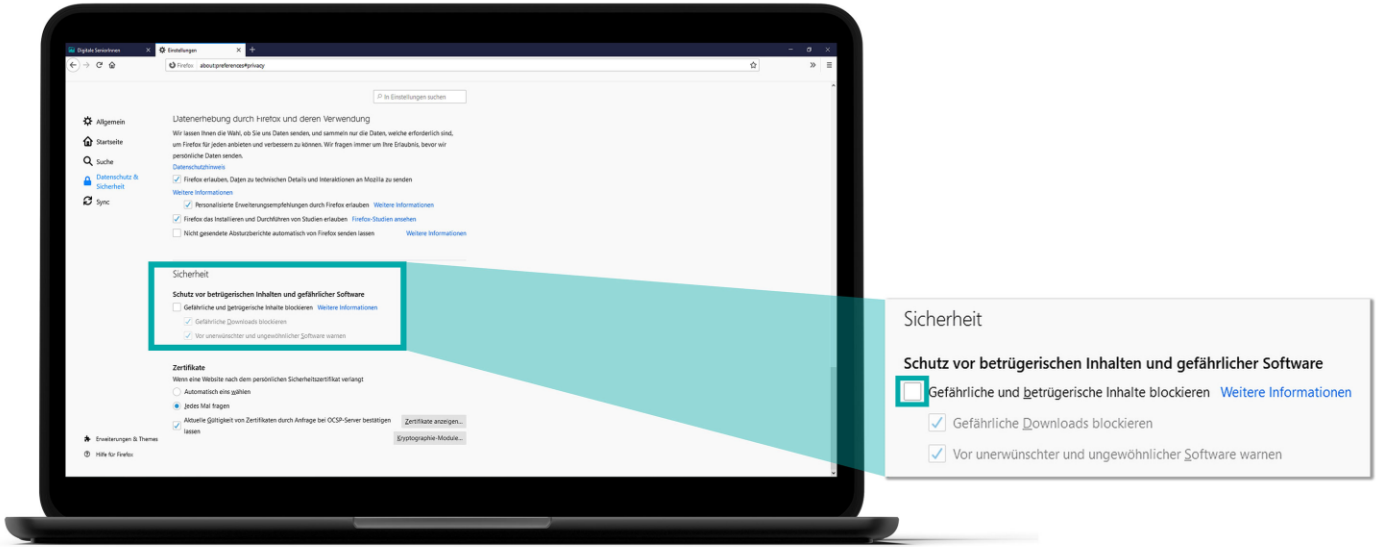
Schutz vor Phishing-Webseiten einschalten (Firefox)



Schritt 3:

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

Schutz vor Phishing-Webseiten einschalten (Firefox)



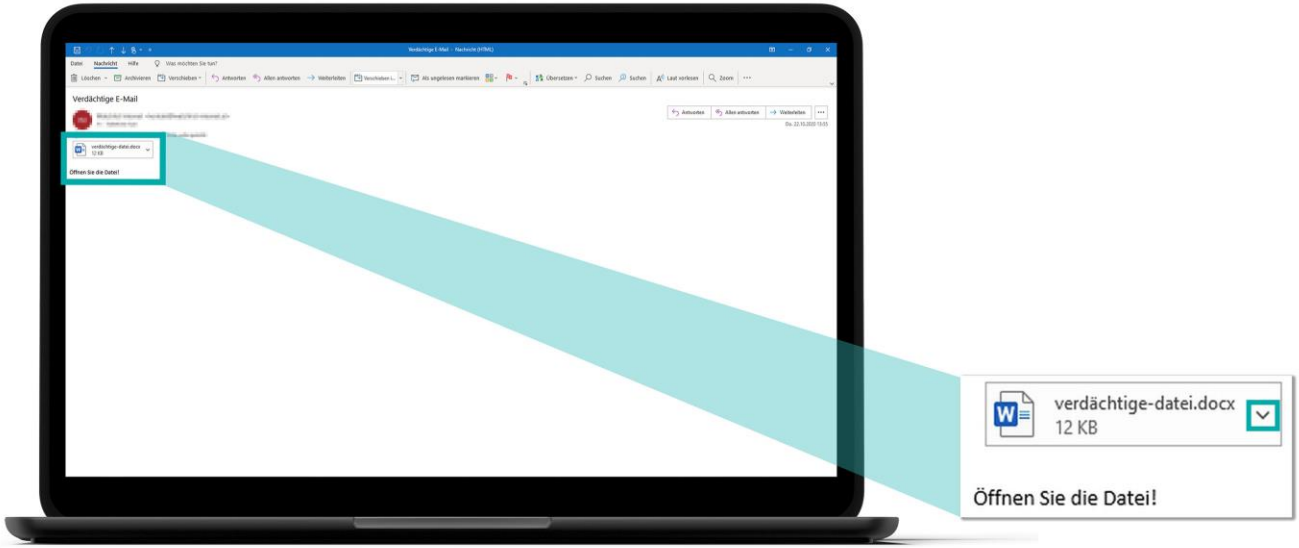
Schritt 4:

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

Dateien auf Viren überprüfen

Virustotal - https://www.virustotal.com

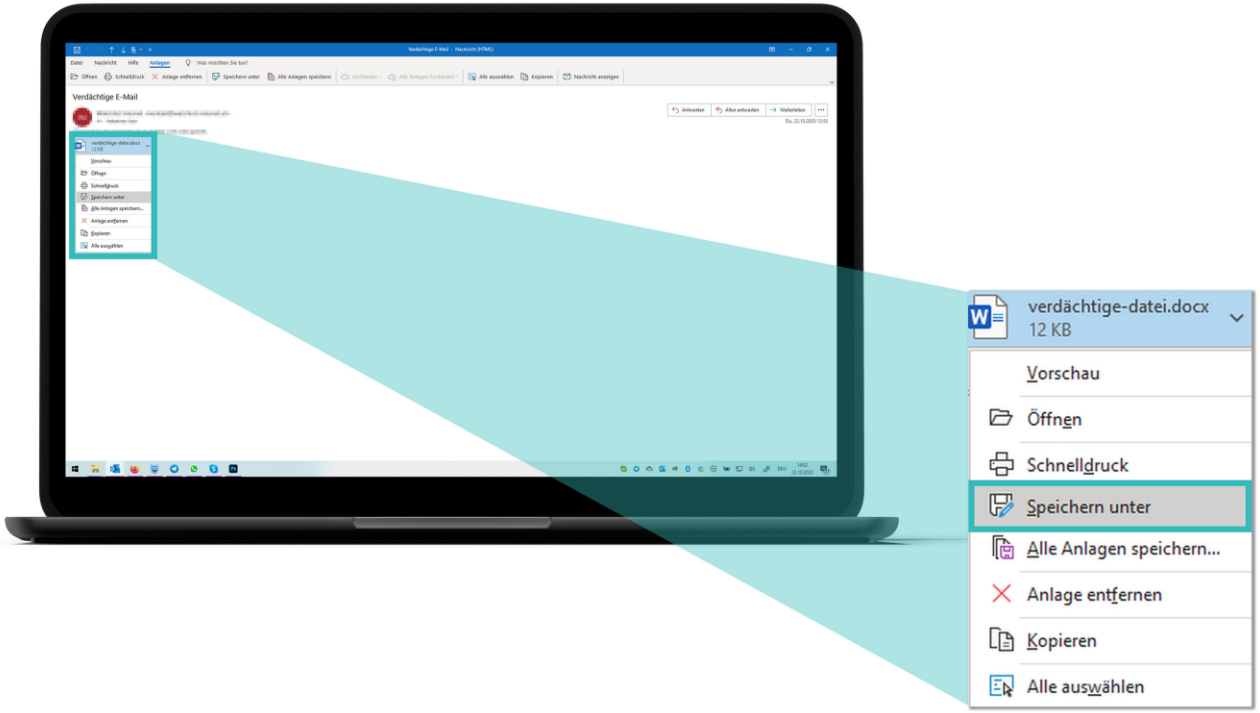
Überprüfung verdächtiger E-Mail-Anhänge



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!

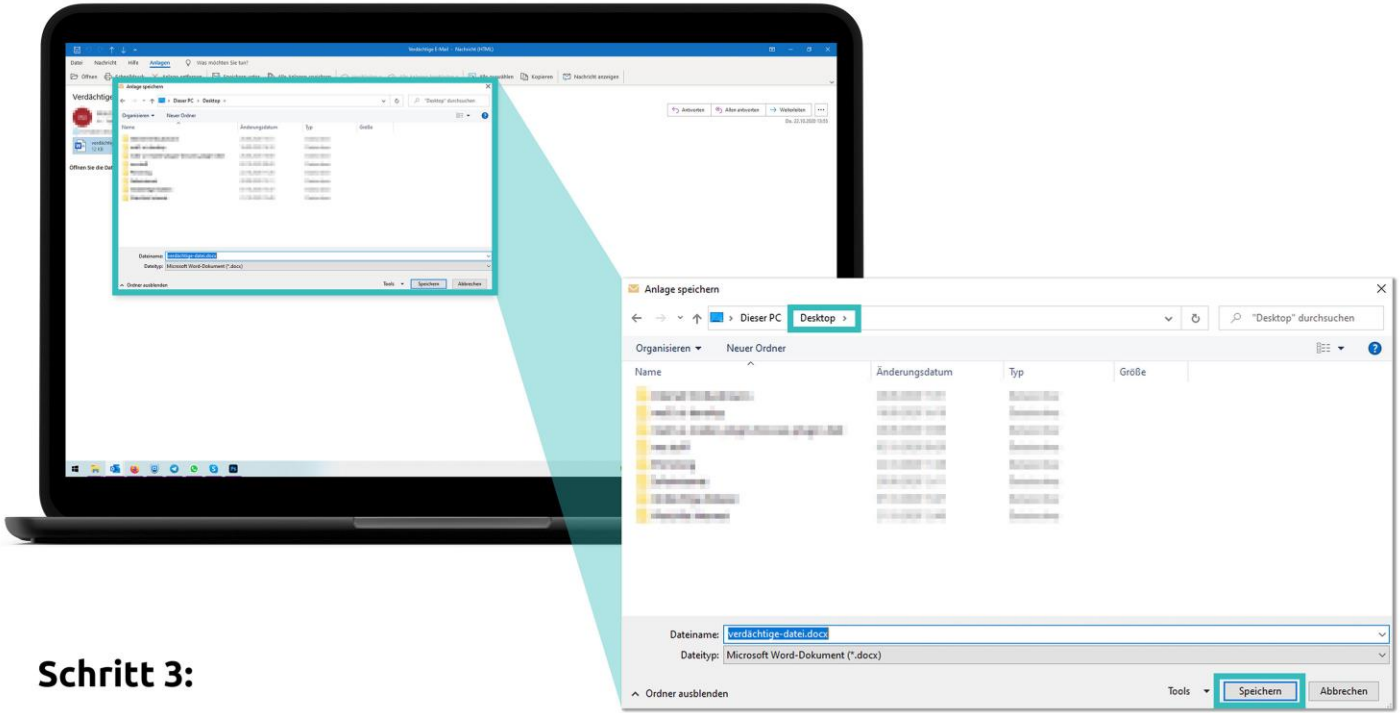
Überprüfung verdächtiger E-Mail-Anhänge



Schritt 2:

Klicken Sie auf „Speichern unter“.

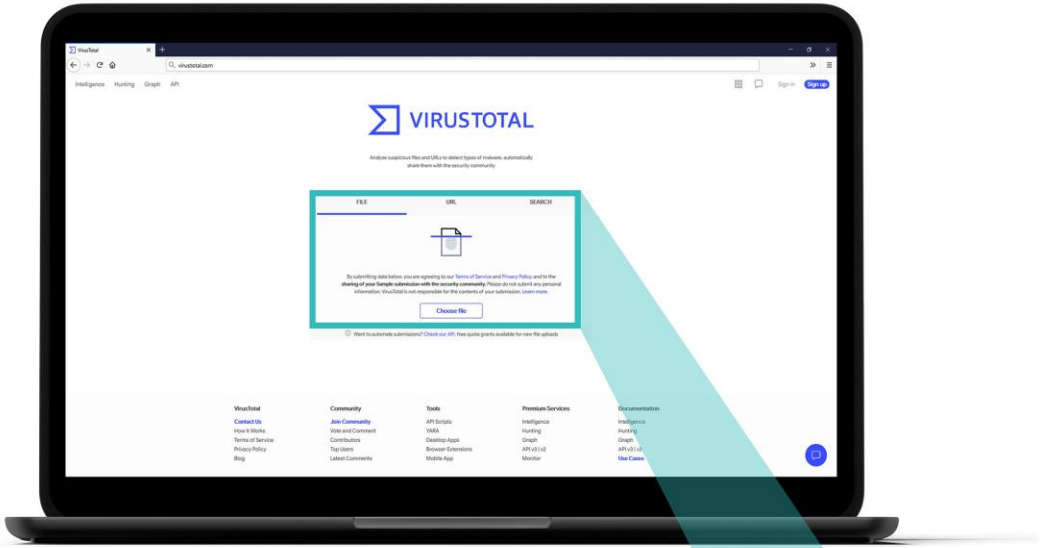
Überprüfung verdächtiger E-Mail-Anhänge

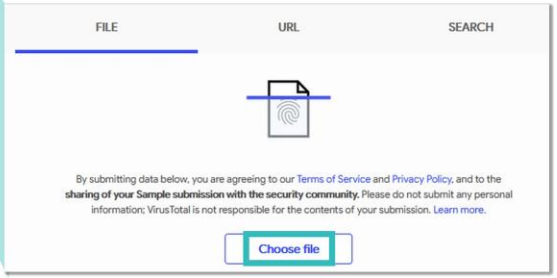


Schritt 3:

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

Überprüfung verdächtiger E-Mail-Anhänge

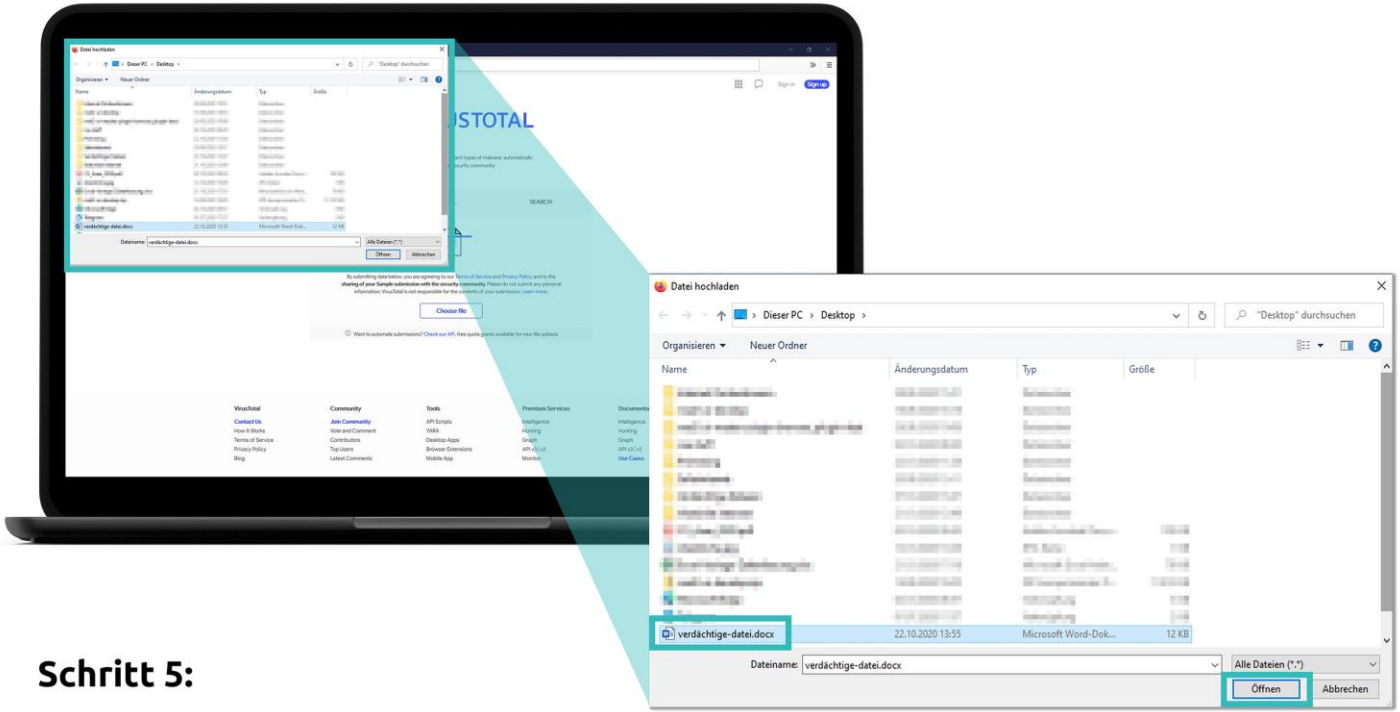




Schritt 4:

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

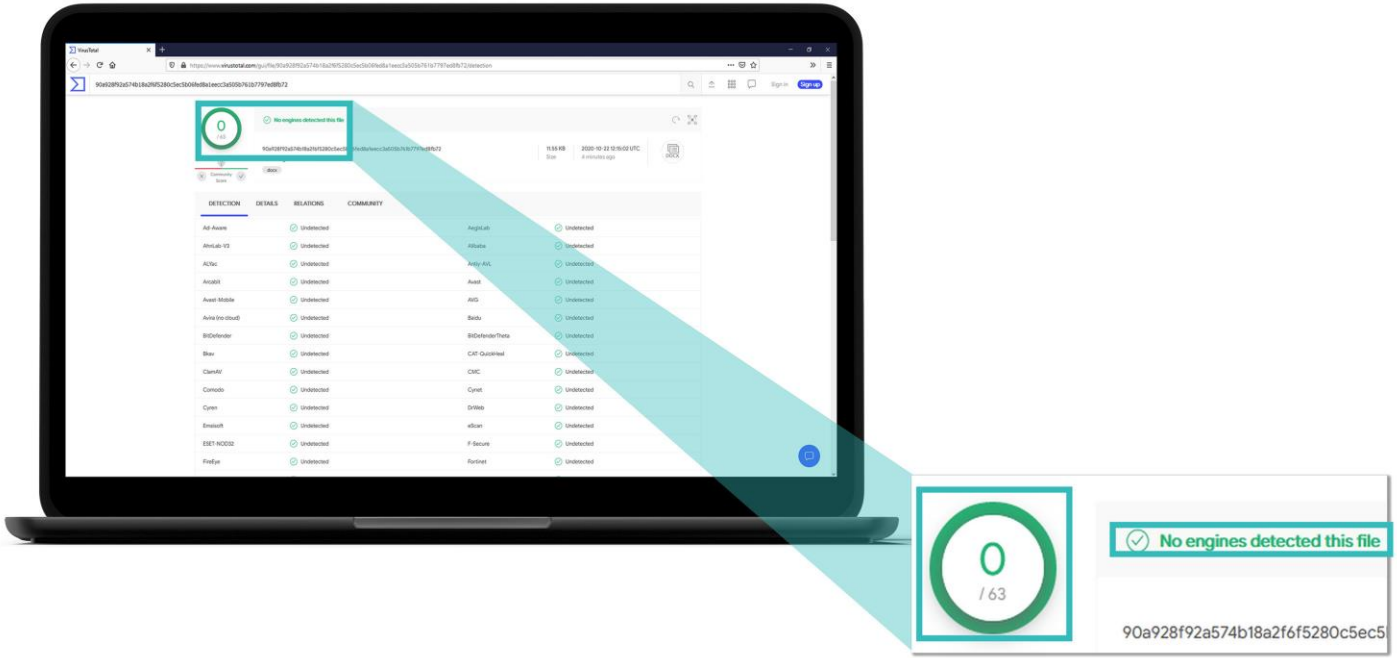
Überprüfung verdächtiger E-Mail-Anhänge



Schritt 5:

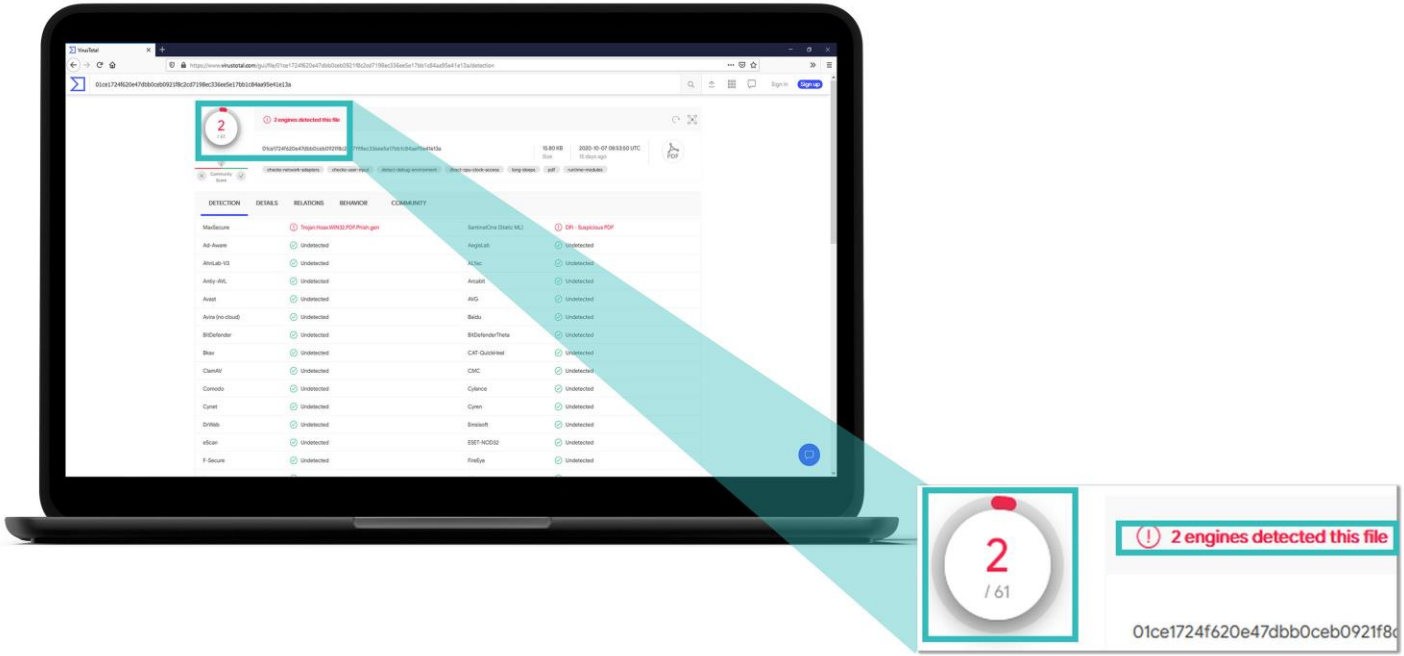
Es öffnet sich ein neues Fenster.
Klicken Sie auf die verdächtige Datei. Klicken Sie auf „Öffnen“.

Überprüfung verdächtiger E-Mail-Anhänge



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



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

digitaleseniorInnen
Servicestelle für Bildungseinrichtungen

DANKE FÜR IHRE AUFMERKSAMKEIT!