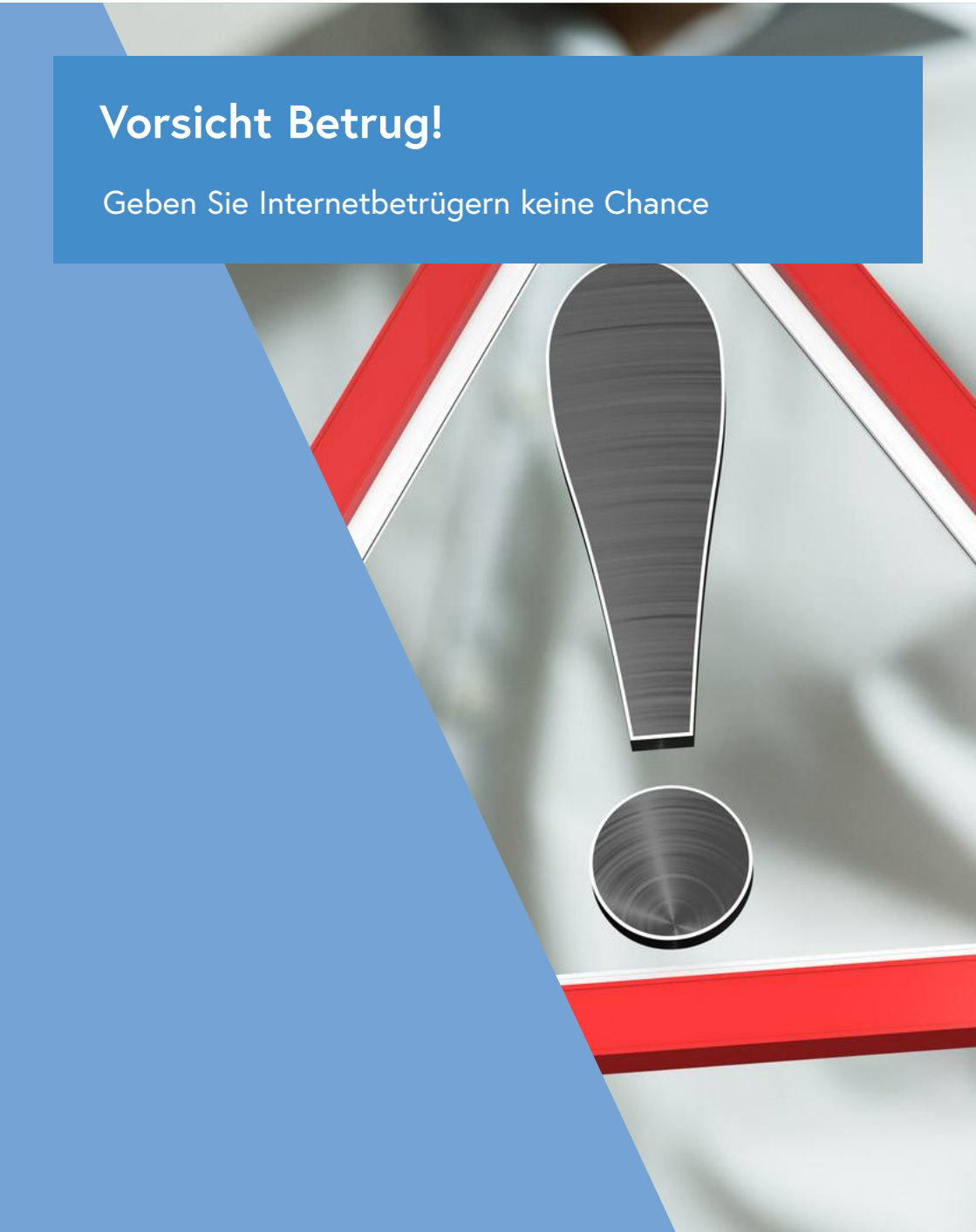
Bundesministerium
Finanzen

Vorsicht Betrug!

Geben Sie Internetbetrügern keine Chance



Impressum

Herausgeber, Eigentümer und Verleger: Bundesministerium für Finanzen
Abteilung GS/KO Öffentlichkeitsarbeit, Kommunikation und Protokoll
Johannesgasse 5, 1010 Wien
Für den Inhalt verantwortlich: BMF – Abteilung GS/PM
Grafik: Druckerei des Bundesministeriums für Finanzen
Fotos: BMF/citronenrot, BMF/Adobe Stock, BMF/Colourbox
Wien, Juli 2019

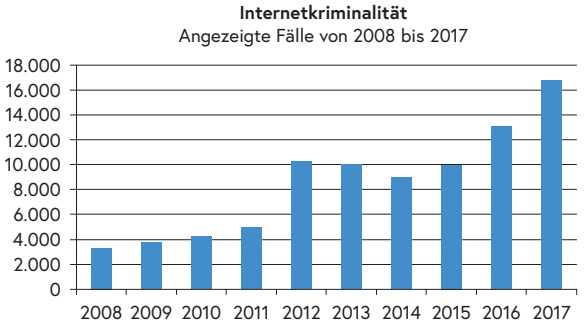
- gedruckt nach der Richtlinie „Druckerzeugnisse“ des Österreichischen Umweltzeichens, Druckerei des Bundesministeriums für Finanzen, UW-Nr. 836

Geben Sie Internetbetrügern keine Chance

Internetbetrüger bedienen sich immer häufiger ausgeklügelter Tricks, um an persönliche Daten ihrer Opfer zu gelangen und sich auf deren Kosten zu bereichern. Und ihre Methoden werden zunehmend professioneller.

Betrügerische E-Mails und Telefonanrufe im Namen von Bankinstituten, Mobilfunkprovidern, Paketzustellern, Behörden und Co sind mittlerweile auch in Österreich zur ‚Normalität‘ geworden. Um ihre Opfer zu täuschen, setzen Internetbetrüger fingierte E-Mails, Telefonanrufe, SMS, Webseiten und Dateianhänge ein. Ihr Ziel ist, ihren Opfern vertrauliche Daten zu entlocken, wie z. B. Bankkontoinformationen, Passwörter und TANs, oder sie gleich zur Überweisung von Geldbeträgen zu verleiten. Für die Betroffenen drohen dadurch finanzielle Schäden in der Höhe von mehreren Tausend Euro.

Aus der polizeilichen Kriminalstatistik des Innenministeriums geht hervor, dass sich die Zahl der angezeigten Fälle im Bereich der Internetkriminalität in den vergangenen zehn Jahren verachtfacht hat, Tendenz steigend.



Quelle: Polizeiliche Kriminalstatistik (Österreich (2017)

Betrugsmaschen im Namen der Finanz

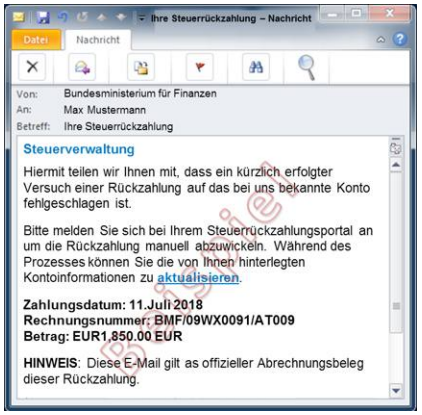
Auch das Bundesministerium für Finanzen (BMF) warnt regelmäßig vor Betrugsfällen, bei denen Bürgerinnen und Bürger gefälschte E-Mails im Namen des BMF sowie Anrufe von vermeintlichen Finanzamtsbediensteten erhalten.

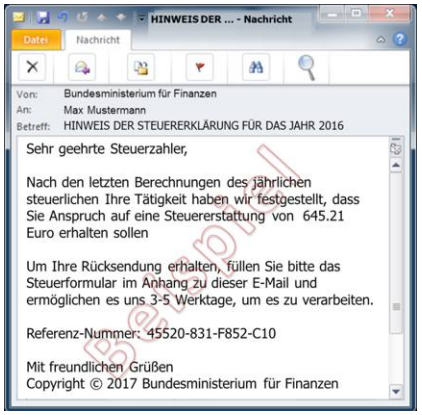
Die Masche mit den gefälschten E-Mails

Bei dieser Betrugsmasche versenden Internetbetrüger fingierte E-Mails an Bürgerinnen und Bürger, die unter anderem durch Fälschung der Absenderadresse den Eindruck eines offiziellen Schreibens des BMF erwecken sollen. Diese sogenannten Phishing-Mails fordern die Empfängerinnen und Empfänger auf, persönliche Daten bekannt zu geben bzw. zu aktualisieren, um eine Steuerrückzahlung zu erhalten oder Steuerschulden zu begleichen. Die Phishing-Mails enthalten dazu entweder einen Link, der auf eine gefälschte Webseite im Stil von FinanzOnline führt, oder einen Dateianhang in Form eines elektronischen Formulars.

Wichtige Klarstellung:
Das BMF fordert Bürgerinnen und Bürger niemals per E-Mail, Telefon oder SMS dazu auf, vertrauliche Daten bekannt zu geben oder Geldbeträge zu überweisen.

Phishing-Beispiel





Bitte beachten Sie, dass diese E-Mails und die darin enthaltenen Informationen Fälschungen darstellen und nicht durch das BMF versendet wurden. Gleiches gilt auch für derartige Telefonanrufe und SMS.

Wenn Sie daher per E-Mail aufgefordert werden, vertrauliche Daten bekannt zu geben oder Geldbeträge zu überweisen, handelt es sich mit hoher Wahrscheinlichkeit um einen Betrugsversuch.

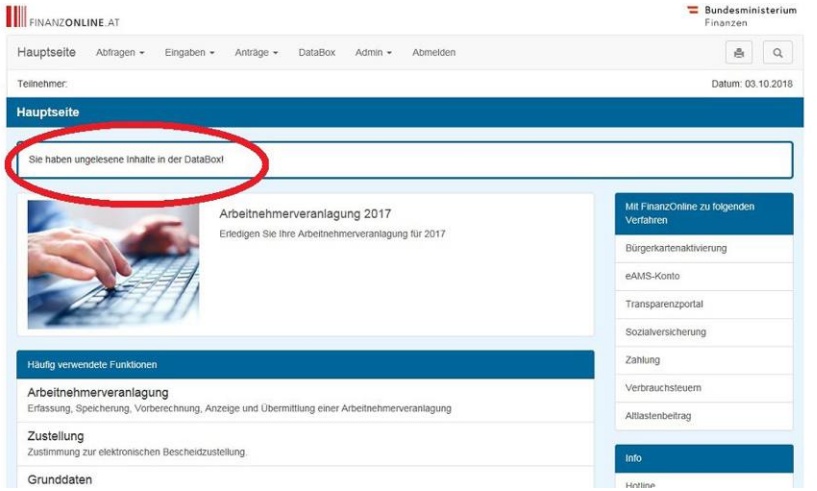
Die Masche mit den falschen Telefonanrufen

Bei dieser Form des Betrugs werden Bürgerinnen und Bürger durch Internetbetrüger telefonisch kontaktiert. Die Internetbetrüger geben sich dabei als Finanzamtsbedienstete aus und fordern ihr Gegenüber unter dem Vorwand einer angeblichen Steuerschuld oder Pfändung auf, eine Geldüberweisung durchzuführen. Damit der Anruf einen offiziellen Charakter erhält, nutzen sie einen technischen Trick, der als sogenanntes Call ID Spoofing bekannt ist. Dadurch kann am Display der angerufenen Telefone eine beliebige Nummer angezeigt werden. Im konkreten Fall verwenden die Internetbetrüger die Telefonnummer der österreichischen Finanzämter (050 233 233).

Betrugsversuche einfach erkennen

Zur Erinnerung das Wichtigste noch einmal: Das BMF fordert Bürgerinnen und Bürger niemals per E-Mail, Telefon oder SMS dazu auf, vertrauliche Daten bekannt zu geben oder Geldbeträge zu überweisen.

Informationen des BMF erfolgen grundsätzlich in Form von Bescheiden und werden per Post oder in die FinanzOnline Databox zugestellt.

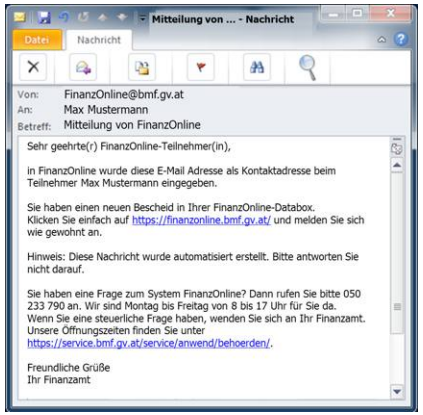


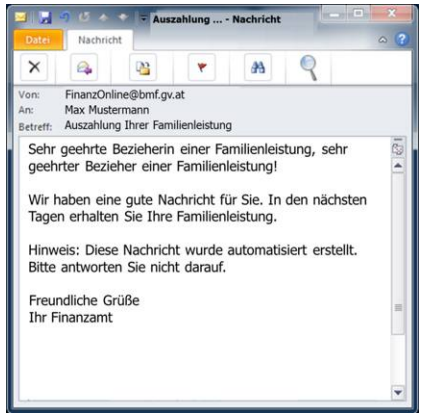
Wenn Sie vom BMF E-Mails erhalten, dann handelt es sich um Statusinformationen, z. B.

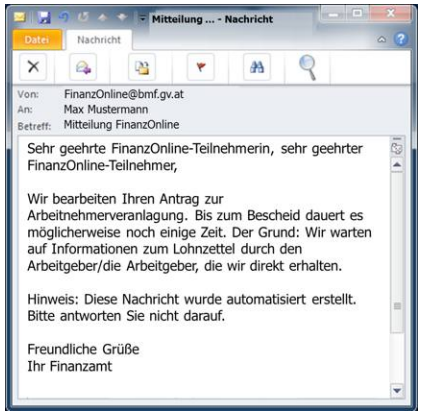
- zu Ihrer Arbeitnehmerveranlagung,
- zur Auszahlung der Familienbeihilfe oder
- zu Databoxzustellungen.

Solche Nachrichten erhalten Sie aber nur dann, wenn Sie Ihre E-Mail-Adresse in FinanzOnline hinterlegt und dieser Form der Kontaktaufnahme ausdrücklich zugestimmt haben.

Beispiele für E-Mails vom BMF







Betrugsversuche Hintergründe und Merkmale

Gefälschte E-Mails, Webseiten und elektronische Formulare können mittlerweile täuschend echt wirken. Auch Absenderadressen und Telefonnummern lassen sich mittlerweile einfach fälschen.

Dass Internetbetrüger gefälschte E-Mails versenden und dabei Absenderadressen bekannter E-Mail-Domänen von Unternehmen und Behörden fälschen, ist technisch machbar. Leider kann dies durch die Inhaberinnen und Inhaber der betroffenen E-Mail-Domänen mit technischen Mitteln nicht verhindert werden. Gleiches gilt auch für fingierte Telefonanrufe und das Fälschen der angezeigten Telefonnummer.

Das Wichtigste für die effektive Erkennung von Betrugsversuchen sind deshalb eine generelle Achtsamkeit und eine gesunde Portion Skepsis. Typische Erkennungsmerkmale von Phishing-Mails sind beispielsweise:

- Gefälschte Absenderadresse
- Unpersönliche oder gänzlich fehlende Anrede
- Vorgetäuschter dringender Handlungsbedarf mit verlockenden oder bedrohlichen Begründungen
- Aufforderung zum Aufruf von Links oder Dateianhängen und zur Bekanntgabe vertraulicher Daten oder zur Überweisung von Geldbeträgen
- Rechtschreib- und Grammatikfehler im E-Mail-Text

Besuchen Sie im Zweifelsfall unsere Homepage unter www.bmf.gv.at und erkundigen Sie sich, ob bereits aktuelle Sicherheitswarnungen existieren.

Sicherheitsmaßnahmen beim Umgang mit E-Mails

Neben obligatorischen Sicherheitsmaßnahmen für PCs, Tablets und Smartphones sollten Sie beim Umgang mit E-Mails und Webseiten zu Ihrer eigenen Sicherheit immer folgende Maßnahmen berücksichtigen:

Prüfung der Internetadresse

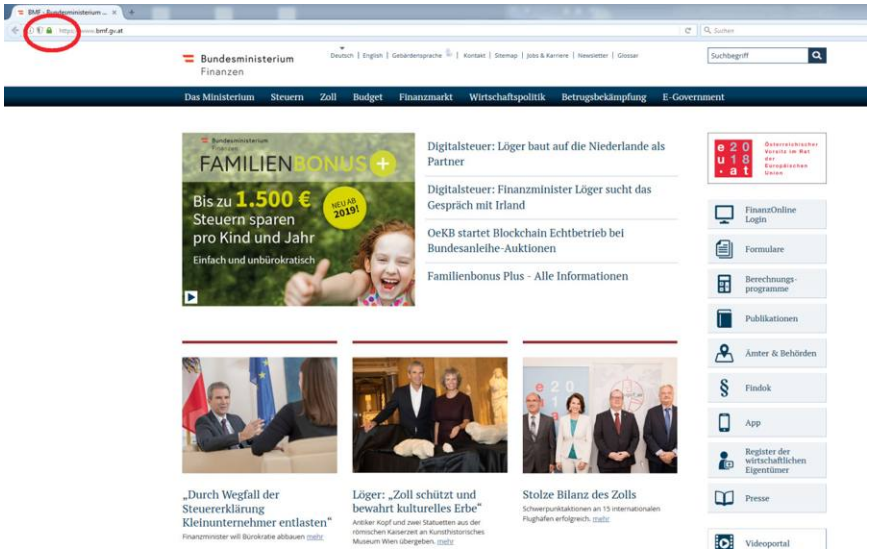
- Bevor Sie auf einen Link in einer E-Mail klicken, sollten Sie zuvor immer die tatsächliche Internetadresse prüfen, auf die der Link verweist. Diese wird in den meisten E-Mail-Programmen angezeigt, sobald Sie den Mauszeiger über den Link ziehen.

- Die Internetadresse von FinanzOnline beginnt immer mit: https://finanzonline.bmf.gv.at/.

Prüfung des SSL-Zertifikats

- Bevor Sie auf einer Webseite vertrauliche Daten eingeben, sollten Sie zuvor immer prüfen, ob diese über ein SSL-Zertifikat verfügt, das eine gesicherte Internetverbindung zwischen Webserver und Browser sicherstellt. Sie erkennen das am „https“ am Beginn der Internetadresse sowie am Schlosssymbol in der Adresszeile Ihres Browsers. Über dieses Symbol können Sie auch prüfen, auf wen das Zertifikat ausgestellt ist.

- Bei FinanzOnline ist das SSL-Zertifikat auf das Bundesministerium für Finanzen ausgestellt.



Wichtige Sicherheitsmaßnahmen
für PCs, Tablets und Smartphones sind z. B. Sicherheitsupdates, Virenschutzprogramme sowie Phishing- und Virenschutz-Sicherheitseinstellungen im Browser.

Sicherheitsstandards Ihres E-Mail-Providers

Internetbetrüger versenden Phishing-Mails in der Regel mittels gekaperter E-Mail-Accounts und Mailservern aus der ganzen Welt. Deshalb unterstützen sämtliche Mailserver des BMF modernste Sicherheitsstandards.

Dank dieser Sicherheitsstandards ist es E-Mail-Providern möglich, bereits beim Empfang von E-Mails zu überprüfen, ob diese tatsächlich von einem autorisierten Mailserver des BMF versendet wurden oder ob es sich um Fälschungen handelt. Für die E-Mail-Domäne bmf.gv.at sind die autorisierten Mailserver eindeutig festgelegt.

E-Mail-Provider, die diese Sicherheitsstandards unterstützen, können dadurch einlangende Phishing-Mails automatisch erkennen, blockieren und somit verhindern, dass diese überhaupt in Ihr persönliches E-Mail-Postfach gelangen.

Achten Sie daher bei der Wahl ihrer E-Mail-Provider verstärkt auf die Unterstützung von Sicherheitsstandards zur automatischen Erkennung und Blockierung von Phishing-Mails. Erkundigen Sie sich bei Ihrer Anbieterin bzw. Ihrem Anbieter, ob und welche Standards unterstützt werden.

Wichtige Sicherheitsstandards sind z. B.:

- SPF – **S**ender **P**olicy **F**ramework
- DKIM – **D**omain **K**eys **I**dentified **M**ail
- DMARC – **D**omain-based **M**essage **A**uthentication **R**eporting & **C**onformance

Auf Betrugsversuche richtig reagieren

Wenn Sie einen Betrugsversuch als solchen entlarvt haben, sollten Sie richtig reagieren:

- Folgen Sie in keinem Fall den Anweisungen der Internetbetrüger!
- Geben Sie unter keinen Umständen vertrauliche Daten wie Bankkontoinformationen, Passwörter und TANs bekannt und überweisen Sie keine Geldbeträge!
- Bedenken Sie die Gefahr einer Schadsoftware-Infektion und klicken Sie in Phishing-Mails keinesfalls auf enthaltene Links oder Dateianhänge, sondern löschen Sie diese am besten sofort!

Im Ernstfall umgehend handeln

Wenn Sie trotz aller Vorsichtsmaßnahmen in die Falle getappt sind und Ihre vertraulichen Daten bekannt gegeben oder Geldbeträge überwiesen haben, handeln Sie sofort:

- Melden Sie den Vorfall Ihrem Bankinstitut und besprechen Sie mit Ihrer Kundenbetreuerin bzw. Ihrem Kundenbetreuer die notwendigen Maßnahmen, um einen finanziellen Schaden zu vermeiden!
- Sollte es bereits zu unbefugten Zugriffen oder Überweisungen gekommen sein, sollten Sie jedenfalls bei einer Polizeidienststelle Strafanzeige erstatten!
- Wenn Sie eine verlinkte Webseite oder einen enthaltenen Dateianhang geöffnet haben, sollten Sie Ihren PC, Ihr Tablet oder Smartphone auf Schadsoftware überprüfen!

Das BMF arbeitet bei Auftreten neuer Betrugsfälle eng mit den Sicherheitsbehörden zusammen und leitet alle maßgeblichen Informationen zu neuen Betrugsmethoden an diese Stellen weiter. Für das polizeiliche Ermittlungsverfahren sind die jeweils zuständigen Polizeidienststellen und Landeskriminalämter bzw. das Bundeskriminalamt zuständig.

Weitere Informationen

Weiterführende Informationen zum Thema Internetbetrug, wie z. B. aktuelle Warnungen, Phishing-Beispiele und Sicherheitstipps, finden Sie darüber hinaus auf den folgenden Webseiten:

- **Bundeskriminalamt**
  https://bundeskriminalamt.at

- **Watchlist Internet**
  https://www.watchlist-internet.at

- **Saferinternet.at**
  https://www.saferinternet.at

- **Onlinesicherheit.gv.at**
  https://www.onlinesicherheit.gv.at