digitaleseniorInnen
Servicestelle für Bildungseinrichtungen

Internetkriminalität

Workshop

Informationen, Tipps und Übungen für den Unterricht

Internetkriminalität

Überblick

- Verkauf im Internet
- Schadsoftware
- Phishing

Quelle: pixabay.com

Internetkriminalität

Verkauf im Internet

- Abo-Fallen
- Kleinanzeigenbetrug
- Identitätsdiebstahl

Quelle: pixabay.com

Internetkriminalität

Abo-Fallen

Abo-Fallen sind vermeintlich kostenlose oder günstige Angebote, die aber zu hohen Rechnungen oder automatisierten Abbuchungen führen.

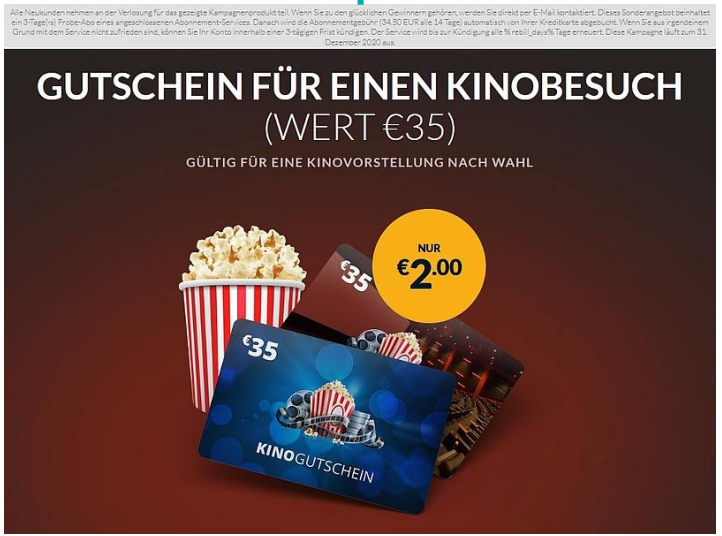
Quelle: pixabay.com

Internetkriminalität

Abo-Falle - Beispiel

Lockmittel: Gutschein

Dahinter versteckt sich eine Verlosung mit einem „Sonderangebot“ (Abo!)



Alle Neukunden nehmen an der Verlosung für das gezeigte Kampagnenprodukt teil. Wenn Sie zu den glücklichen Gewinnern gehören, werden Sie direkt per E-Mail kontaktiert. Dieses Sonderangebot beinhaltet ein 3-Tage(-s) Probe-Abo eines angeschlossenen Abonnement-Services. Danach wird die Abonnementgebühr (34.50 EUR alle 14 Tage) automatisch von Ihrer Kreditkarte abgebucht. Wenn Sie aus irgendeinem Grund mit dem Service nicht zufrieden sind, können Sie Ihr Konto innerhalb einer 3-tägigen Frist kündigen. Der Service wird bis zur Kündigung alle %rebill_days% Tage erneuert. Diese Kampagne läuft zum 31. Dezember 2020 aus.

Internetkriminalität

Abo-Fallen - Schutzmaßnahmen

Quelle: pixabay.com

- Seien Sie skeptisch bei unglaublich günstigen Angeboten.
- Achten Sie auf widersprüchliche oder unklare Beschreibung.
- Geben Sie keine persönlichen Daten (Name, Adresse, etc.) bekannt.
- Kontrollieren Sie die Websites ausführlich (Impressum, AGB, etc.).
- Suchen Sie nach dem Angebot auf www.watchlist-internet.at.
- Handeln Sie nicht unüberlegt.

Internetkriminalität

Kleinanzeigenbetrug

Quelle: pixabay.com

Kleinanzeigenportale wie Ebay, Willhaben, Shpock und Co. sind beliebt, um gebrauchte Ware entweder günstig zu kaufen oder verkaufen.

Kriminelle nutzen gezielt die Anonymität auf diesen Kleinanzeigenportalen.

Internetkriminalität

Kleinanzeigenbetrug - Varianten

Käuferinnen und Käufer werden Opfer durch

- Vorkasse-Trick
- Treuhandbetrug
- Liquiditätsbetrug

Verkäuferinnen und Verkäufer werden Opfer durch

- Scheckbetrug
- Trick mit der Track-ID
- PayPal-Trick

Internetkriminalität

Kleinanzeigenbetrug - Schutzmaßnahmen

Quelle: pixabay.com

- Seien Sie skeptisch bei überhöhten Zahlungen.
- Wickeln Sie den Kauf bzw. Verkauf persönlich ab und bezahlen Sie direkt bei der Übergabe der Ware und umgekehrt.
- Tauschen Sie keine Ausweiskopien beim Kleinanzeigenverkauf aus.
- Nutzen Sie die Kommunikationsmöglichkeiten der jeweiligen Kleinanzeigen-Plattform.

Internetkriminalität

Identitätsdiebstahl

Quelle: pixabay.com

Mit gestohlenen Ausweispapieren (Pass, Führerschein, etc.) können Kriminelle vorgeben eine andere Person zu sein, Konten eröffnen, Einkäufe tätigen und unter falschem Namen Straftaten begehen.

Internetkriminalität

Identitätsdiebstahl - Beispiele

- Betrügerische Marktforschungsinstitute
- Betrügerische Stellenausschreibungen

***** *Mitarbeiter gesucht!* *****

Wir suchen ab sofort wieder österreichweit engagierte Damen und Herren, die uns in der vorweihnachtlichen Zeit unterstützen und uns behilflich sind im Verkauf von Christbaumschmuck und Weihnachtsaccessoires.

Arbeitszeit: 20 Stunden Woche (Freitag/Samstag)
Arbeitsbeginn: 1. bis 23. Dezember 2017
Verdienst: € 950,–/netto

Unsere 350 Verkaufsstände sind in Form von 3×3 Meter großen Holzhütten mit Beleuchtung und Deko fix und fertig für Sie bereits in diversen Shoppingcentern in ganz Österreich aufgestellt.

Für diese Tätigkeit sind keine besonderen Berufserfahrungen notwendig; ein fließendes Deutsch in Wort und Schrift sowie die Volljährigkeit werden jedoch vorausgesetzt.

Haben wir Ihr Interesse geweckt?

Dann senden Sie Ihre vollständigen Bewerbungsunterlagen inklusive einer Kopie (Foto) des Reisepasses an Hr. Ivanovic unter jobcenter.austria@outlook.com

Internetkriminalität

Identitätsdiebstahl - Schutzmaßnahmen

Quelle: pixabay.com

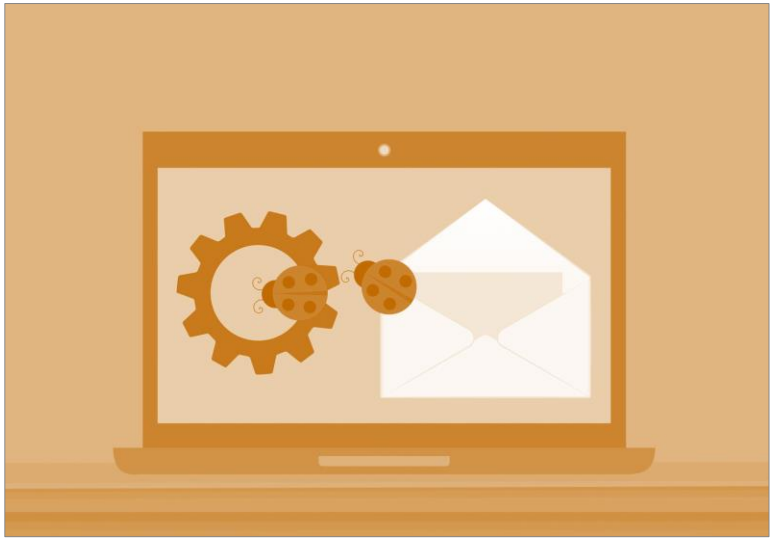
- Fügen Sie ein Wasserzeichen ein.
  Das Wasserzeichen soll darüber Auskunft geben, dass es sich um eine Kopie handelt, welchem Zweck die Kopie dient, für wen sie bestimmt ist und wann sie erstellt wurde.
- Schwärzen Sie nicht benötigte Informationen.

https://www.watchlist-internet.at/news/ausweiskopien-mit-wasserzeichen-versehen/

Internetkriminalität

Schadsoftware

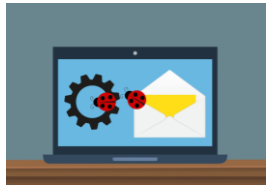
- Ransomware
  verschlüsselt Systeme
- Spyware
  spioniert Systeme aus
- Viren
  zerstören Systeme



Quelle: pixabay.com

Internetkriminalität

Schadsoftware - Schutzmaßnahmen



Quelle: pixabay.com

- Installieren Sie Programme nur von offiziellen Websites.
- Öffnen Sie keine Datei-Anhänge deren Herkunft unklar ist.
- Installieren Sie Updates.
- Trennen Sie Administrator- und Benutzerkonten.
- Aktivieren Sie Firewall- und Anti-Viren-Programme.
- Führen Sie regelmäßig Backups durch.

Internetkriminalität

Phishing

Phishing ist ein Begriff, der sich aus dem Englischen für „password harvesting“ (Passwort ernten) und „fishing“ (angeln, fischen) zusammensetzt.

Quelle: pixabay.com

Internetkriminalität

Phishing - Beispiel

In der Nachrichten wird aufgefordert auf einen Link zu klicken.

Dieser führt zu einer Phishing-Seite, die der Website des nachgeahmten Unternehmens ähnelt.

Die Opfer sollen sich dort einloggen und/oder ihre Kreditkartendaten eingeben.

Ihre Rechnung

Ihre letzte Rechnung wurde zweimal bezahlt

Sehr geehrte Frau, Herr,

Aufgrund eines Fehlers unserer Rechnungsabteilung wurde Ihnen das Doppelte Ihrer letzten Rechnung in Rechnung gestellt
Bitte fordern Sie eine sofortige Rückerstattung

Offener Betrag: €159,25
Rechnungsnummer: 151813247

Haben Sie Fragen zu Ihrer Rechnung?
Hier finden Sie eine Rechnungserklärung, die alle Abschnitte der Rechnung im Detail beschreibt.

Nutzen Sie schon Mein Magenta - Ihr Online Kundenportal?
Sie können damit jederzeit

- Ihre Daten aktualisieren
- Ihre letzten 12 Rechnungen einsehen
- Rechnungen mit einer elektronischen Signatur anfordern

Falls Sie Mein Magenta noch nie genutzt haben, registrieren Sie sich bitte zuerst.

Internetkriminalität

Phishing - Schutzmaßnahmen

Quelle: pixabay.com

- Überprüfen Sie die Absenderadresse.
- Hinterfragen Sie den Inhalt der Nachricht.
- Achten Sie auf Grammatik und Rechtschreibung.
- Kontaktieren Sie das Unternehmen direkt und fragen Sie nach.
- Überprüfen Sie die Internetadresse auf Fehler. *(bawagpks.at ≠ bawagpsk.at)*
- Aktivieren Sie in Ihrem Browser den Schutz vor Phishing-Webseiten.

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

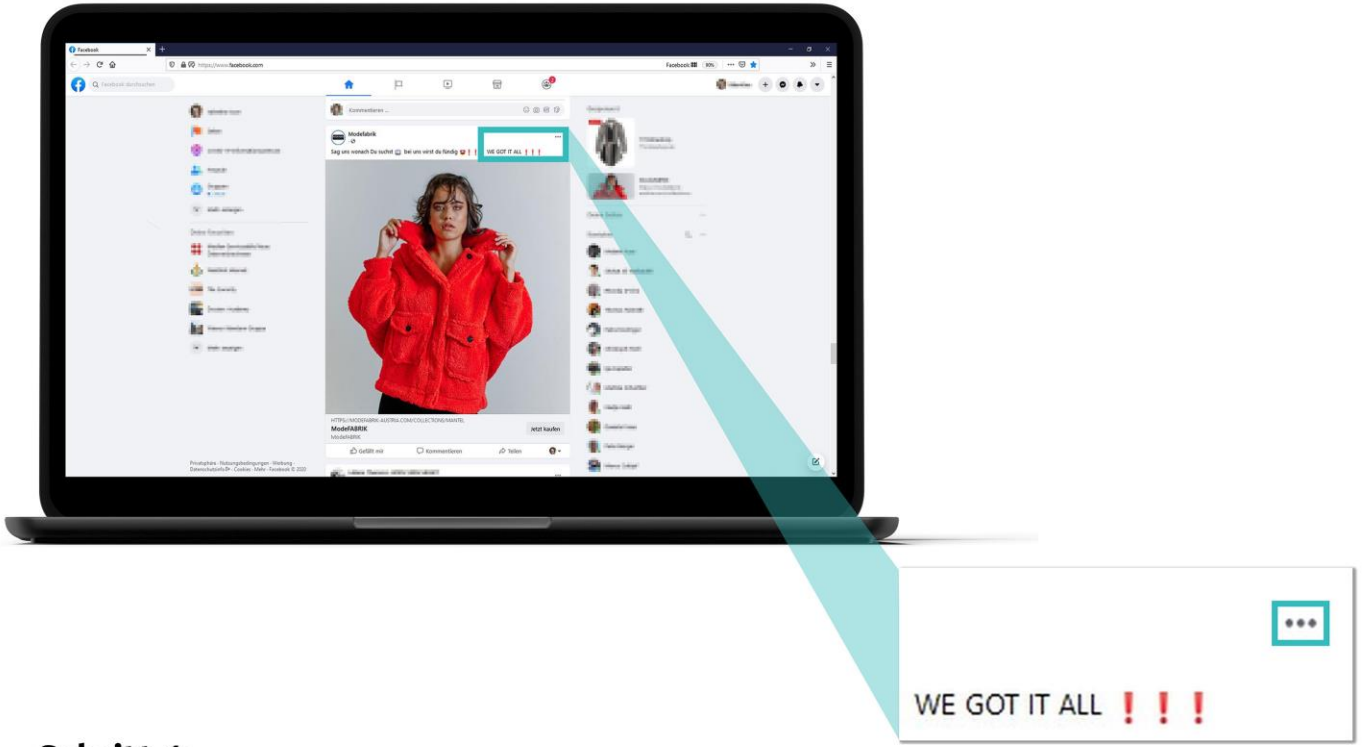
Quelle: pixabay.com

Betrügerische Werbung melden

Facebook

Quelle: pixabay.com

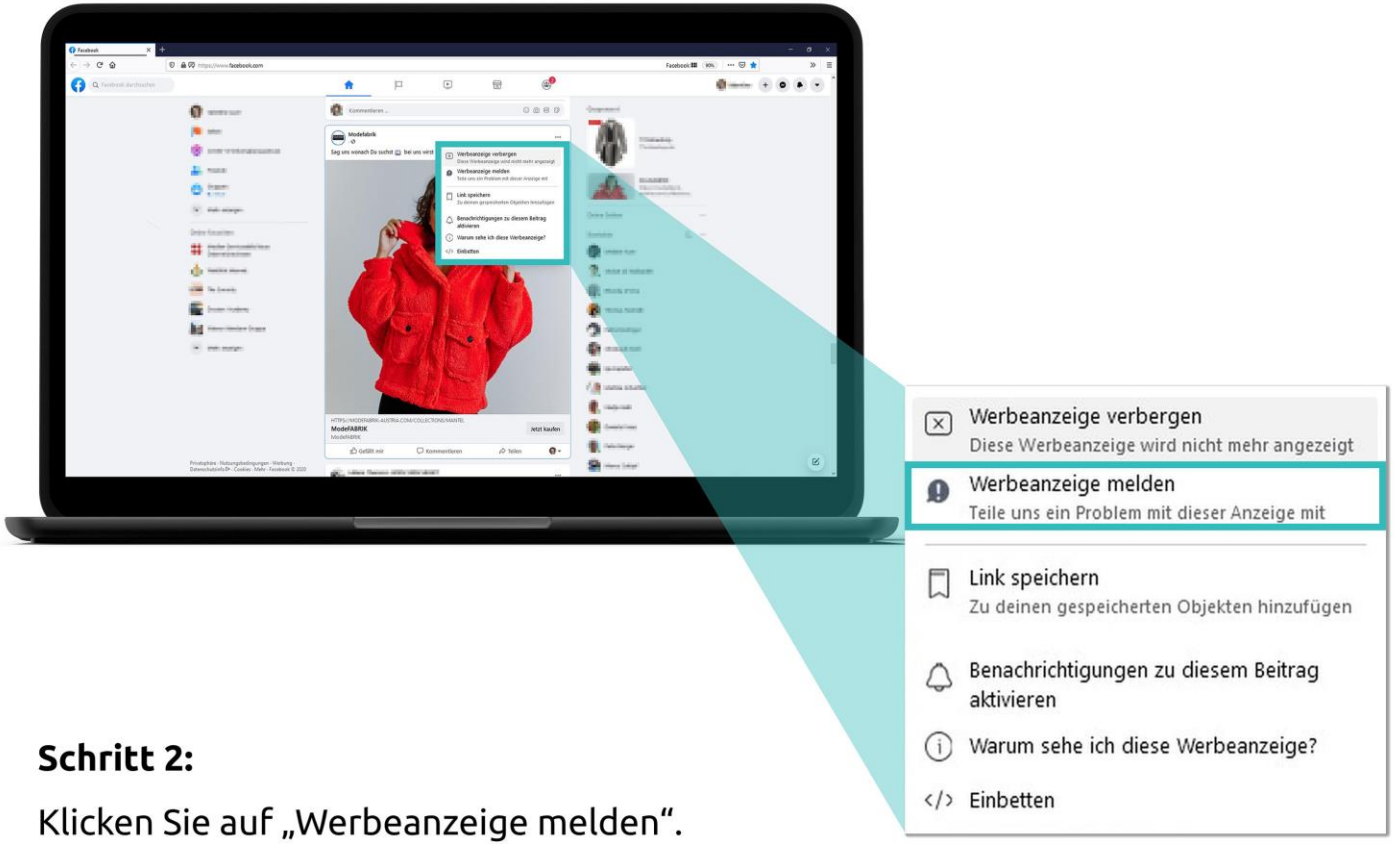
Betrügerische Werbung melden (Facebook)



Schritt 1:

Klicken Sie auf die drei Punkte.

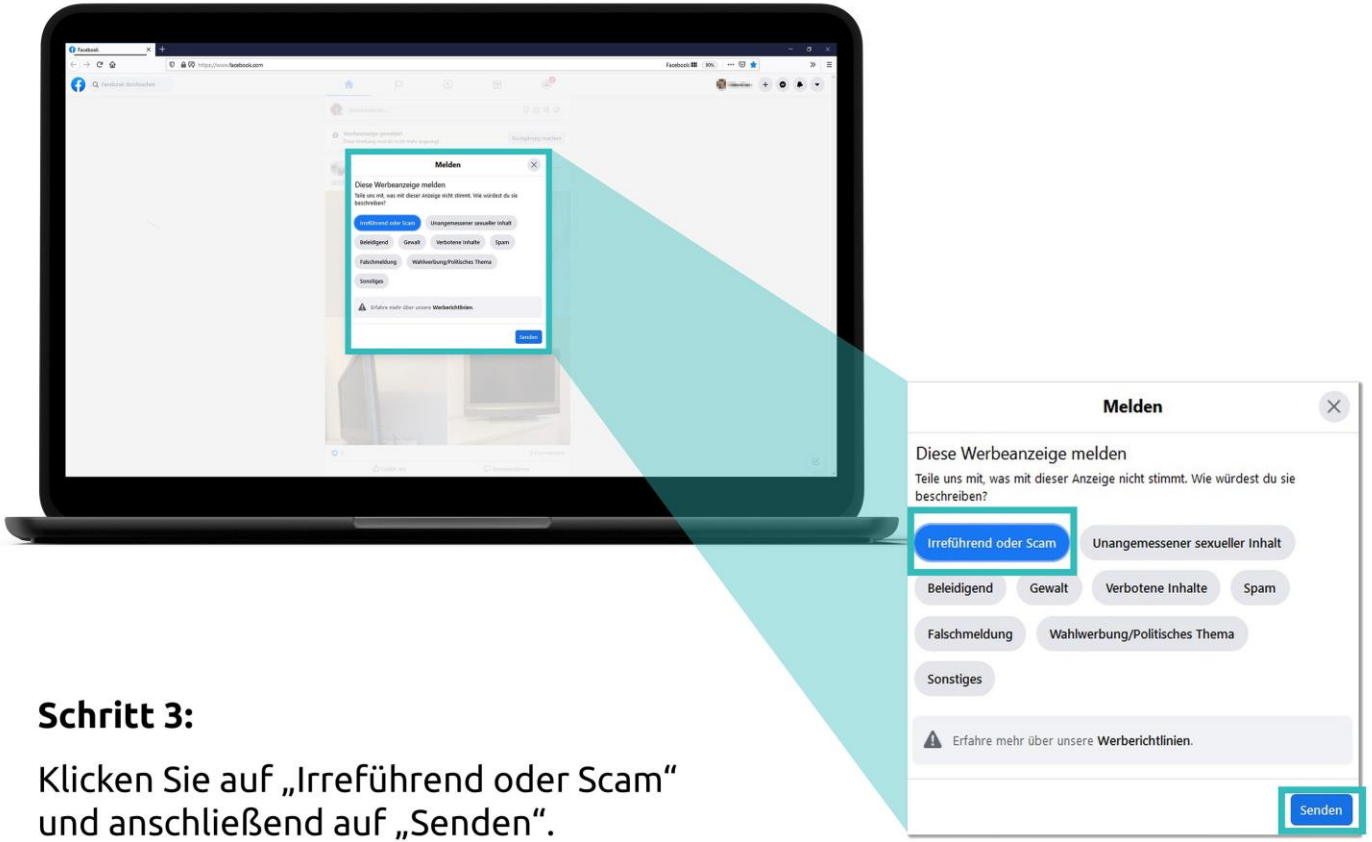
Betrügerische Werbung melden (Facebook)



Schritt 2:

Klicken Sie auf „Werbeanzeige melden“.

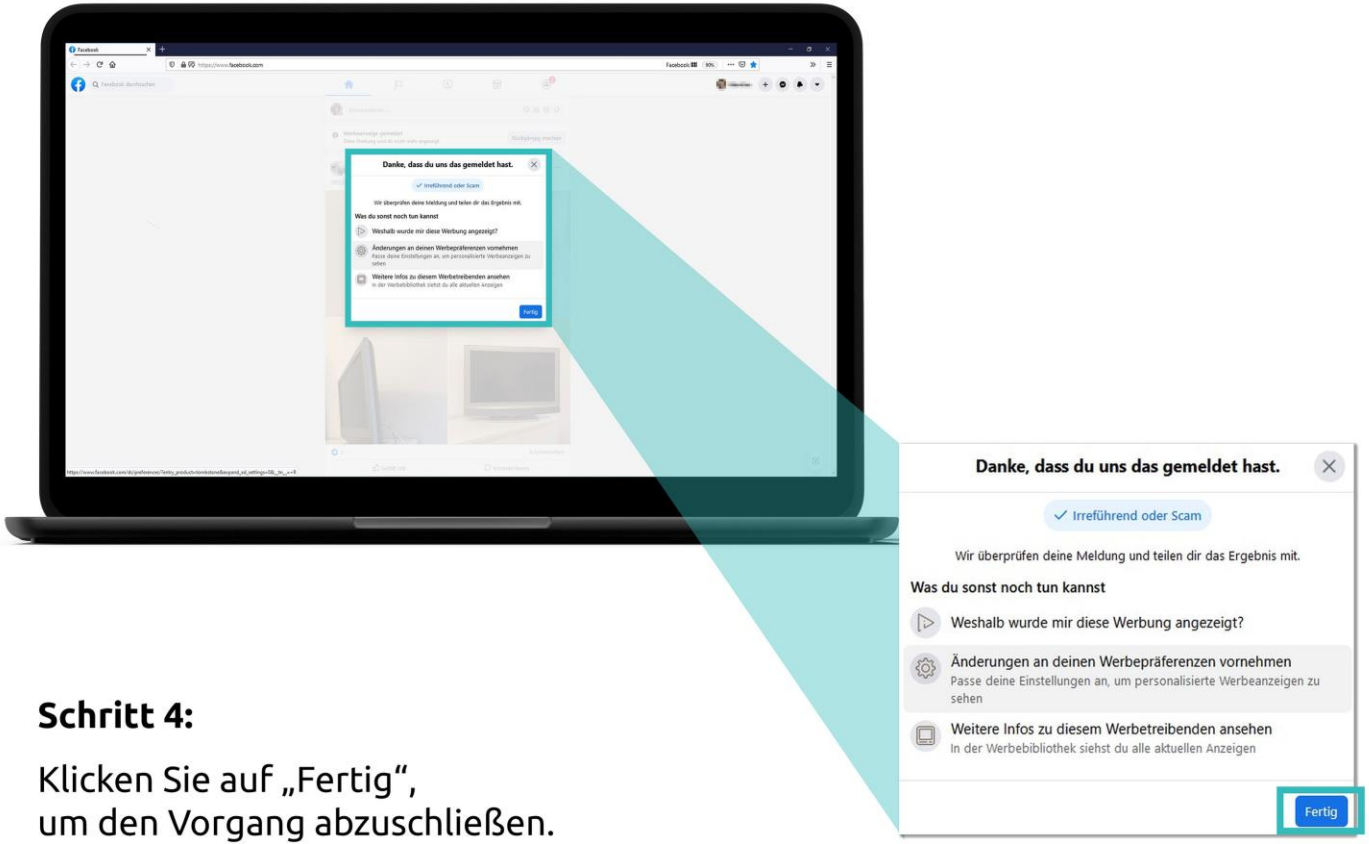
Betrügerische Werbung melden (Facebook)



Schritt 3:

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

Betrügerische Werbung melden (Facebook)



Schritt 4:

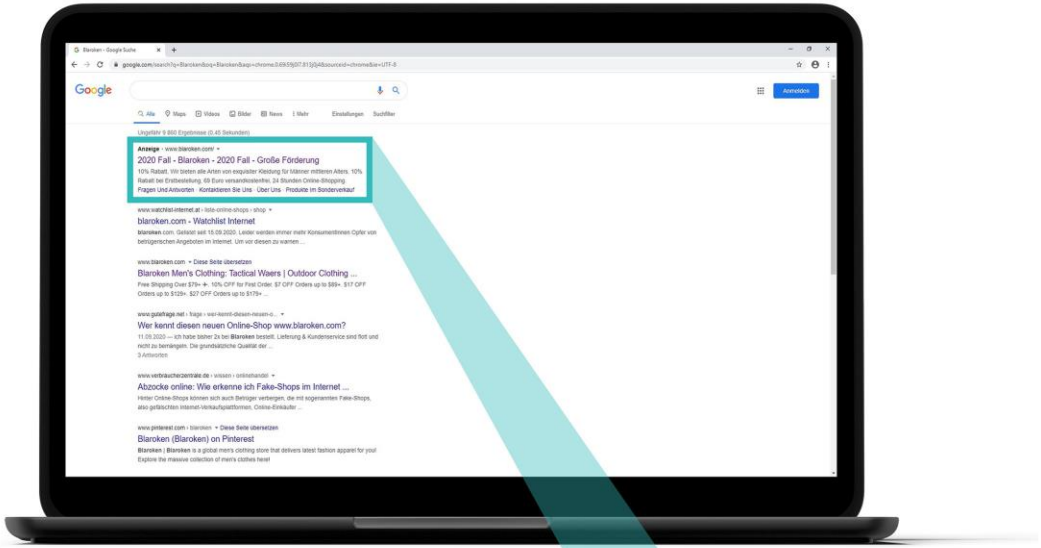
Klicken Sie auf „Fertig“,
um den Vorgang abzuschließen.

Betrügerische Werbung melden

Google

Quelle: pixabay.com

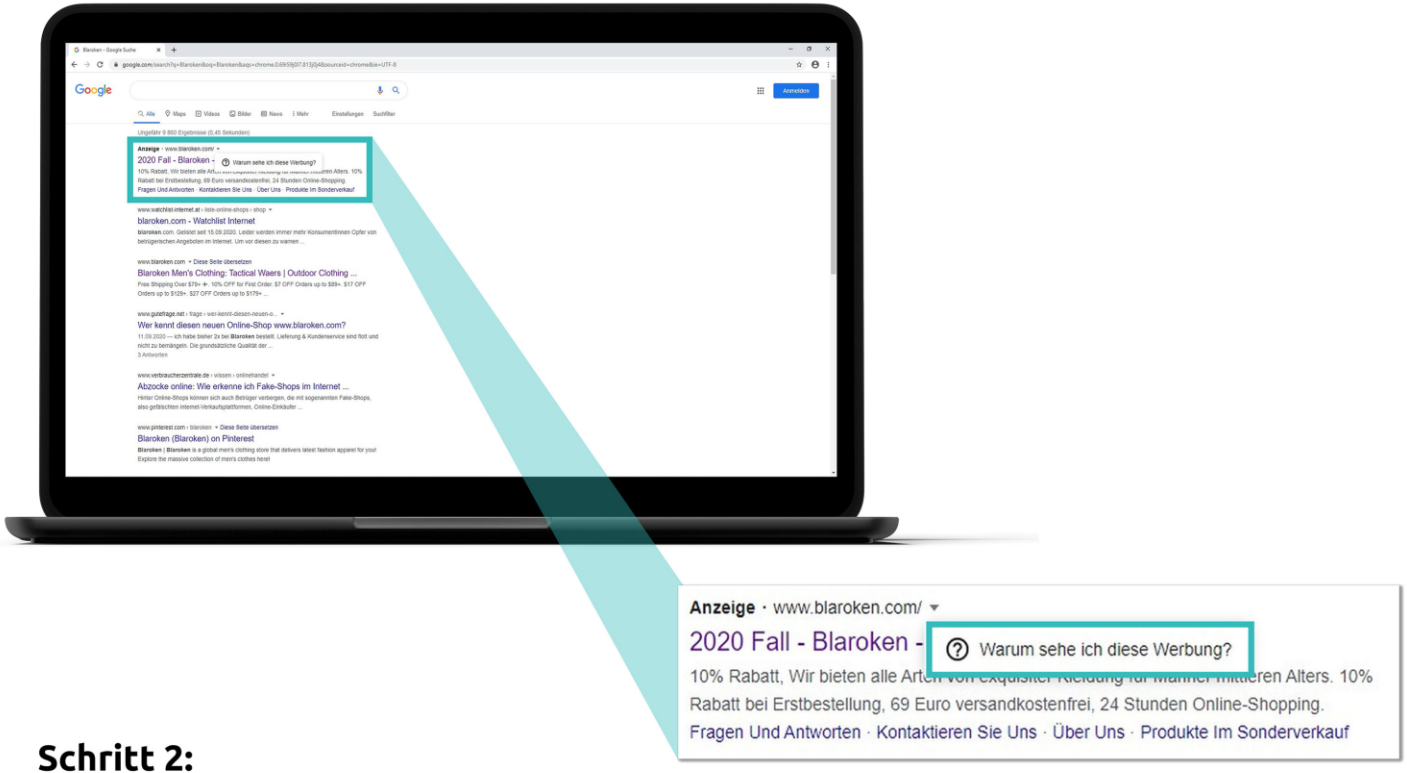
Betrügerische Werbung melden (Google)



Schritt 1:

Klicken Sie auf den Pfeil.

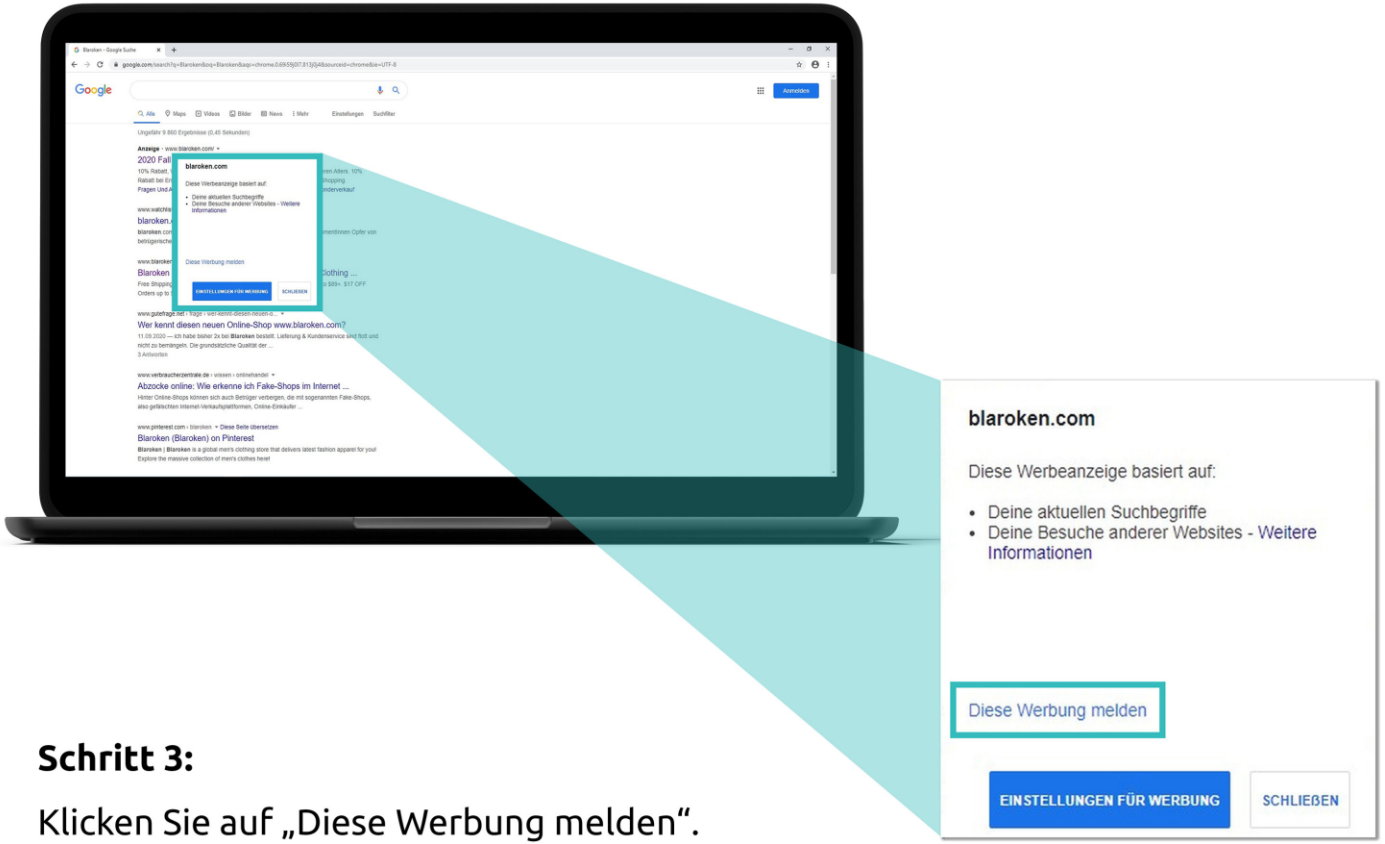
Betrügerische Werbung melden (Google)



Schritt 2:

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

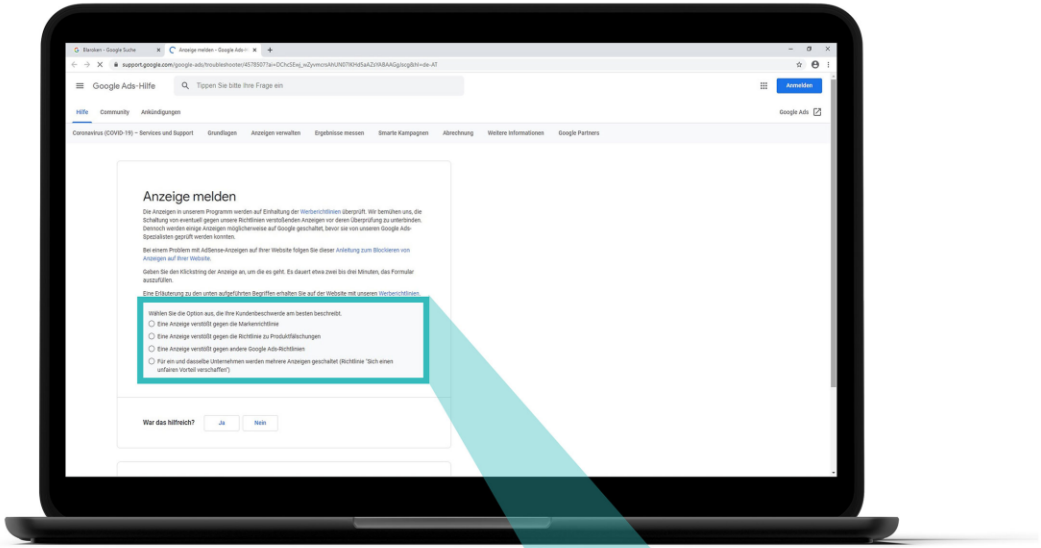
Betrügerische Werbung melden (Google)



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:

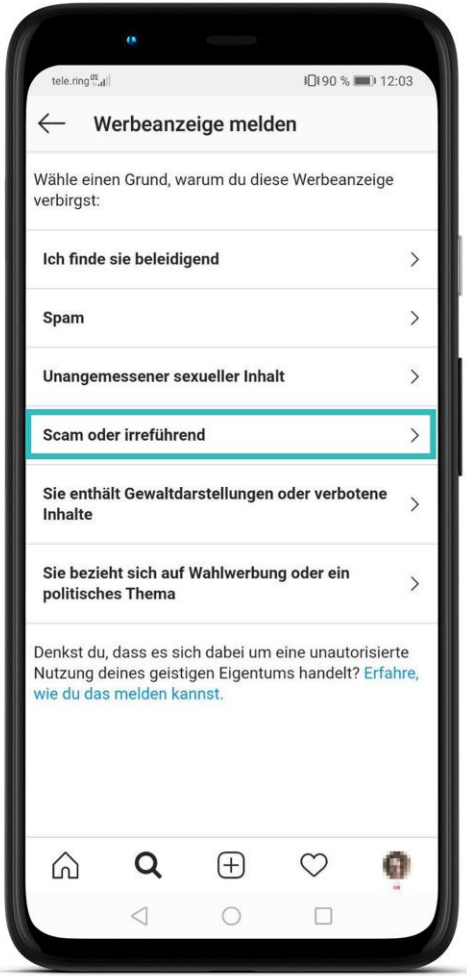
Klicken Sie auf die drei Punkte.

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

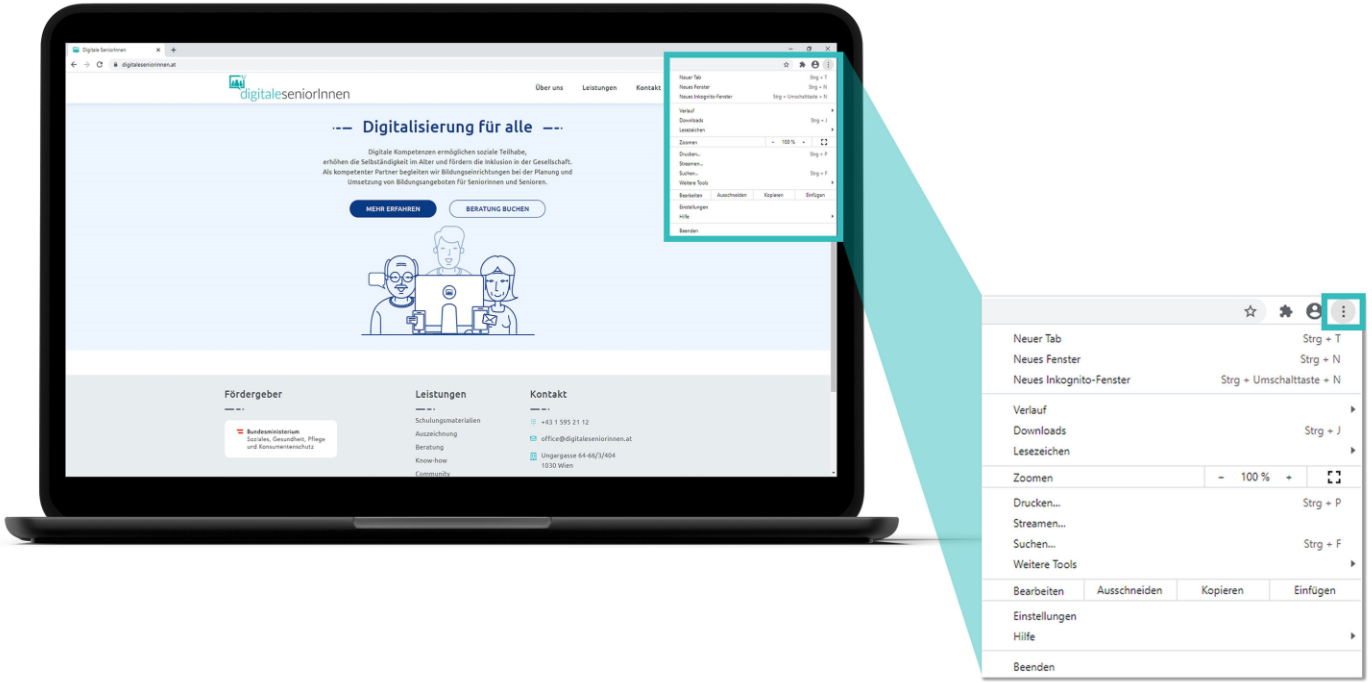
Quelle: pixabay.com

Phishing-Schutz einschalten

Chrome

Quelle: pixabay.com

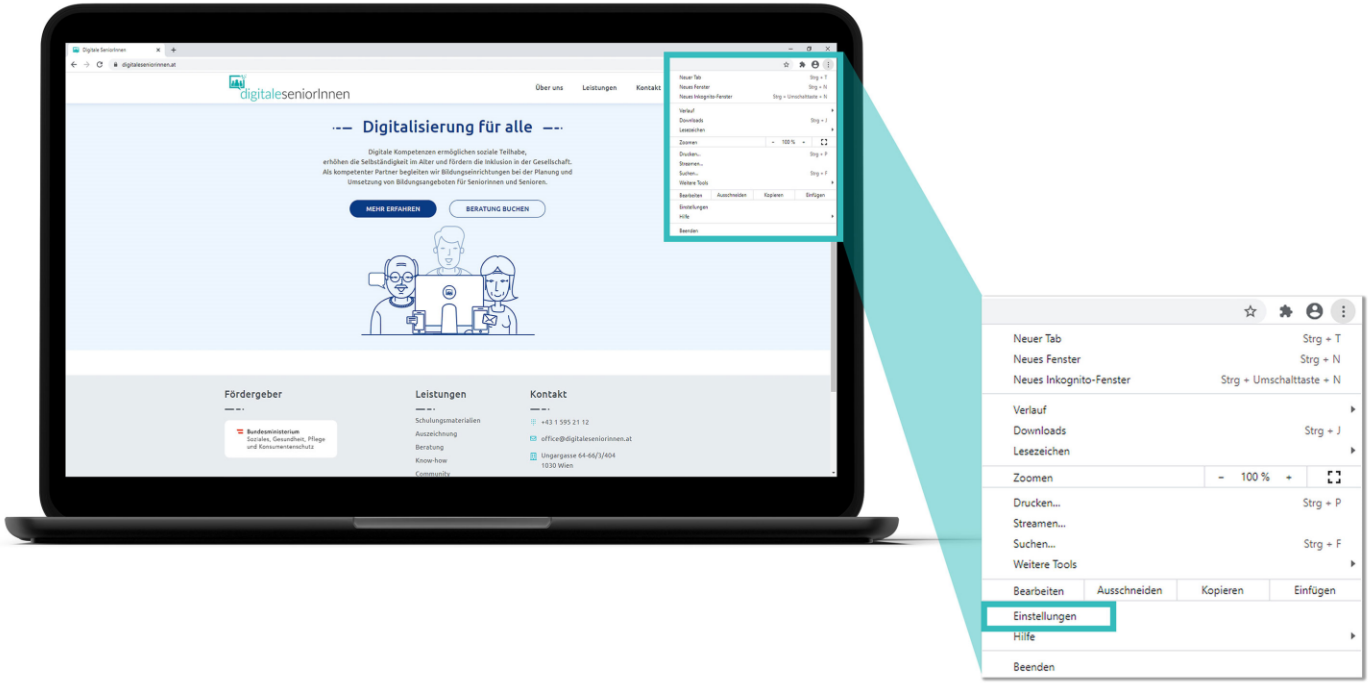
Schutz vor Phishing-Webseiten einschalten (Chrome)



Schritt 1:

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

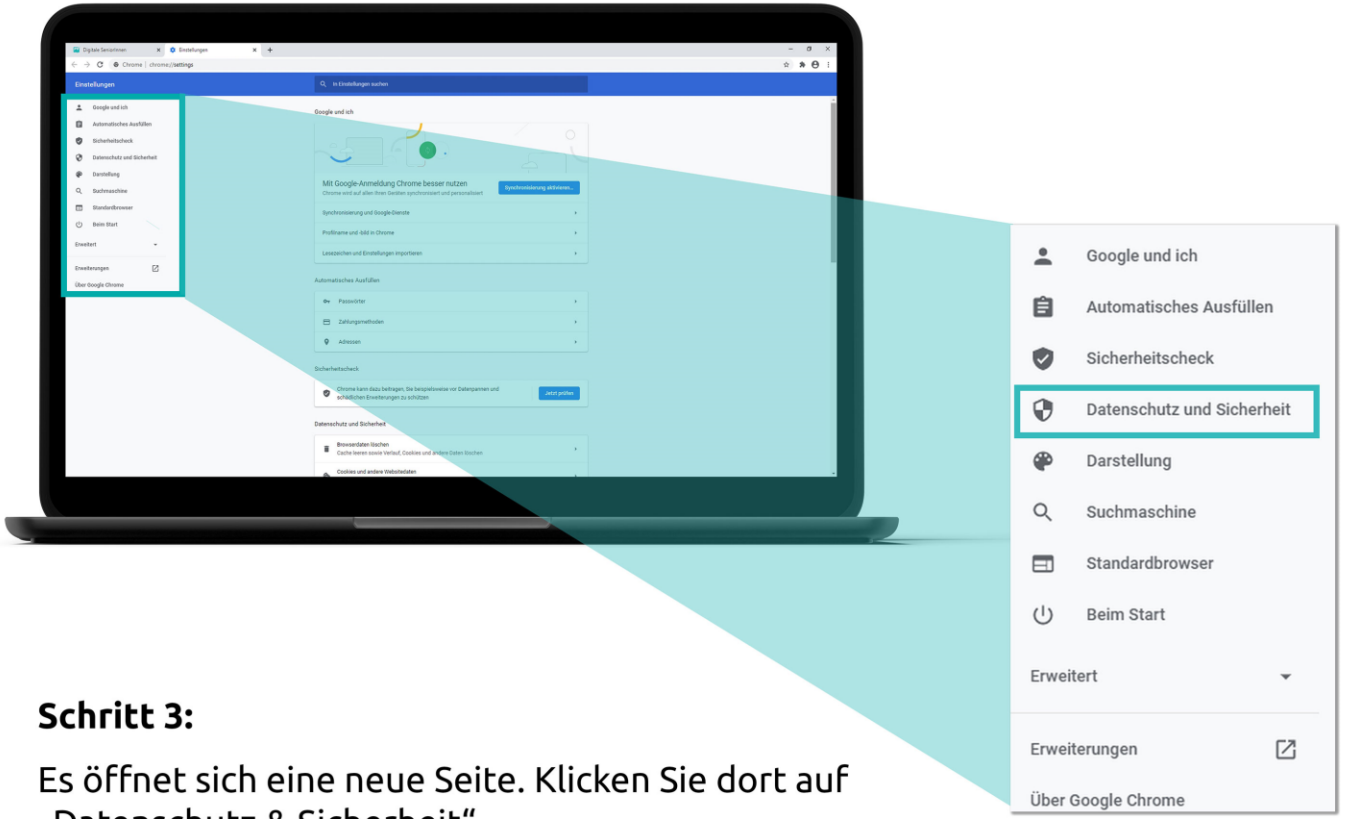
Schutz vor Phishing-Webseiten einschalten (Chrome)



Schritt 2:

Klicken Sie auf „Einstellungen“.

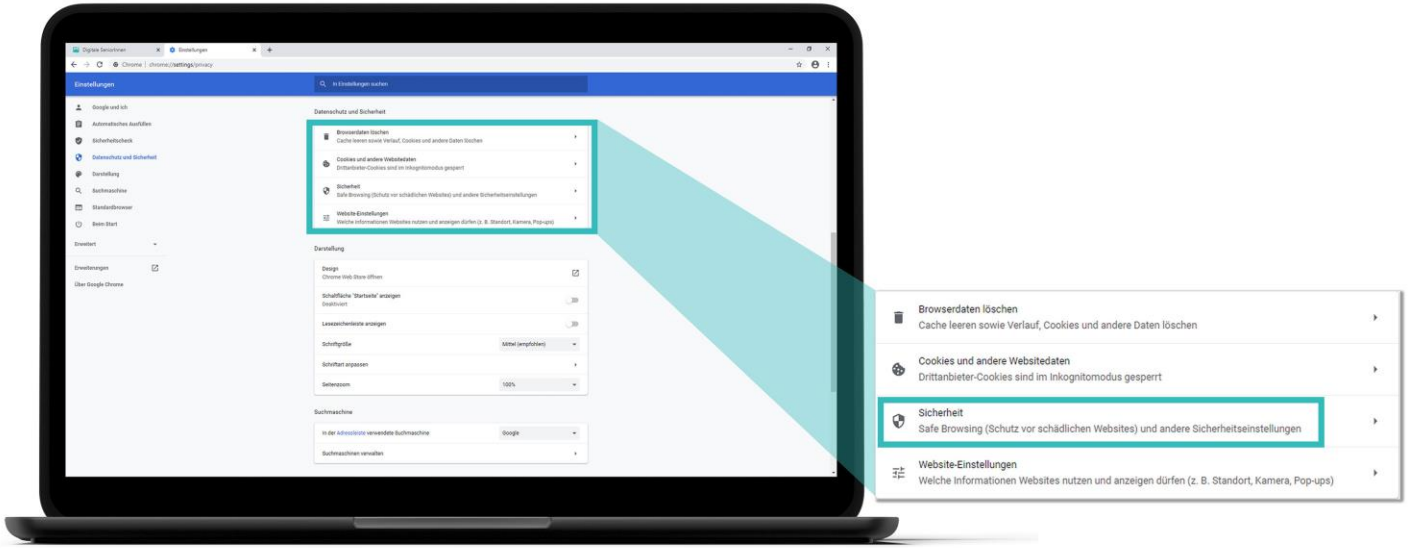
Schutz vor Phishing-Webseiten einschalten (Chrome)



Schritt 3:

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

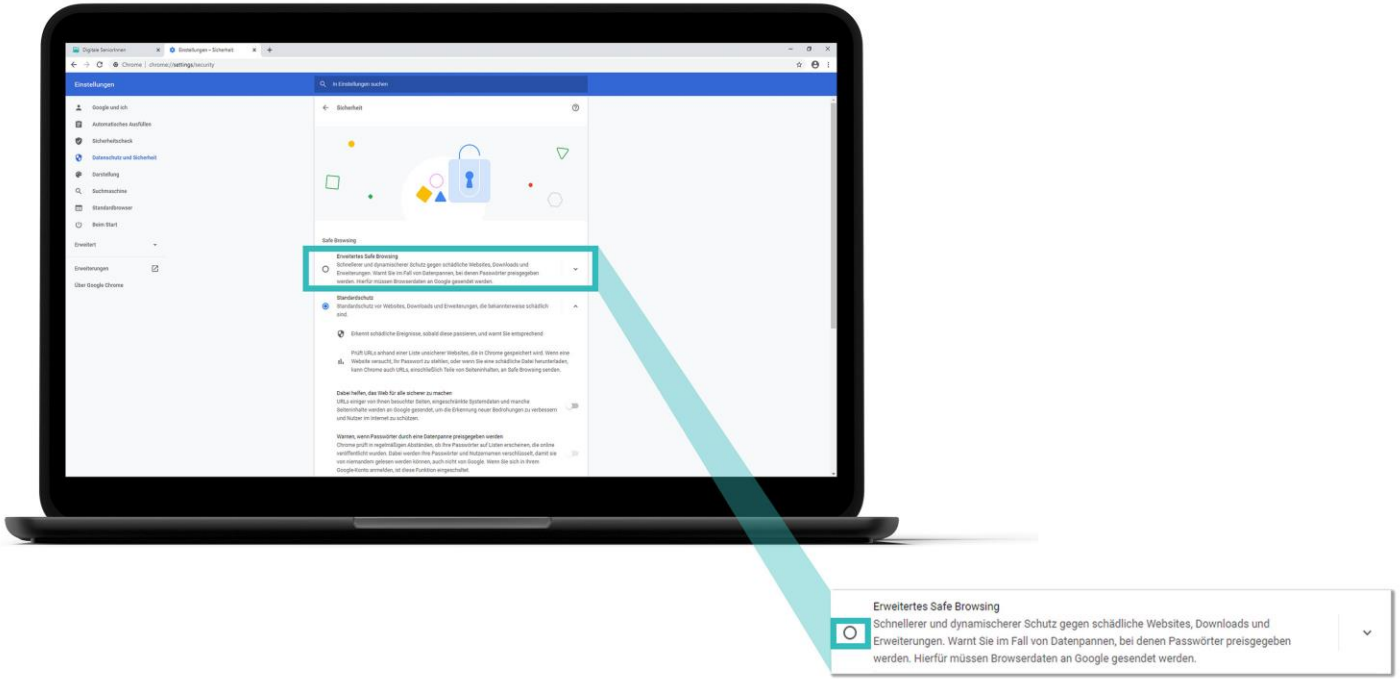
Schutz vor Phishing-Webseiten einschalten (Chrome)



Schritt 4:

Klicken Sie auf „Sicherheit“.

Schutz vor Phishing-Webseiten einschalten (Chrome)



Schritt 5:

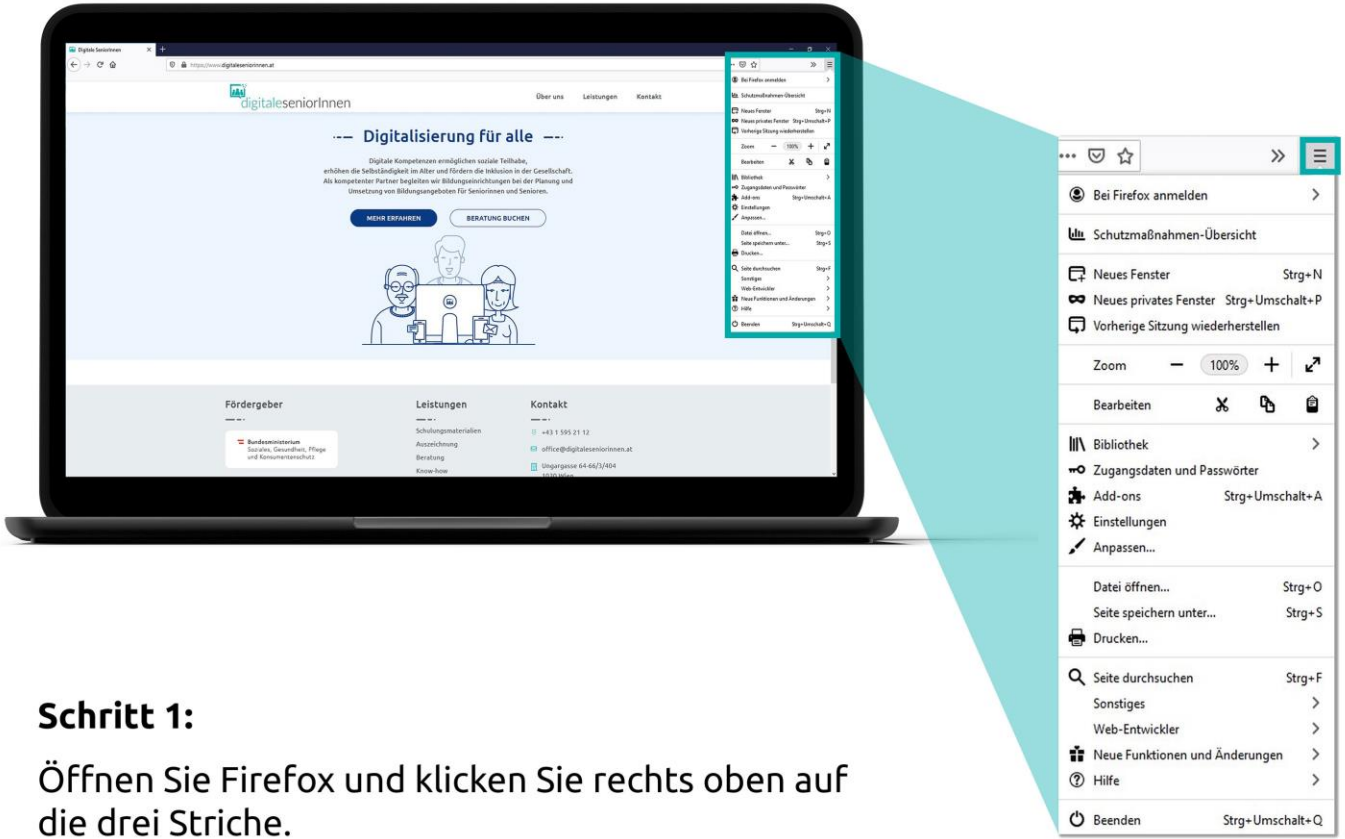
Klicken Sie auf „Erweitertes Safe Browsing“.

Phishing-Schutz einschalten

Firefox

Quelle: pixabay.com

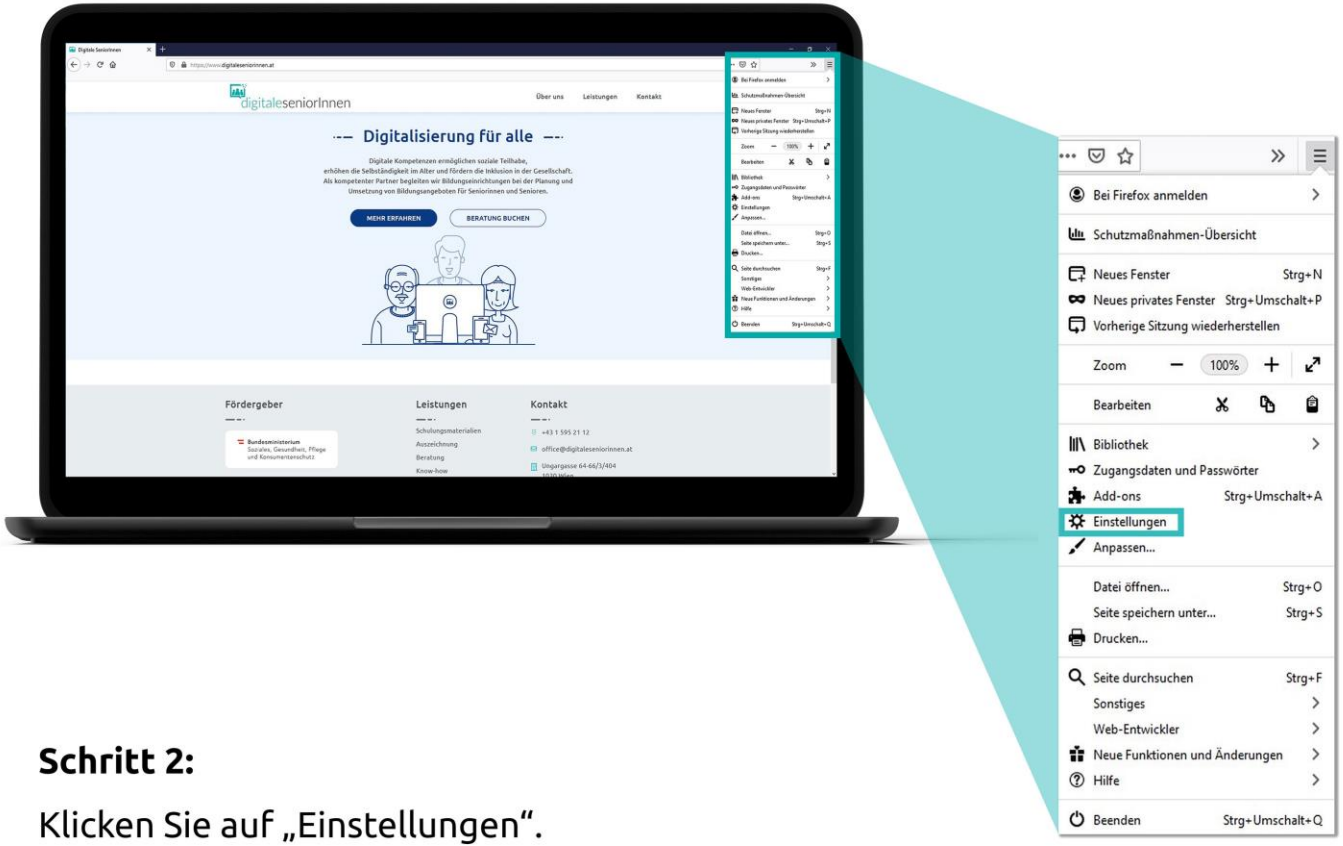
Schutz vor Phishing-Webseiten einschalten (Firefox)



Schritt 1:

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

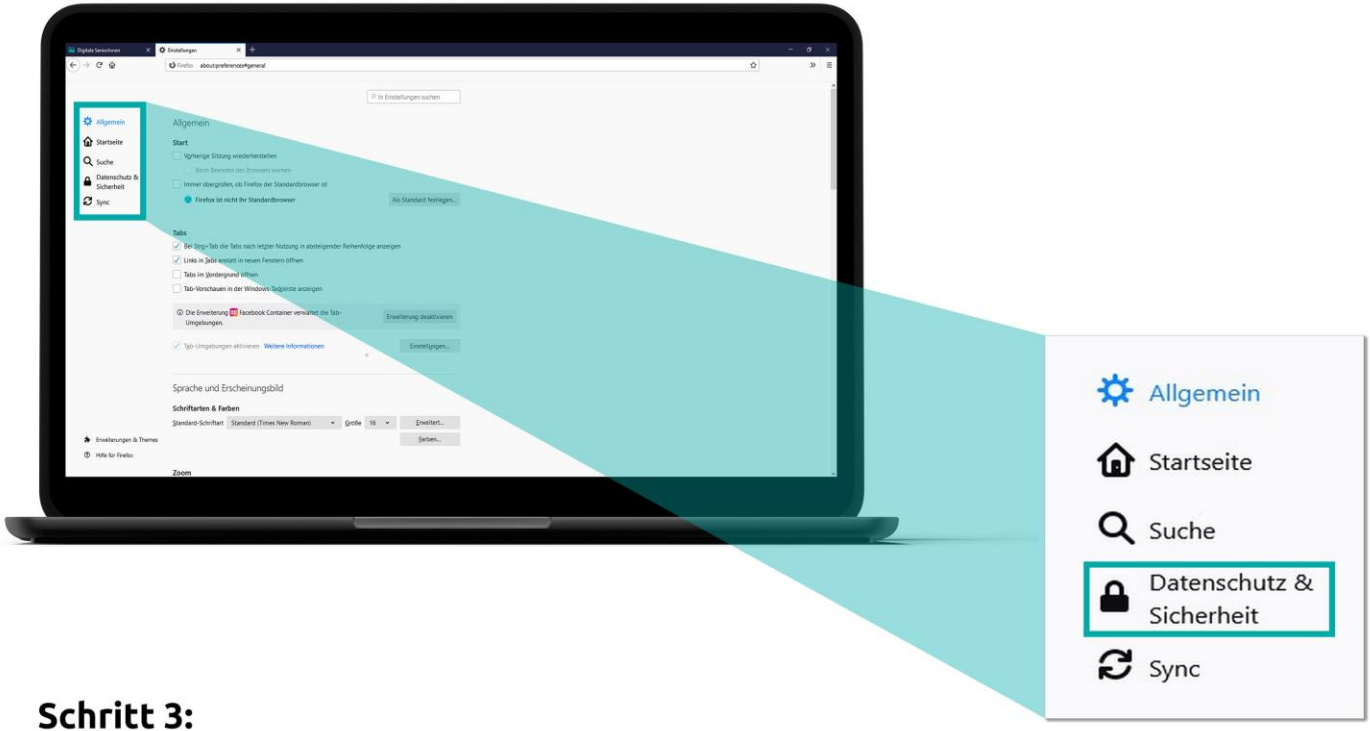
Schutz vor Phishing-Webseiten einschalten (Firefox)



Schritt 2:

Klicken Sie auf „Einstellungen“.

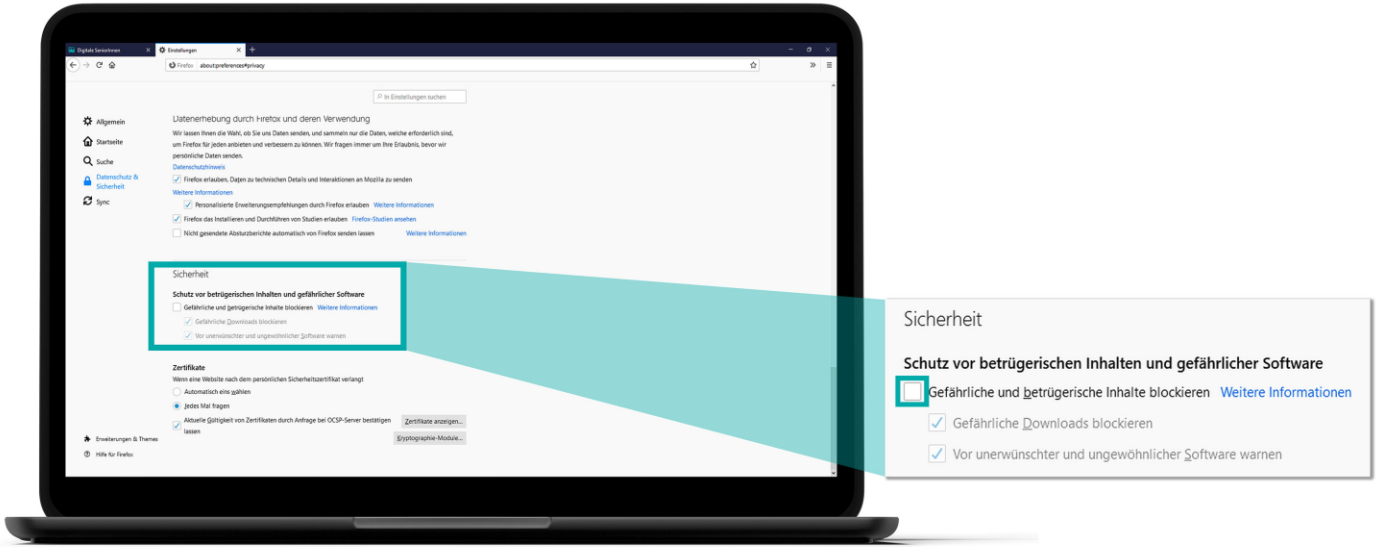
Schutz vor Phishing-Webseiten einschalten (Firefox)



Schritt 3:

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

Schutz vor Phishing-Webseiten einschalten (Firefox)



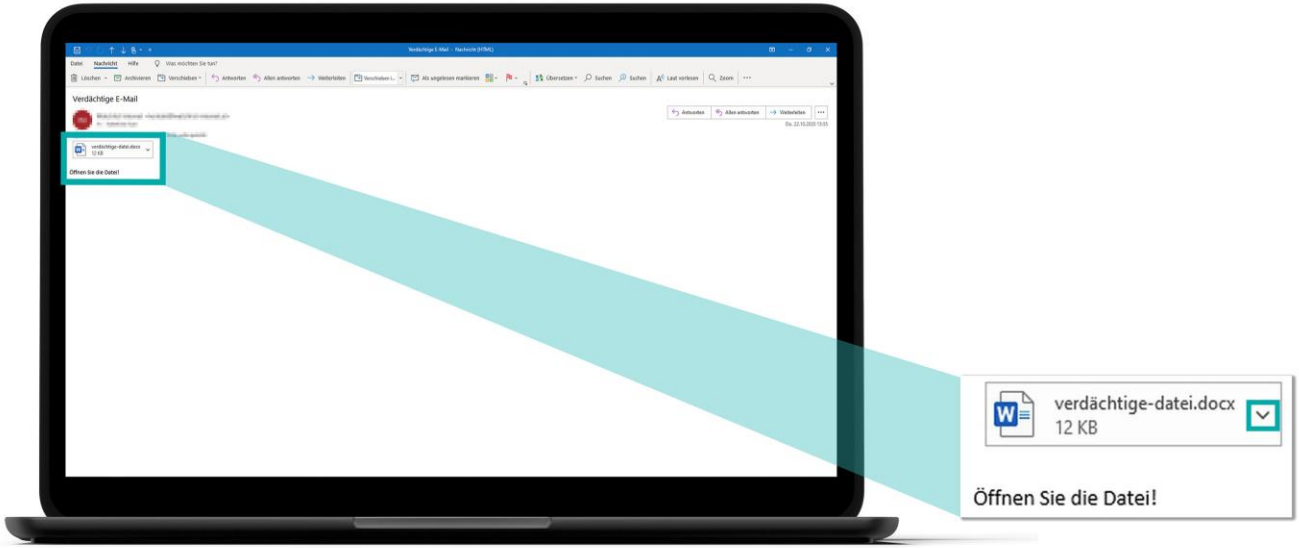
Schritt 4:

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

Dateien auf Viren überprüfen

Virustotal - https://www.virustotal.com

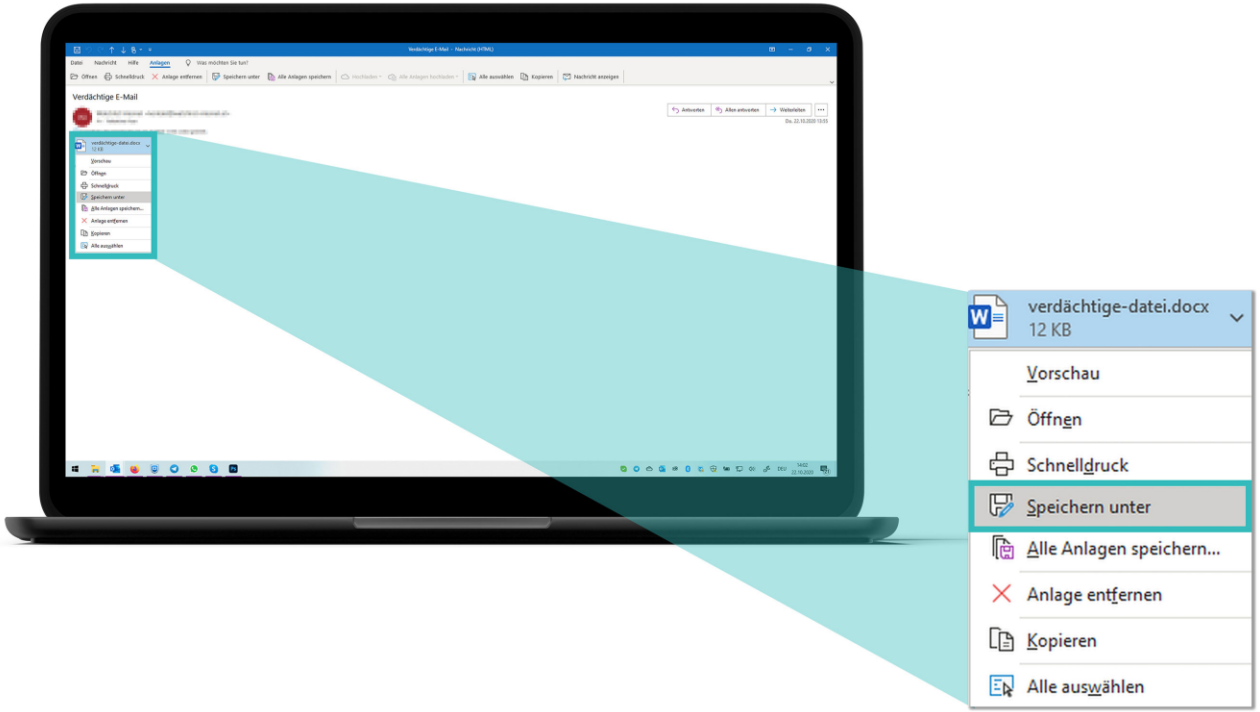
Überprüfung verdächtiger E-Mail-Anhänge



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!

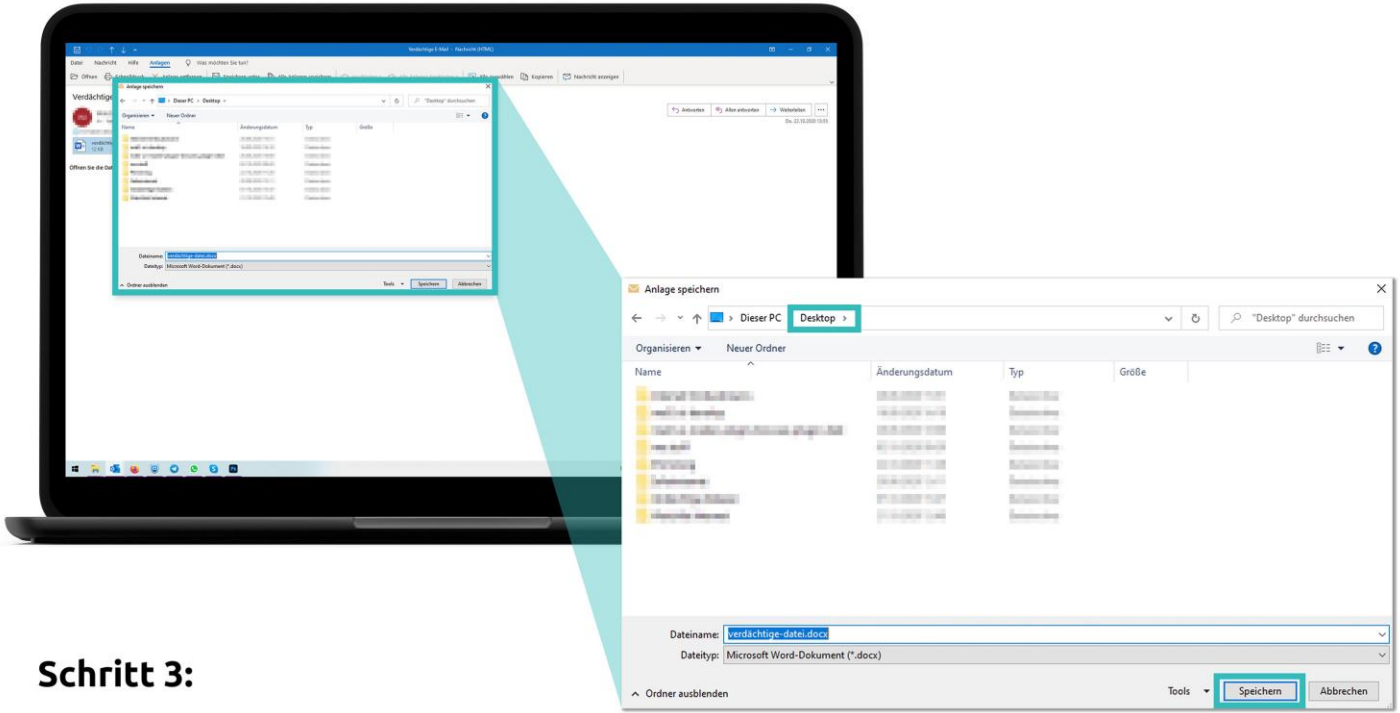
Überprüfung verdächtiger E-Mail-Anhänge



Schritt 2:

Klicken Sie auf „Speichern unter“.

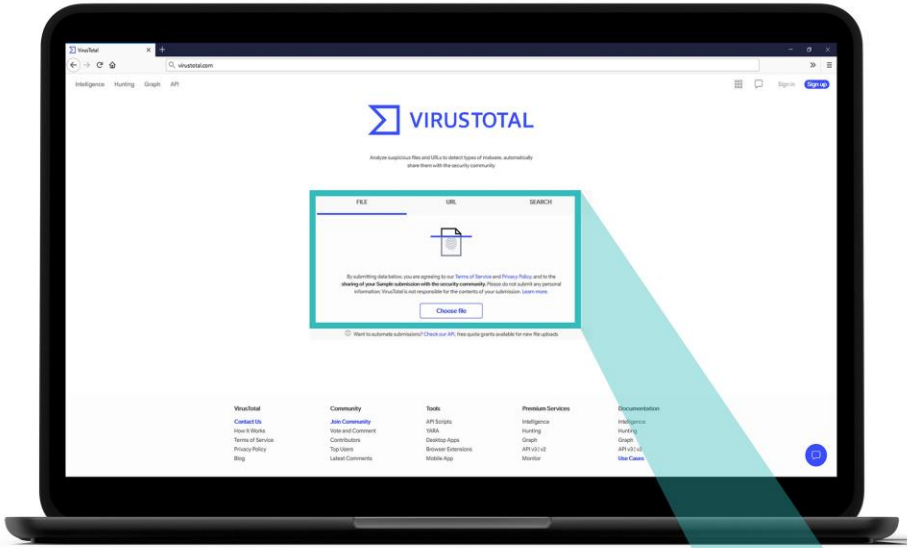
Überprüfung verdächtiger E-Mail-Anhänge

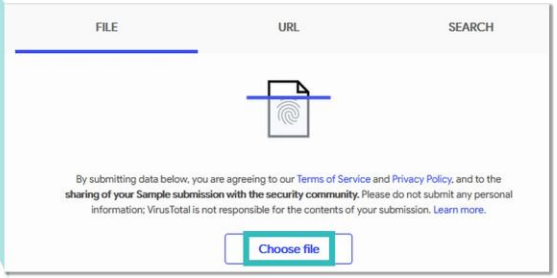


Schritt 3:

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

Überprüfung verdächtiger E-Mail-Anhänge

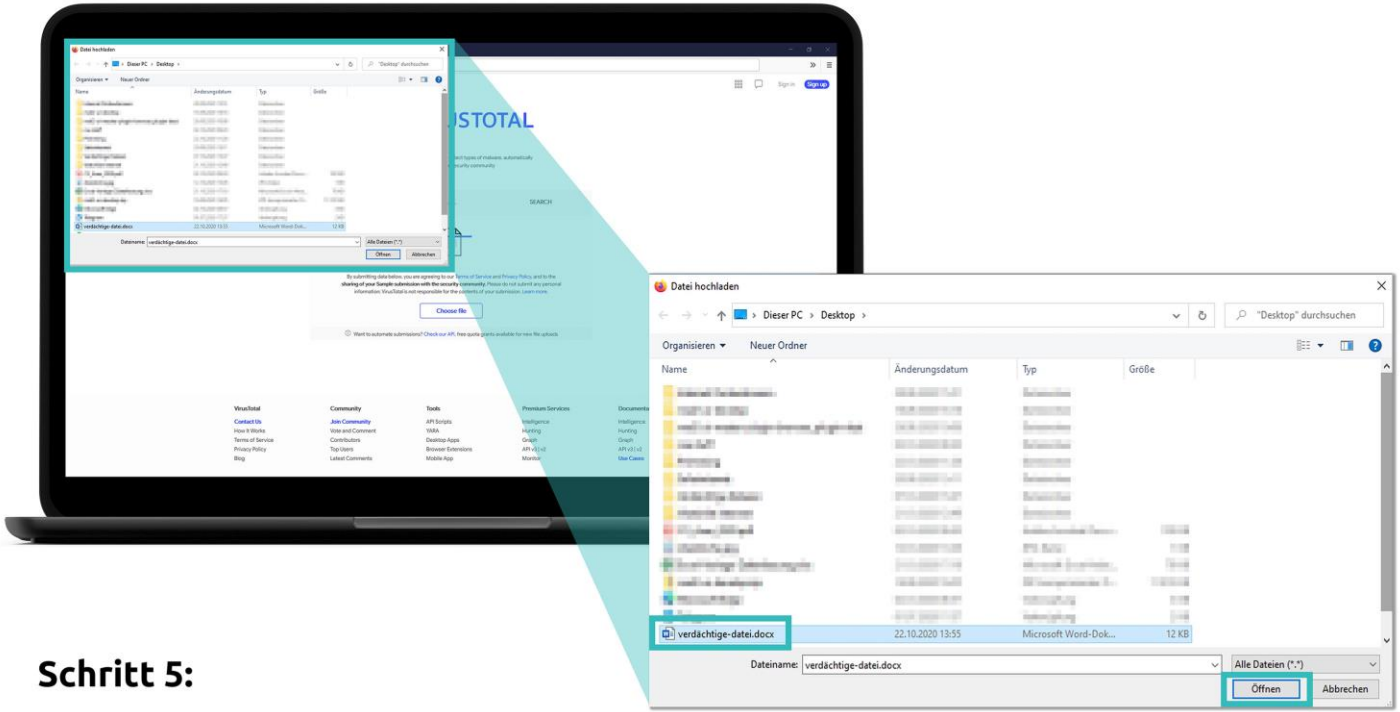




Schritt 4:

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

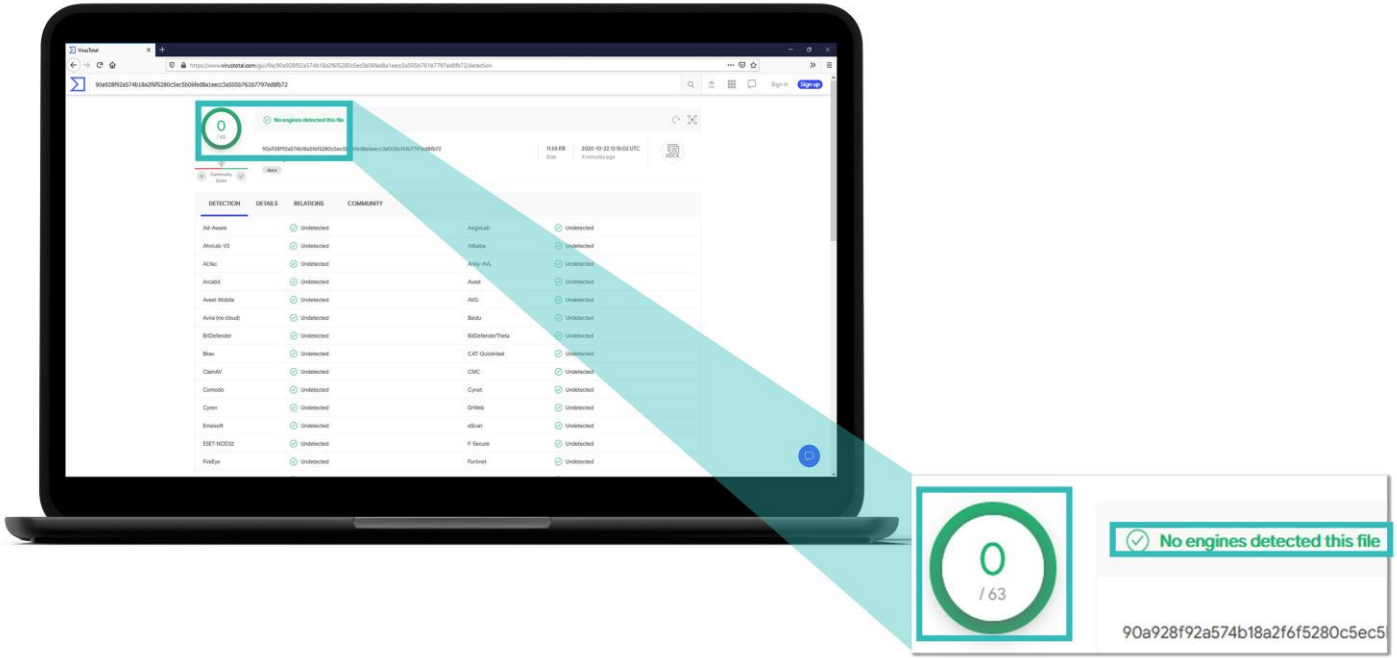
Überprüfung verdächtiger E-Mail-Anhänge



Schritt 5:

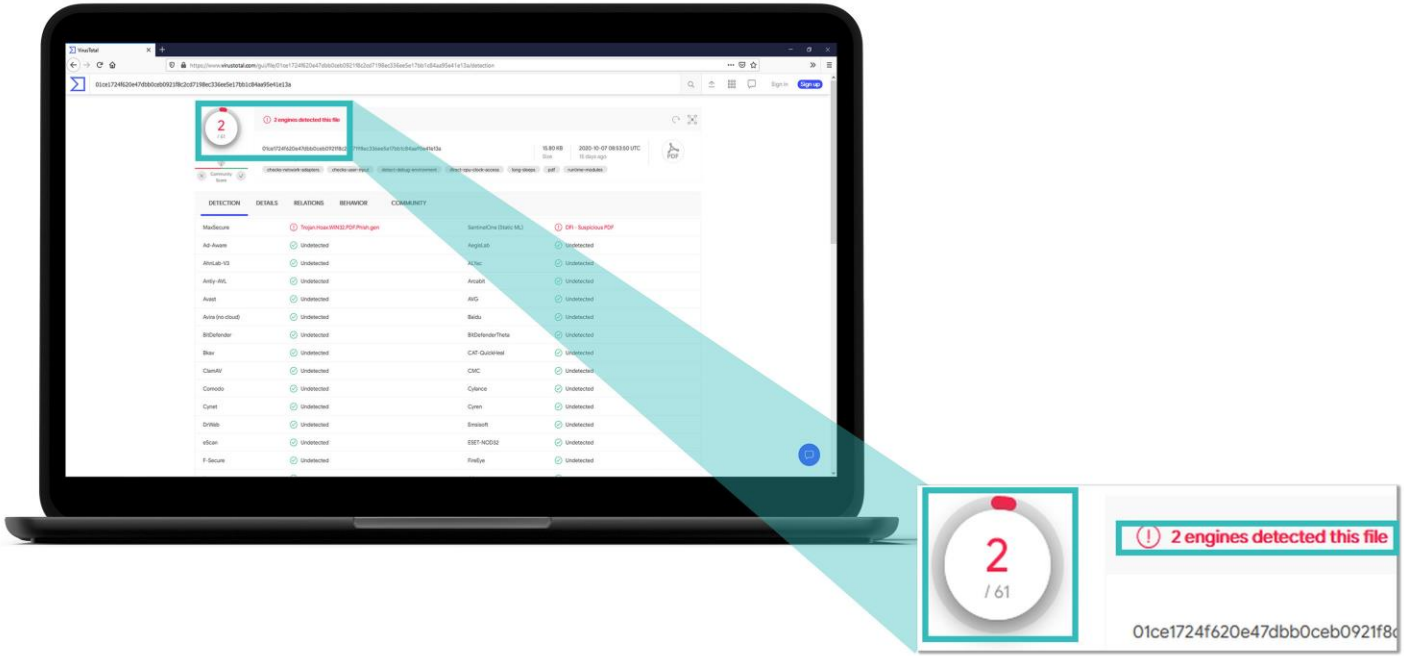
Es öffnet sich ein neues Fenster.
Klicken Sie auf die verdächtige Datei. Klicken Sie auf „Öffnen“.

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!