# So geht's leichter...

# Stoppt Phishing & Passwortklau

- So funktioniert Phishing
- Phishingangriffe vermeiden
- Ransomware abwehren
- Richtig mit Passwörtern umgehen
- Zwei Faktor Authentifizierung

Jörg Schieb

Autoren:
Jörg Schieb
Andreas Erle

**Impressum:**
**Redaktion schieb.de**
**Humboldtstr. 10**
**40667 Meerbusch**
**Kontakt: fragen@schieb.de**
**www.schieb.de**

# So geht's leichter | Stoppt Phishing und Passwortklau

## Inhalt

# So geht's leichter | Stoppt Phishing und Passwortklau

# So geht’s leichter | Stoppt Phishing und Passwortklau

Der Tag hat 24 Stunden (empfunden manchmal auch mehr), und ohne Unterbrechung bekommt Ihr eine E-Mail nach der anderen. Oft so viele, dass Ihr kaum noch in Ruhe lesen könnt. Und dann sticht eine E-Mail aus den anderen hervor: Euer Amazon-Konto ist kompromittiert, Eure Online-Banking-Zugang wurde missbraucht. Kurz: Vermeintlich greift jemand auf Eure Konten zu und richtet Schaden an.

Die erste Reaktion: Schnell reagieren, auf den Link klicken und das Problem lösen, bevor allzu viel passiert ist. Nur: Die allermeisten dieser E-Mails sind nicht echt, sondern zielen darauf, Eure Zugangsdaten abzugreifen.

Erst dann kommen die Angreifer an Eure Daten und können damit Schaden anrichten: Der klassische Phishing-Angriff.

Wie zeigen Euch, wie Ihr Phishing E-Mails erkennt und richtig darauf reagiert. Auch eine Phishing-E-Mail kann es schnell passieren, dass Ihr versehentlich Eure Benutzerdaten auf einer gefälschten Webseite

# So geht’s leichter | Stoppt Phishing und Passwortklau

eingebt: Tolle Angebote auf Facebook, Twitter und anderen Webseiten gaukeln Euch vor, dass Ihr ein tolles Produkt für einen verlockend niedrigen Preis bekommt. Ihr zahlt vermeintlich über PayPal oder einen anderen Zahlungsdienstleister, aber in Wirklichkeit handelt es sich um eine Fake-Seite, die Eure echten Zugangsdaten abgreift. Wiz zeigen Euch, wie Ihr solche Seiten erkennen könnt.

Auch Eure Passwörter an sich können Unbefugten Zugang zu Euren Daten verschaffen. Dann nämlich, wenn sie zu einfach sind oder bereits bei einem Datenleck abgeflossen sind und im Internet verfügbar sind. Wir zeigen Euch, wie Ihr Eure Passwortsicherheit erhöhen könnt.

## Phishingangriffe vermeiden

Viele Anwender glauben immer noch, dass das größte Risiko für die Sicherheit ihrer Daten ein Virenscanner ist. Auch wenn Malware immer noch ein Thema ist, so ist in den vergangenen Jahren der Fokus der Angreifer mehr dahin gegangen, Eure Zugangsdaten zu bekommen und so auf E-Mails, Benutzerkonten und Webseiten zuzugreifen. Das verlagert die Verantwortung leider von einem automatischen System wie einem Virenscanner auf Eurem Rechner auf Euch und Eure Fähigkeit, Angriffe zu erkennen.

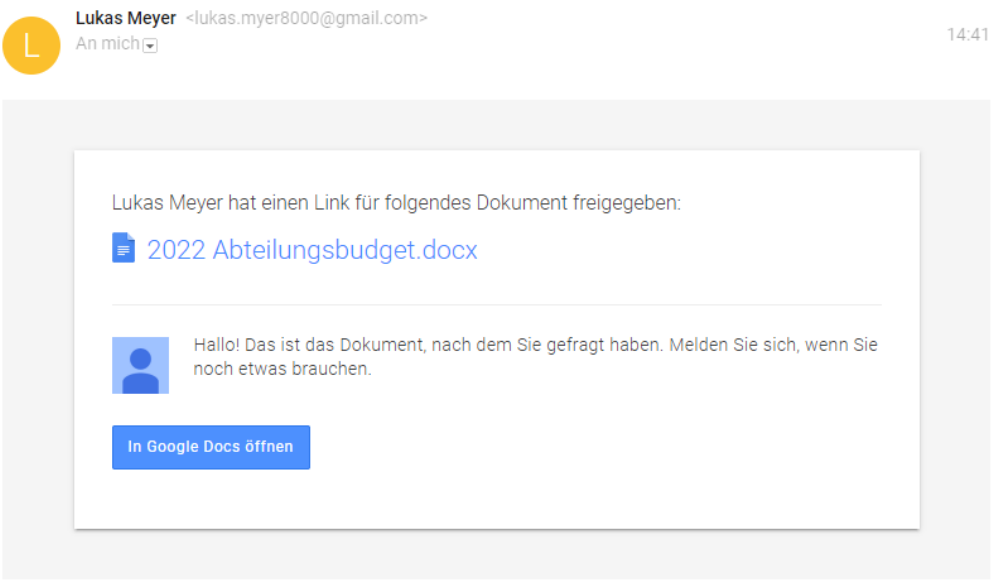
Ein Virenscanner prüft Codemuster in den Dateien gegen eine Liste bekannter Viren und warnt, wenn er eine (vermeintlich) infizierte Datei findet.

Wofür es aber  keine App gibt, das ist das natürliche Vertrauen darauf, dass eine Mail von Apple oder Amazon oder ein Anruf von Microsoft schon echt sein werden. Das ist leider aber nicht immer der Fall!

# So geht’s leichter | Stoppt Phishing und Passwortklau

## Der wichtige Link/Anhang in einer E-Mail

Ihr seid von Natur aus neugierig. Sobald eine E-Mail einen Anhang hat, dann wollt Ihr auch wissen, was darin ist. Je interessanter die E-Mail klingt, je drängender ihr Ton, desto größer wird der Reiz.




Das wissen auch die Angreifer. Eine interessante E-Mail mit einem Anhang schafft es durch die meisten Schutzsysteme der Mail-Server, denn im Normalfall handelt es sich um Dokumente, in denen wieder Links versteckt sind, die Euch dann auf die Seiten der Angreifer führen. Oder der Anhang ist – wie im Beispiel – keine echte Datei, sondern nur ein Link zu einer Webseite.

**So schützt Ihr Euch:**

- Überprüft, ob Ihr den Absender der E-Mail kennt. Bei vielen Phishing-Mails sind der Absendername und die Absender-E-Mail-Adresse nicht konsequent: Lukas Meyer und lukas.myer8000@gmail.com sind schon auffällig.

# So geht's leichter | Stoppt Phishing und Passwortklau

- Bewegt Eure Maus über die Links in der E-Mail, bevor Ihr darauf klickt. Der Browser oder das E-Mail-Programm zeigen Euch dann die tatsächliche URL an. Schaut genau hin: Oft sind die Bezeichnungen „so ähnlich" wie bei einem echten Cloud-Dienst, aber eben nur ähnlich.

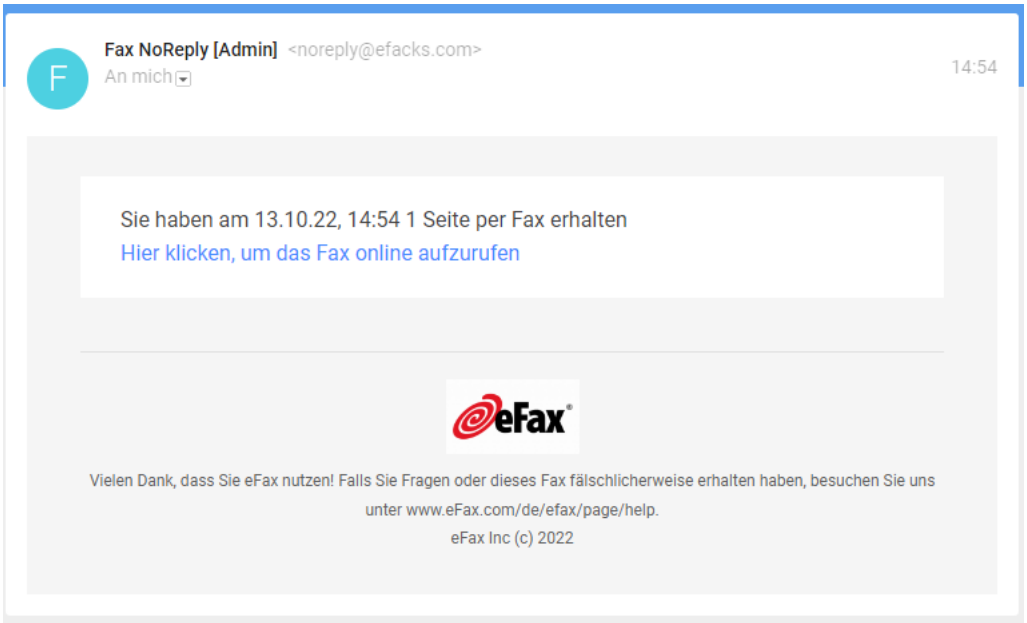

- Im Beispiel ist die URL drive—google.com, Ihr sollt denken, dass es sich um Google Drive handelt. Der Cloudspeicher hat aber die URL drive.google.com. Ein Klick auf den falschen Link führt Euch auf eine täuschend echte Google-Anmeldungsseite. Merkt Ihr das nicht, sind Eure Google-Anmeldedaten kompromittiert.

## Die Nachricht aus dem Internet

Fax, MMS, SMS: Nachrichten-Dienste, die viele von uns noch kennen, die aber schon lange an Gewicht verloren haben. Wer von Euch hat noch ein Faxgerät und nutzt es regelmäßig? Um kompatibel zu bleiben, benutzen tatsächlich viele Anwender Webdienste dafür, beispielsweise den Dienst eFax.

Wenn Ihr dann von einem solchen Dienst eine E-Mail bekommt, dass ein Fax eingegangen sei, dann liegt auch hier wieder nah, auf den Link zu klicken, schließlich kommen per Fax nur wichtige Informationen.

# So geht’s leichter | Stoppt Phishing und Passwortklau




Schaut Euch solche E-Mails genau an: Beim Phishing werden oft die Symbole und das allgemeine Design von echten Diensten verwendet, um Euch in Sicherheit zu wiegen, dahinter.

**So schützt Ihr Euch:**

- Schaut Euch den Absender der E-Mail an. Um die echten Anbieter nicht zu alarmieren, wenn mal ein Empfänger versehentlich auf Antworten klickt, sind die Absenderadressen dieser E-Mails meist ganz leicht verändert. Im Beispiel oben statt eFax.com efacks.com.  eine solche E-Mail ist mit an Sicherheit grenzender Wahrscheinlichkeit nicht echt.

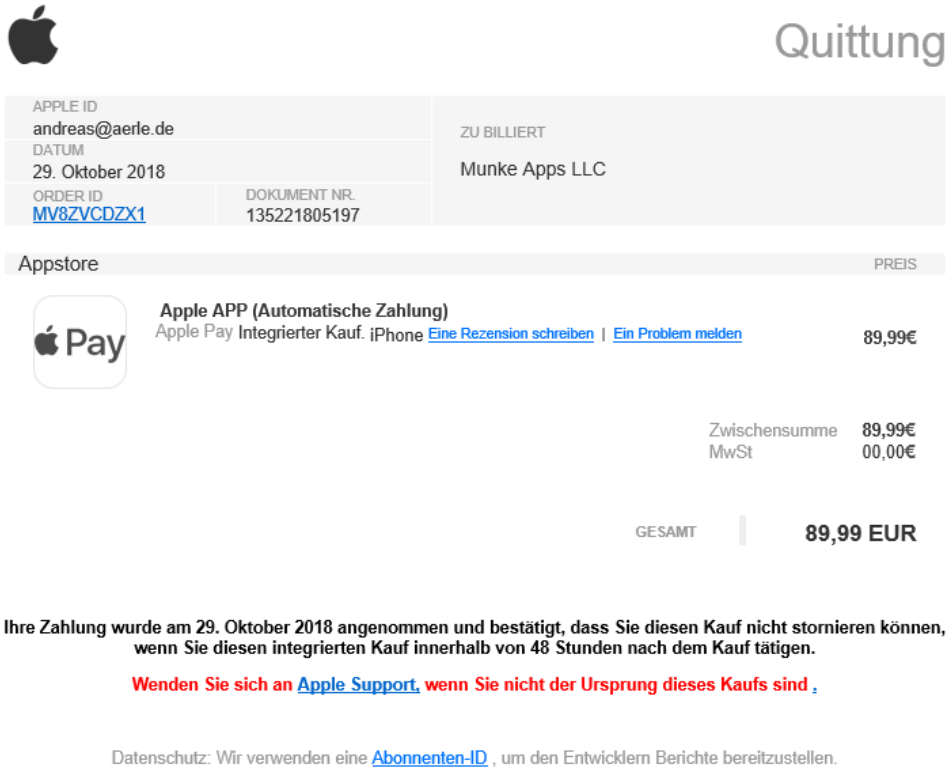
# So geht's leichter | Stoppt Phishing und Passwortklau

- Auch hier: Kontrolliert den Link, indem Ihr die Maus ohne zu Klicken darüber bewegt. Im Beispiel findet Ihr eine URL, die „mail.ru" enthält. Nie ein gutes Zeichen, und definitiv kein Link, den der Echte Dienst nutzen würde.


## Angebliche Bestell-Emails

Es gibt eine bestimmte Menge von Händlern im Internet, bei denen die Wahrscheinlichkeit hoch ist, dass ein Benutzer ein Konto bei ihnen hat. Amazon, Media Markt, die Telekom, Apple gehören beispielsweise dazu. Wenn man also nun eine Liste von E-Mail-Adressen nimmt und an diese Adresse dann eine vermeintliche Rechnung über ein gar nicht gekauftes Produkt schickt, dann ist die Wahrscheinlichkeit hoch, dass eine Reaktion erfolgt. Auch eine Aufforderung, aufgrund eines Sicherheitsvorfalles unbedingt die Zugangsdaten zu ändern, ist Garant dafür, dass der betroffene Anwender sich umgehend in Bewegung setzt. Er klickt auf den Link in der E-Mail und meldet sich schnell an. Mit seinem echten Benutzernamen und seinem echten Passwort. Dummerweise ist in vielen Fällen die Webseite, auf die Ihr geleitet werden, nicht echt. Und so hat unversehens ein Fremder Eure Zugangsdaten und kann fröhlich Bestellungen auslösen, das Konto übernehmen und Schaden anrichten.

# So geht’s leichter | Stoppt Phishing und Passwortklau



Quittung

APPLE ID
andreas@aerle.de
DATUM
29. Oktober 2018
ORDER ID
MV8ZVCDZX1
DOKUMENT NR.
135221805197

ZU BILLIERT
Munke Apps LLC

Appstore — PREIS

Pay
Apple APP (Automatische Zahlung)
Apple Pay Integrierter Kauf. iPhone Eine Rezension schreiben | Ein Problem melden — 89,99€

Zwischensumme 89,99€
MwSt 00,00€

GESAMT 89,99 EUR

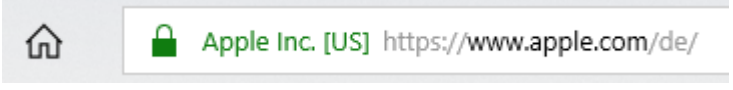
Ihre Zahlung wurde am 29. Oktober 2018 angenommen und bestätigt, dass Sie diesen Kauf nicht stornieren können, wenn Sie diesen integrierten Kauf innerhalb von 48 Stunden nach dem Kauf tätigen.

Wenden Sie sich an Apple Support, wenn Sie nicht der Ursprung dieses Kaufs sind .

Datenschutz: Wir verwenden eine Abonnenten-ID , um den Entwicklern Berichte bereitzustellen.

**So schützt Ihr Euch:**

- Die wichtigste Empfehlung in diesem Fall: Klickt auf keine Links in solchen E-Mails. Ruft manuell die Webseite des Händlers auf und meldet Euch sich an. Damit könnt Ihr vermeiden, dass Ihr auf eine falsche Seite geleitet werdet. Die Unterschiede zwischen echter und gefälschter URL sind manchmal so marginal, dass sie nicht auf den ersten Blick erkennbar sind. Ein Bindestrich statt eines Punktes machen hier einen riesigen Unterschied!
- Wenn Ihr bereits versehentlich auf den Link geklickt habt, dann kontrolliert unbedingt die Adresse, die angezeigt wird. Steht dort die „echte“ Internet-Adresse, dann ist alles gut.

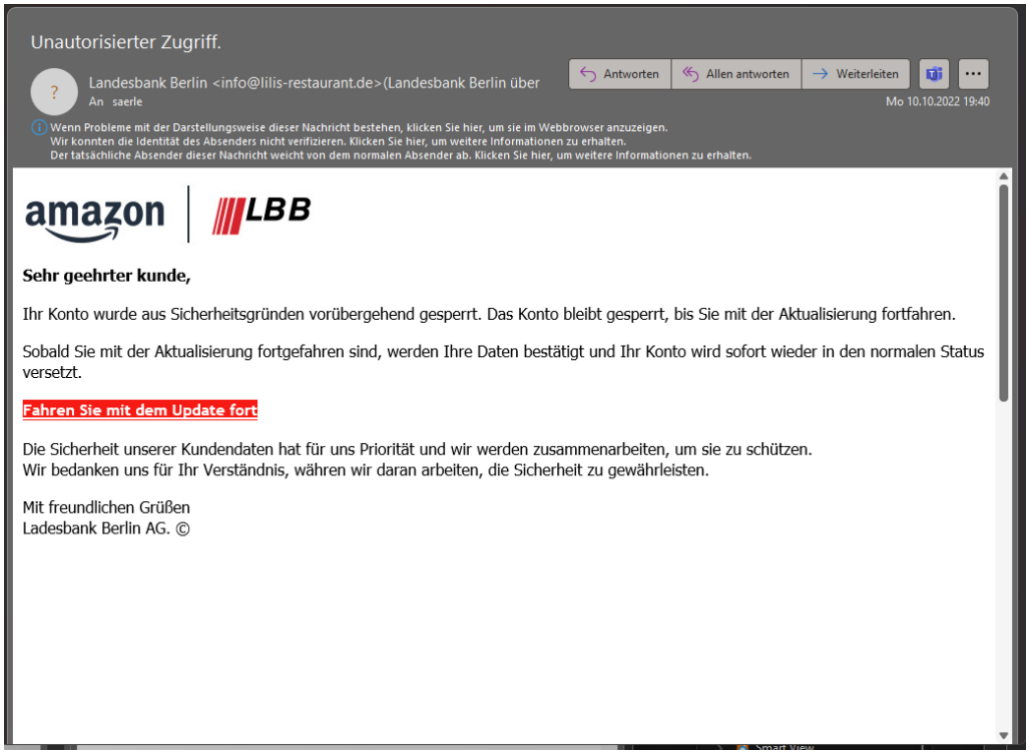


# So geht’s leichter | Stoppt Phishing und Passwortklau

- Meist versuchen die Phishing-Seiten, durch möglichst ähnliche Adressen den Anschein der Echtheit zu erwecken, im Beispiel vielleicht apple.xxlservices.com oder ähnlich. Abgewandelte Adressen sind ein nahezu sicheres Zeichen für einen Betrugsversuch.

## Konto kompromittiert? Danach schon!

Die perfidesten Phishing-Angriffe sind die, die mit der Angst der Benutzer spielen. Wenn Ihr von Eurem Netzbetreiber, PayPal, Eurer Bank oder Eurem Online-Versandhaus eine E-Mail bekommt, dass Euer Konto gehackt wurden, dann bricht schnell Panik aus.




Das ist psychologisch verständlich, denn diese bedienen unsere tiefe Angst vor finanziellem Schaden oder Kompromittierung der eigenen Identität. Genau darauf setzen die Angreifer: Wenn Ihr in einem Anfall

# So geht's leichter | Stoppt Phishing und Passwortklau

von Panik schnell reagieren wollt, dann kontrolliert Ihr naturgemäß weniger genau und meldet Euch auf einer täuschend echt aussehenden Webseite mit Euren echten Benutzerdaten an. Die werden ausgelesen. Teilweise leiten diese Seiten Euch dann noch an die echte Webseite weiter und melden Euch mit Euren echten Benutzerdaten an, sodass Euch der Umweg über die Phishing-Webseite nicht mal auffällt.

**So schützt Ihr Euch:**

- Zuallererst: Ruhe bewahren! Das klingt einfach, ist in der Praxis in einer solchen Drucksituation aber alles andere als einfach umsetzbar. Trotzdem: Wenn eine solche Warnung echt ist, dann ist der Schaden schon angerichtet. Die Minute Durchatmen und Sammeln wird es wahrscheinlich nicht schlimmer machen.
- Auch hier wieder: Klickt auf keine Links in solchen E-Mails. Ruft manuell die Webseite des Händlers/Dienstes auf und meldet Euch mit Euren Daten an. Wenn es tatsächlich ein Sicherheitsproblem gibt, dann werdet Ihr nach der Anmeldung einen unübersehbaren Hinweis dazu sehen.
- Ein Passwortwechsel ist immer eine gute Idee, auch wenn er in einem solchen Fall, in dem der Angreifer ja nur so getan hat, als wäre er in Euer Konto gekommen, nicht unbedingt nötig ist.

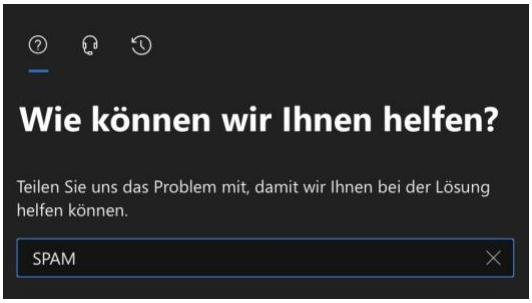
## Der freundliche Anrufer

Eine ebenfalls gerne gewählte Masche, Zugriff auf einen fremden Rechner oder die Daten darauf zu bekommen, ist der Anruf eines freundlichen Servicemitarbeiters. In oft gebrochenem Deutsch ist angeblich Microsoft aufgefallen, dass es einen Defekt oder Virenbefall auf Eurem Rechner gibt und man bietet ganz selbstlos Hilfe an. Das nennt man „Tech Support SCAM".

# So geht’s leichter | Stoppt Phishing und Passwortklau

Dazu müsst Ihr nichts mehr machen als dem Anrufer durch Aufruf einer Webseite oder Fernwartungssoftware Zugang zum Rechner geben, am besten noch unter Preisgabe der eigenen Zugangsdaten. Ist das geschehen, dann behebt der Bösewicht natürlich nicht etwaige Probleme auf dem Rechner, ganz im Gegenteil: Er schließt den Benutzer aus dem Rechner durch Änderung des Passwortes aus, und verlangt dann Geld dafür, ihn wieder hineinzulassen. Oder er schleust Schadsoftware ein, die ihm dann die Fernsteuerung des Rechners und den Zugriff auf die Daten erlaubt.

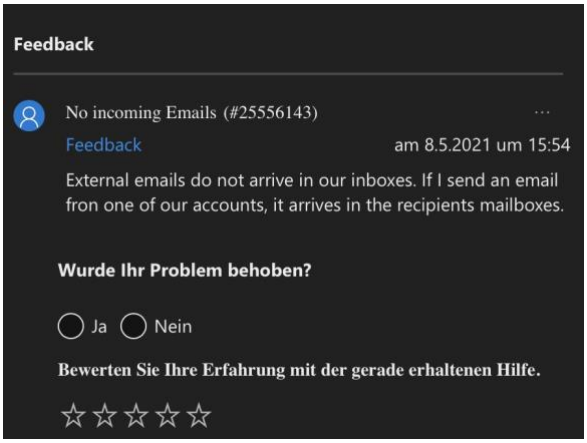
**So schützt Ihr Euch:**




- Gerade im Beispiel von Microsoft ist ein Anruf immer ausgelöst von einem Ticket, das Ihr selbst selber aufmachen müsst.
- Wenn Ihr Microsoft 365-Kunde seid, dann meldet Euch dazu am Admin-Center an. Dort klickt auf das Fragezeichen oben rechts und gebt eine Beschreibung des Problems an.
- Das System stellt jetzt automatisch verschiedene Lösungsmöglichkeiten zur Verfügung. Wenn diese nicht helfen, dann könnt Ihr auf das vorher noch gesperrte Symbol mit dem Kopf mit Headset klicken und alle relevanten Daten inklusive der Rückrufnummer eingeben.

# So geht’s leichter | Stoppt Phishing und Passwortklau

- Erst dann erfolgt ein Anruf von Microsoft, und wenn Ihr das Ticket zu den deutschen Geschäftszeiten aufmacht, dann findet der Kontaktversuch auch auf Deutsch statt.
  Im Ticket könnt Ihr sogar live verfolgen, dass Microsoft gerade anruft!




## Das nicht zustellbare Paket


Eine ebenfalls gerne gewählte Masche, Zugriff auf einen fremden Rechner zu bekommen, ist eine E-Mail, die angeblich von einem bekannten Paketdienst stammt. DHL, UPS, FedEx, DPD, vollkommen egal.

Das Paket könne nicht zugestellt werden und würde vernichtet/zurückgeschickt/es würden horrende Gebühren anfallen, Ihr müsst dringend reagieren und Eure Daten angeben. Die lassen sich dann nämlich wunderbar verkaufen oder anderer Unsinn damit anstellen!

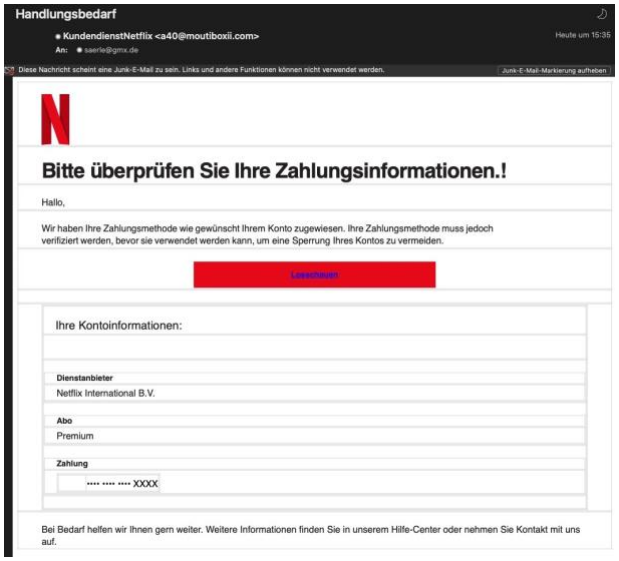
# So geht’s leichter | Stoppt Phishing und Passwortklau

**So schützt Ihr Euch:**

- Habt Ihr überhaupt etwas bestellt, das über diesen Paketdienst kommen soll? Wenn nicht, ignoriert die E-Mail einfach.
- In den meisten Fällen enthalten diese E-Mails keine Paketnummern. Sonst könntet Ihr nämlich über die Webseite des angeblichen Paketdienstes schnell herausfinden, dass es dieses Paket gar nicht gibt und die E-Mail ein reiner Schwindel ist. Wenn Ihr – wie im Beispiel – eine solche Nummer vorfindet, dann versucht, sie zu tracken. Dazu geht manuell auf die Webseite des Paketdienstes.

## Die falschen Kontoinformationen

Es gibt diverse kostenpflichtige Dienste, die Ihr mit einer hohen Wahrscheinlichkeit nutzt, du für die Ihr Irgendeine Zahlungsmethode hinterlegen müsst. Netflix, Amazon Prime Video oder Music, Disney+ und andere würden Euch natürlich den Zugang sperren, wenn Ihr  nicht zahlt.



# So geht’s leichter | Stoppt Phishing und Passwortklau

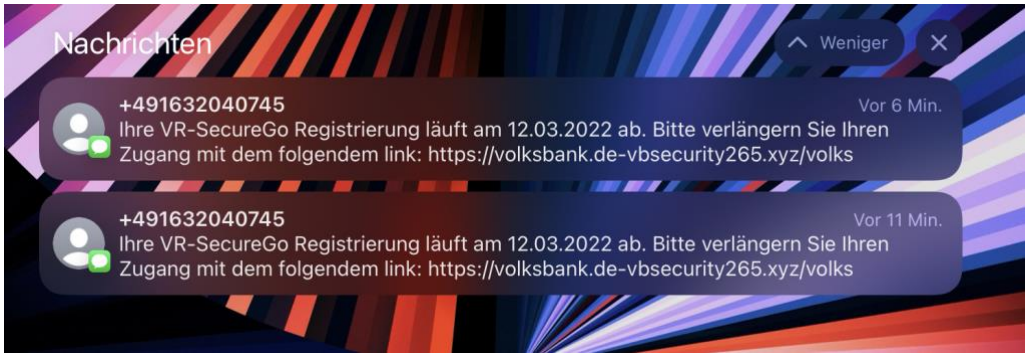
Bei einer Phishing E-Mail geht es nicht darum, Eure Zahlungsinformationen zu validieren, sondern die abzugreifen. Ihr gebt sie zur Bestätigung auf der vermeintlichen Netflix-Seite ein, und schon haben die Angreifer Eure Kontoverbindung und können sie für Einkäufe nutzen. Die Webseite meldet Euch natürlich den erfolgreichen Abgleich der Zahlungsdaten, um Euch nicht misstrauisch zu machen!

**So schützt Ihr Euch:**

- Habt Ihr überhaupt ein Abo bei diesem Dienst? Wenn nicht, ignoriert die E-Mail einfach.
- Überprüft Eure Zahlungsdaten, indem Ihr manuell über den Browser die Webseite des Dienstes aufruft und Euch anmeldet.

## Phishing in sozialen Netzwerken, WhatsApp, SMS

Ihr nutzt keine E-Mails? Macht nichts. Facebook, WhatsApp, SMS und iMessage: Die Wege, auf denen Phishing-Versuche an Euch herangetragen werden, sind vielfältig.

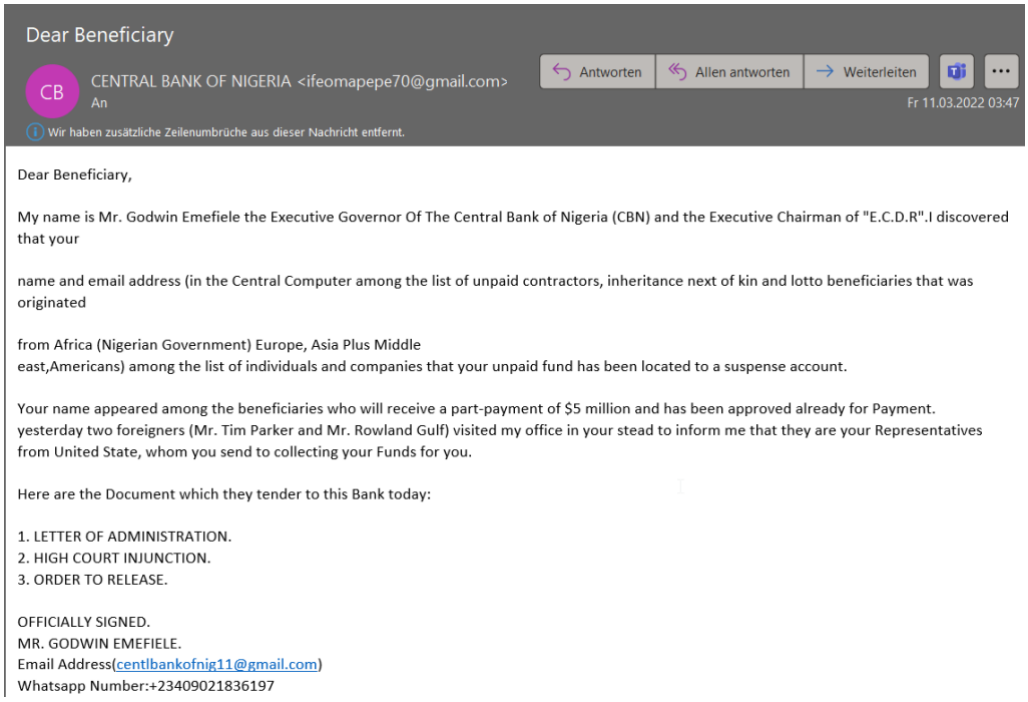



Eure Handynummer ist nicht ganz so geheim, wie sie es vielleicht sein sollte. Aus diversen Datenlecks ausgelesen wird sie verwendet, um Eure Daten zu kompromittieren.

# So geht’s leichter | Stoppt Phishing und Passwortklau

Meist kommen die Anfragen von fremden Telefonnummern, die Ihr nicht in Euren Kontakten gespeichert habt. Auch hier gilt: Ignoriert die Nachrichten. Wenn Euch darin ein Sicherheitsvorfall wie ein geknacktes Konto oder ein kompromittiertes Passwort gemeldet werden, ruft wieder manuell – und nicht über den Link in der Nachricht – die betroffene Webseite auf. Meist stellt Ihr erleichtert fest, dass alles in Ordnung ist.

Und Ihr müsst tapfer sein: Die fünf Millionen Dollar, die die nigerianische Bank Euch aus dem Nachlass eines unbekannten Gönners verspricht, werdet Ihr auch nie bekommen!



Dear Beneficiary

CB CENTRAL BANK OF NIGERIA <ifeomapepe70@gmail.com>
An

Antworten | Allen antworten | Weiterleiten | ...

Fr 11.03.2022 03:47

Wir haben zusätzliche Zeilenumbrüche aus dieser Nachricht entfernt.

Dear Beneficiary,

My name is Mr. Godwin Emefiele the Executive Governor Of The Central Bank of Nigeria (CBN) and the Executive Chairman of "E.C.D.R".I discovered that your

name and email address (in the Central Computer among the list of unpaid contractors, inheritance next of kin and lotto beneficiaries that was originated

from Africa (Nigerian Government) Europe, Asia Plus Middle
east,Americans) among the list of individuals and companies that your unpaid fund has been located to a suspense account.

Your name appeared among the beneficiaries who will receive a part-payment of $5 million and has been approved already for Payment.
yesterday two foreigners (Mr. Tim Parker and Mr. Rowland Gulf) visited my office in your stead to inform me that they are your Representatives from United State, whom you send to collecting your Funds for you.

Here are the Document which they tender to this Bank today:

1. LETTER OF ADMINISTRATION.
2. HIGH COURT INJUNCTION.
3. ORDER TO RELEASE.

OFFICIALLY SIGNED.
MR. GODWIN EMEFIELE.
Email Address(centlbankofnig11@gmail.com)
Whatsapp Number:+23409021836197

## Phishing im Internet

Der Einzelhandel ist unter Druck: Mehr und mehr Anwender kaufen ihre Waren im Internet. Dank Zahlungsdienstleistern wie PayPal und anderen

# So geht's leichter | Stoppt Phishing und Passwortklau

nicht nur in Deutschland oder Europa, sondern weltweit. Zahlung und Versand sind so einfach, und die Preise im Ausland oft verlockend günstig. Diese Tatsache öffnet einen weiteren Kanal für Phishing und Betrug.

## Fake-Shops erkennen

Ein immer größer werdendes Übel sind die sogenannten Fake-Shops. Wie die gleich genannten Nachrichten versuchen diese, Euch etwas vorzugaukeln. Tolle Angebote, günstige, meist zeitlich limitierte Preise und schneller Versand sollen Euch zum Kauf animieren. Habt Ihr erst mal bezahlt, dann wartet Ihr oft ewig auf die Lieferung. Wenn Ihr überhaupt kommt, dann entspricht die Ware oft nicht dem, was Ihr bestellt und erwartet habt.

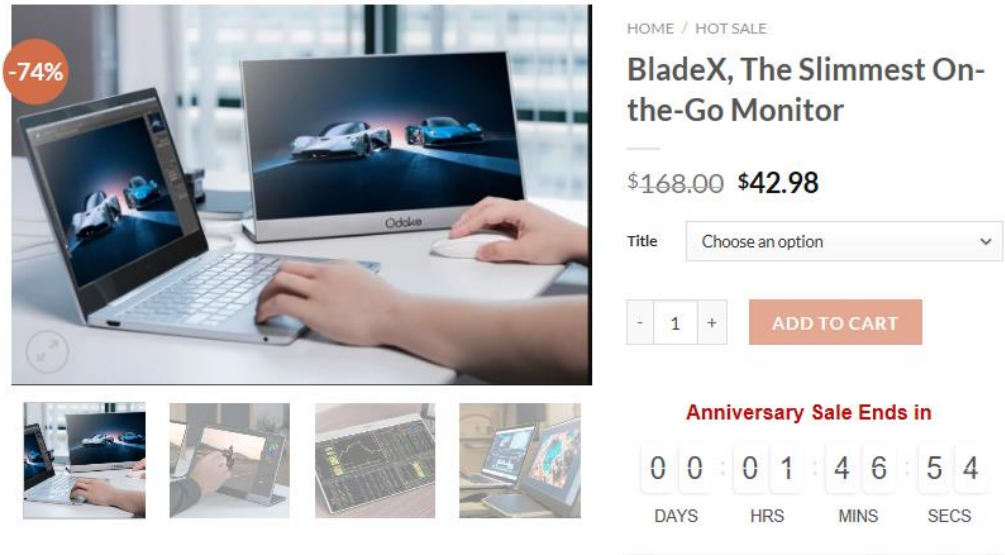
Noch schlimmer: Legt Ihr ein Benutzerkonto an und verwendet schon mal woanders benutzte Zugangsdaten, dann landen die schnell in Datenbanken, die im Internet verkauft werden und Übertätern dazu dienen, einfach mal bei allen möglichen Seiten zu versuchen, sich damit in Eurem Namen anzumelden!

Absolute Sicherheit bei der Erkennung der schwarzen Schafe gibt es nicht. Wir zeigen Euch aber Merkmale, die Euch stutzig machen sollten.

### Der Preis

Bei vielen Fake-Shops ist es eine Kombination aus dem vollkommen unrealistisch niedrigen Preis und der Aussage, dass der ja nur noch ganz kurz gilt. Oder die Zahl der verfügbaren Geräte schon fast ausgeschöpft ist.

# So geht’s leichter | Stoppt Phishing und Passwortklau




Vergesst einfach die Hoffnung, dass es Händler gibt, die Euch teure Hardware nahezu schenken. Das ist eine Illusion, die Euch nur unnötig Geld kostet und Frust bringt.

***Tipp***

Diese Warnungen gelten natürlich nicht für die Angebotsschlachten der großen Anbieter wie Amazon und andere: Black Friday, Cyber Monday und wie sie alle heißen beinhalten tatsächlich in den meisten Fällen stark reduzierte und von der Anzahl her limitierte Waren!

## Die Zahlweise

Die meisten Internetshops bieten sichere Zahlweisen über bekannte Zahlungsanbieter wie PayPal, Klarna oder andere an. Wenn eine Webseite entweder nur „sonderbare“ Zahlungsanbieter verwendet oder aber die ganzen üblichen bei der Bezahlung nicht funktionieren und nur die Vorabüberweisung übrigbleibt: Finger weg! Ist das Geld erst einmal auf der Reise, dann habt Ihr wenig Handhabe, wenn die Ware nicht kommt. Käuferschutz gibt es nun mal bei Überweisungen nicht.

# So geht’s leichter | Stoppt Phishing und Passwortklau

## Die Millionen zufriedener Kunden

Wer kann besser Auskunft über die Vertrauenswürdigkeit eines Shops geben als andere Kunden? Prinzipiell richtig, bei Fake-Seiten aber ein zweischneidiges Schwert: Nichts einfacher, als automatisiert positive Bewertungen auf eine Seite zu stellen, wenn man sie selber programmiert hat.

Wenn die Bewertungen größtenteils positiv sind, dann schaut Euch diese genauer an: Bei Fake-Shops habt Ihr ganz oft dieselben Wortlaute und Formulierungen, die immer und immer wieder verwendet werden. Auch sonderbarer Satzbau und Wortwahl sollten skeptisch machen: Fake-Bewertungen werden meist per automatischem Übersetzer erstellt und ungeprüft hochgeladen.

Mittlerweile lassen sich Bewertungen gar im Hunderterpack online kaufen. Das ist vom Münchner Landgericht Ende 2019 als rechtswidrig erklärt worden. Doch auch unabhängig von der Rechtslage: Wenn ein Shop es nötig hat, sich Bewertungen zu kaufen, dann kann es mit der Qualität nicht weit her sein!

## Besonders tolle Siegel

Der Käufer an sich ist ja schon kritisch: Wenn er schon im Internet kauft, dann muss es zumindest ein geprüfter Händler sein. Zumindest sind wir Europäer so aufgestellt. Und bei „echten“ Online-Shops sind die Siegel tatsächlich ein Zeichen für Kontrollinstanzen. Ob die nun besonders aussagekräftig sind, darüber kann man streiten. Zumindest führt Euch ein Klick auf ein solches Siegel zu der Zertifizierungsstelle.

# So geht’s leichter | Stoppt Phishing und Passwortklau

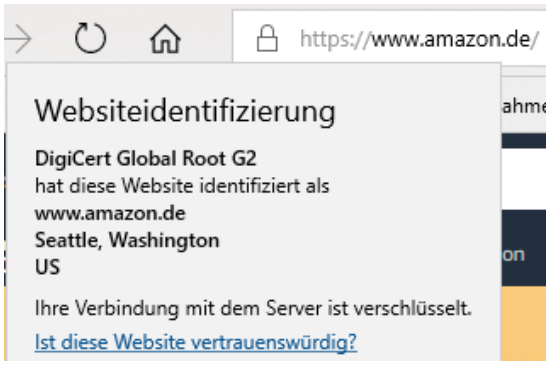

Bei den meisten Fake-Shops bekommt Ihr unzählige bunte Bildchen angezeigt, teilweise auch von namhaften Anbietern. Wenn Ihr darauf klickt, dann passiert entweder gar nichts, oder Ihr werdet auf eine echte Seite geleitet, die aber keinen Bezug zu der Shop-Seite hat. Auch das ist ein Warnsignal!

## Sichere Webseiten

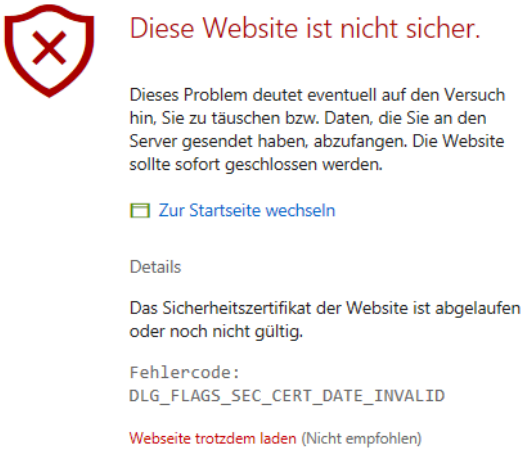
Eine Webseite schafft Euch eine leicht andere Einkaufsumgebung als ein echter Laden. Beim Shopping in der Stadt könnt Ihr Euch vor dem Kauf anhand des Angebots, der Lage des Ladens, der Mitarbeiter zumindest einen visuellen Eindruck verschaffen. Und vor allem könnt Ihr die Produkte anfassen und deren Qualität vorher beurteilen. Im Internet ist vieles Vertrauenssache. Wenn Ihr kauft, dann könnt Ihr nur hoffen, auch die bestellte und meist vorbezahlte Ware zu bekommen.

# So geht’s leichter | Stoppt Phishing und Passwortklau

Einen Hinweis wenig bietet hier das Zertifikat der Webseite. Ein SSL-Zertifikat ist quasi ein Siegel, das die Organisation, der die Webseite gehört, und die Webseitenadresse miteinander in Verbindung bringen. Das Zertifikat ermöglicht es dann, die Kommunikation zwischen Eurem Rechner und dem Shop zu verschlüsseln.




Das ist wichtig, damit beispielsweise Kreditkarten- oder Kontoinformationen für die Bezahlung nicht auf dem Weg abgefangen und missbraucht werden können. Erkennen können Ihr den Einsatz eines SSL-Zertifikats daran, dass links (oder rechts, je nach Browser) der Internetadresse ein Schloss angezeigt wird. Klickt darauf, dann seht Ihr die sogenannte Webseitenidentifizierung. Die zeigt an, auf welchen Händler die Seite registriert ist. Keine Fake-Seite könnte sich also hier als Apple oder Amazon ausgeben, weil sie gar nicht erst durch den Prüfprozess zur Erteilung des SSL-Zertifikats kommen würde.




Vorsicht ist geboten, wenn eine Webseite nicht verschlüsselt ist oder gar das Zertifikat nicht zu Seite passt oder abgelaufen ist. Letzteres kann immer mal passieren, ist aber bei einem Online-Händler kein gutes Zeichen. Ihr

# So geht's leichter | Stoppt Phishing und Passwortklau

könnt die Webseite dann trotzdem besuchen, empfehlenswert (gerade bei Shopping- oder Online-Banking-Seiten) ist das nicht!

## Gütesiegel als Qualitätsmerkmal

Wenn eine Webseite nicht schon bekannt ist und sich einen gewissen Ruf erarbeitet hat, dann ist es recht schwer, Vertrauen zu schaffen. Da hilft es, sich von einem unabhängigen Zertifizierer die Aussage zu besorgen, dass man als Händler vertrauenswürdig ist. Wenn Ihr auf ein solches Siegel klickt, dann gelangt Ihr im Normalfall auf die Webseite des Zertifizierers und bekommt angezeigt, welche Eigenschaften des Shops dieser mit dem Siegel bestätigt.


Nun ist Papier geduldig, und nicht jedes Siegel ist gleich wertvoll. Trusted Shops (https://www.trustedshops.de/) beispielsweise vergibt sein Siegel nur an Shops mit besonders hohen Standards. Als Zeichen der Überzeugung bietet Trusted Shops dann gleich noch einen eigenen Käuferschutz an: Habt Ihr Probleme beim Kauf, dann findet Ihr dort Unterstützung. Andere bekannte und renommierte Siegel sind das **EHI geprüfter Online-Shop** und das **Safer Shopping** vom TÜV Süd.

Es gibt noch viele andere Zertifikate, aber manche sind nicht das virtuelle Papier wert, auf dem sie stehen.

# So geht's leichter | Stoppt Phishing und Passwortklau

## Impressum, Kontakt und Datenschutz

Vertrauensbildend, aber auch eine rechtliche Notwendigkeit: Ein Impressum und eine Datenschutzerklärung muss eine jede Webseite haben. Auch hierauf solltet Ihr einen genauen Blick werfen. Aus mehreren Gründen:

### Impressum und Unternehmenssitz

Das Impressum, alternative auch „Anbieterkennzeichnung" genannt, gibt Euch vor allem Auskunft über den Betreiber der Webseite. Das zeigt Euch vor allem, ob es sich um einen Betreiber in Deutschland oder dem Ausland handelt. Dazu übrigens später noch ein paar weitere Anmerkungen. Wenn eine Webseite aber kein Impressum hat, dann solltet Ihr skeptisch sein: Euch fehlt der Ansprechpartner, wenn es einmal hart auf hart geht und Ihr einen Anwalt einschalten müsst. Zum Beispiel, weil die Ware nicht kommt oder eine Rücksendung nicht funktioniert oder Ihr sicher seid, dass aus diesem Shop Eure Benutzerdaten entwendet oder missbraucht wurden. Und da in Deutschland Impressumspflicht herrscht und jeder Händler eine Abmahnung scheut, ist der Shop entweder schludrig oder schert sich nicht darum. Keine gute Voraussetzung für einen Einkauf!


impressum

Verantwortlich für die auf dieser Website publizierten Artikel und Inhalte (mit Ausnahme der Kommentare), sofern keine anderen Angaben gemacht werden:

Jörg Schieb
Humboldtstr. 10
D-40667 Meerbusch

FON: 02132-6733305
FAX: 02132-67333059

MAIL: fragen@schieb.de

Bitte verwenden Sie mein Kontaktformular.

Autoren auf schieb.de
Das Infoportal schieb.de enthält Artikel von verschiedenen Autoren/Redakteuren.

Chefredakteur:
Jörg Schieb

Allgemein gilt: Das Impressum sollte nicht mehr als einen Klick von der Startseite entfernt sein. Meist finden Sie es am oberen oder unteren Bildschirmrand.

# So geht's leichter | Stoppt Phishing und Passwortklau

### Kontaktmöglichkeiten

Neben den rechtlichen Kontaktdaten, wie sie im Impressum zu finden sein sollten, ist auch die Beratungsmöglichkeit ein Thema. Ein Online-Händler, der etwas auf Kundenservice hält, bietet Euch Hilfestellung. Ob per Telefon, Chat oder Ticketsystem, zumindest aber per E-Mail. Auch bei einem Umtausch oder einer Reklamation solltet Ihr wissen, wie Ihr jemanden erreicht.

Oft wird das Impressum kombiniert mit den Allgemeinen Geschäftsbedingungen (AGB). In diesen sollte sich auch die Abwicklung bei der Rückgabe gekaufter Ware finden.

## Phishing-Erkennung trainieren

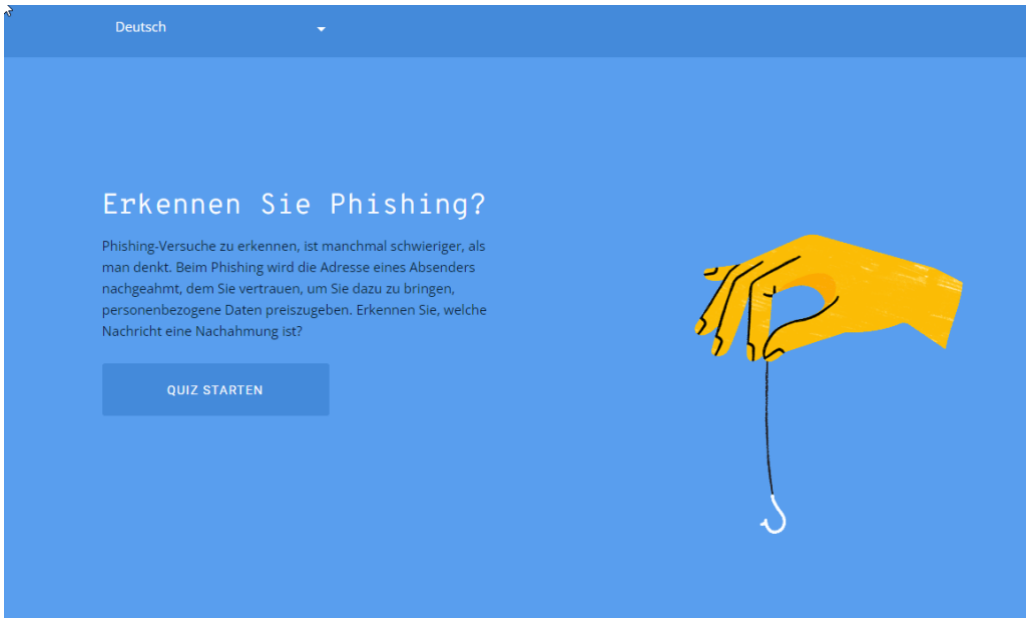
Ihr habt auf den vorangegangenen Seiten eines gemerkt: Phishing-Attacken sind vielfältig und immer anders. Es gibt keinen wirklichen Schutz, außer Euch immer und immer wieder damit zu beschäftigen, Euch zu trainieren, solche Mails und Nachrichten zu erkennen und gar nicht erst darauf zu reagieren.

Natürlich könnt Ihr mit unseren Tipps oben schon viele Phishing-Maschen erkennen. Es gibt aber auch zwei Quellen im Internet, die Euch da unterstützen:

# So geht’s leichter | Stoppt Phishing und Passwortklau

## Google's Jigsaw Phishing-Quiz

Google als Anbieter verschiedenster Webdienste ist natürlich hoch interessiert daran, Phishing-Seiten zu identifizieren und auf der anderen Seite Euch als Benutzer davon abzuhalten, auf sie reinzufallen. Schließlich könnten die ja auch im Suchergebnisse einer Google-Suche auftauchen und Anwender auf den Link klicken!




Unter diesem Link findet Ihr das Quiz. Ihr gebt Euren Namen und Eure E-Mail-Adresse an, dann zeigt Euch das Quiz verschiedene E-Mails und fordert Euch auf, diese zu bewerten: Phishing oder nicht?

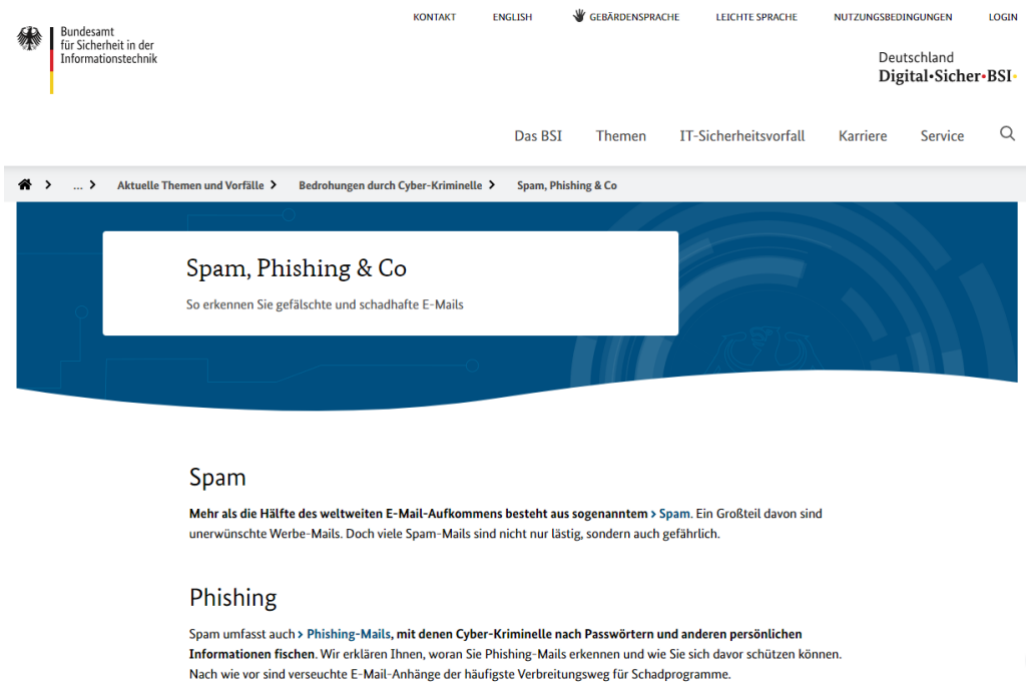
Keine Sorge: Weder werden Eure eingegebenen Informationen verwendet (die dienen nur dazu, die angezeigten E-Mails noch ein wenig realistischer zu machen), noch sind die Links in den Beispielen klickbar.  Google will Euch ja schließlich nicht gefährden!

Die Beispiel-E-Mails ändern sich immer mal wieder, es macht also Sinn, das Quiz regelmäßig zu machen!

# So geht’s leichter | Stoppt Phishing und Passwortklau

## Der E-Mail-Sicherheits-Check des BSI

Das Bundesamt für Sicherheit in der Informationstechnik, kurz: BSI, ist die Behörde, die sich intensiv mit Sicherheitslücken beschäftigt. Die Aufklärung der Bürger ist dabei ein wichtiges Thema.




Hier findet Ihr den Bereich zum Thema SPAM und Phishing. Darin findet Ihr ein Video, in dem anschaulich dargestellt wird, woran Ihr gefälschte E-Mails erkennen könnt.  Auch auf der BSI-Seite werden die Inhalte immer wieder angepasst und verändert, regelmäßiger Besuch lohnt sich also.

## Vorsicht bei Anmeldung über Facebook § Co.

Fast jeder Shop oder Dienst im Internet erfordert ein Konto, in dem Ihr Eure Adress- und Zahlungsdaten hinterlegt. Das führt schnell dazu, dass Ihr Zugangsdaten mehrfach verwendet. Als Alternative bieten viele

# So geht’s leichter | Stoppt Phishing und Passwortklau

Anbieter daher die Anmeldung über soziale Netzwerke an. Hier solltet Ihr Vorsicht walten lassen!

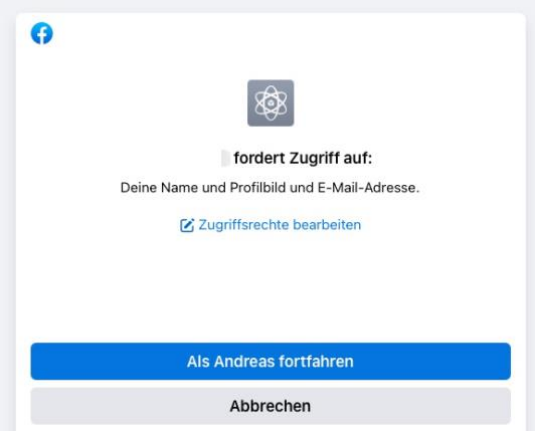

Die Idee ist simpel: Die sozialen Netzwerke nutzt Ihr regelmäßig, kennt also die Zugangsdaten. Wenn Ihr Eure Kennwörter regelmäßig ändert (was wir dringend empfehlen!), dann macht Ihr das an einer zentralen Stelle, statt jede Seite einzeln aufrufen zu müssen.

Eigentlich also eine hilfreiche Möglichkeit. Die hat allerdings auch ein Risiko: Ihr müsst bei der Einrichtung des Nutzerkontos bei einer solchen Webseite einmal eine Anmeldung bei dem sozialen Netzwerk Eurer Wahl durchführen. Dazu gebt Ihr die Zugangsdaten ein.

Kontrolliert hier unbedingt, dass die Anmeldemaske tatsächlich von dem sozialen Netzwerk stammt, das Ihr ausgewählt haben, im Beispiel oben Facebook. Fake-Seiten können Euch nach einem Klick auf **Mit Facebook fortfahren** eine täuschend echte Anmeldemaske von Facebook präsentieren, die aber in Wirklichkeit nur dazu da ist, Eure Zugangsdaten abzugreifen. Um das zu kontrollieren, könnt Ihr Euren Browser nutzen. Klickt im Anmeldebildschirm oben in die Adresszeile des Browsers und stellt sicher, dass die angezeigte Adresse tatsächlich

# So geht's leichter | Stoppt Phishing und Passwortklau

zu dem sozialen Netzwerk gehört, über das Ihr Euch anmelden wollt! Ist das nicht der Fall, dann gebt keinesfalls irgendwelche Zugangsdaten ein!




Wichtig auch: Kontrolliert, welche Berechtigung die Webseite anfordert. Warum beispielsweise sollte eine Shop-Seite in Eurem Namen Posts schreiben oder Eure komplette Freundesliste sehen können?

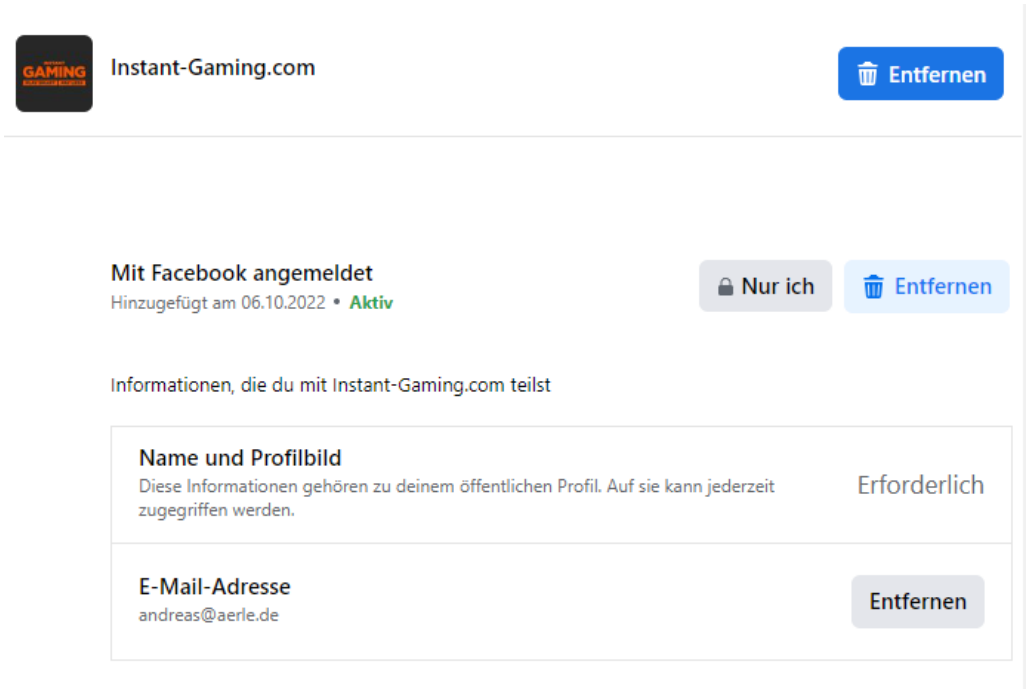
Auch wenn es sich um keine Phishing-Seite handelt, solltet Ihr regelmäßig die Webseiten, bei denen Ihr Euch mit Facebook anmelden könnt, ansehen und bereinigen.

## Übersicht über die Anmeldungen

Wenn Ihr das erste Mal die Anmeldung per Facebook bei einer neuen App oder Webseite vorgenommen habt, informiert Euch Facebook darüber. Per Push-Nachricht, E-Mail und Benachrichtigung auf der Webseite. Ein Klick auf diese Benachrichtigung führt Euch dann direkt zur Übersicht der aktiven Apps und Webseiten.

- Alternativ klickt auf **Einstellungen** > **Apps und Websites**, um in die Übersicht derjenigen zu kommen, die mit Eurem Facebook-Konto gekoppelt sind.
- Wenn Ihr auf eines der Symbole klickt, dann zeigt Euch Facebook alle Berechtigungen, die die App/die Webseite hat.

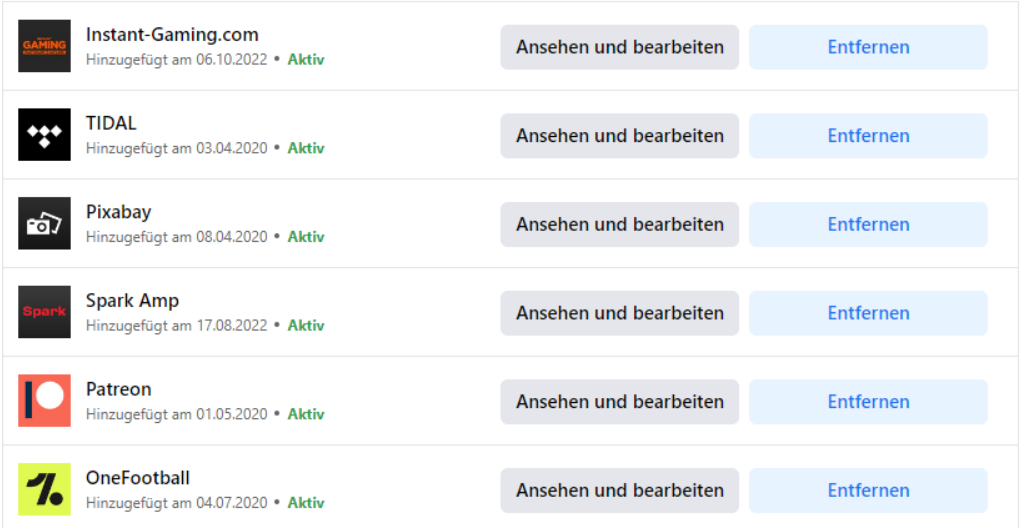
# So geht’s leichter | Stoppt Phishing und Passwortklau




## Löschen der Anmeldung per Facebook

Im Normalfall verwendet Ihr die Anmeldung per Facebook für Dienste und Seiten, die Ihr nur selten nutzt und wo der Aufwand des Anlegens eines eigenen Benutzerkontos übertrieben scheint. Da macht es Sinn, die Zugriffsrechte auch wieder zu löschen! In der Übersicht der **Apps und Websites** bei Facebook könnt Ihr für jedes Element, auf das Zugriff besteht, diesen Zugriff ein- oder ausschalten. Das Ausschalten kann natürlich dazu führen, dass bestimmte Funktionen nicht mehr funktionieren.

# So geht’s leichter | Stoppt Phishing und Passwortklau




Markiert in der Übersicht einen Eintrag und klickt dann auf **Entfernen**, um den Zugriff der App/Webseite zu löschen. Besonders bei nur einmal verwendeten Anmeldungen solltet Ihr dies direkt machen, dann vergesst Ihr es später nicht mehr.

## Ransomware und mehr: Die Erpressung

Ein weiteres Übel in der Arbeit mit PC und Mac abseits des Phishings ist die versuchte Erpressung: Ihr bekommt eine E-Mail, in der man Euch mit einem vermeintlich schlüpfrigen Video erpressen will, oder der PC meldet plötzlich, er könne nicht mehr auf die Dateien zugreifen, weil diese verschlüsselt sind. Je nach Art der Erpressung müsst Ihr unterschiedlich reagieren!

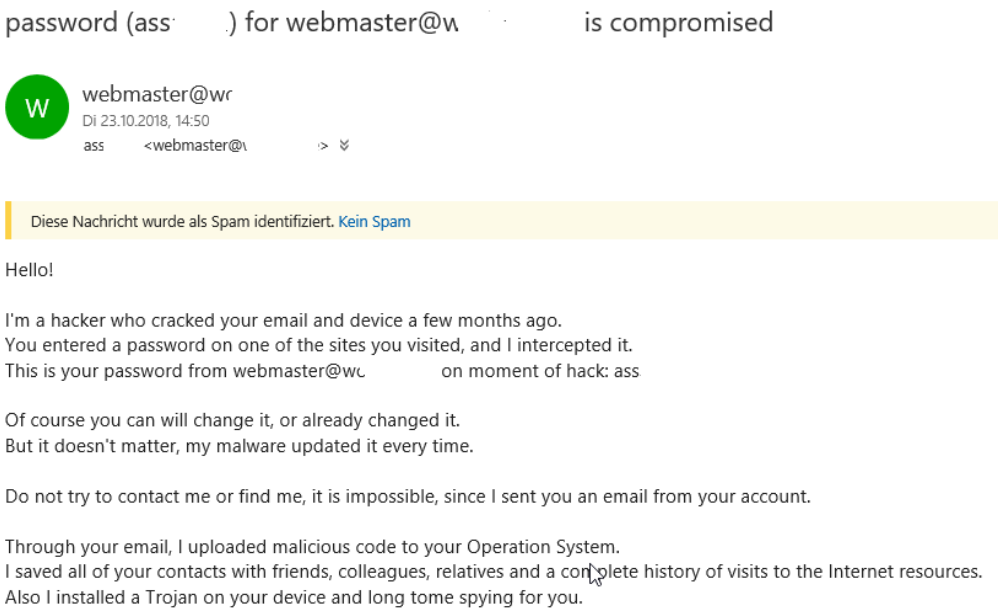
# So geht's leichter | Stoppt Phishing und Passwortklau

## Der Erpressungs-E-Mail

Habt Ihr auch schon einmal die Mail bekommen, dass der E-Mail-Account gehackt wurde und das mit einer richtigen E-Mail-Adresse und einem korrekten Passwort?

Diese vermeintlich authentische E-Mail fordert Euch dann auf, ganz schnell einen bestimmten Betrag in Bitcoins zu beschaffen und an den Absender zu überweisen. Ein Ändern des Passwortes nütze nichts, weil der Rechner schon lange mit einem Virus infiziert sei… und so weiter.

In den allermeisten Fällen sind diese E-Mails heiße Luft. Sie beziehen ihre Informationen aus Datenbanken, die gestohlene Passwörter enthalten, und versuchen einfach mal, Panik zu erzeugen. Überweist nichts… aber prüft natürlich, ob das Kennwort tatsächlich noch aktuell ist und ändert es.


password (ass .) for webmaster@w is compromised

W webmaster@wc
Di 23.10.2018, 14:50
ass <webmaster@\ >

Diese Nachricht wurde als Spam identifiziert. Kein Spam

Hello!

I'm a hacker who cracked your email and device a few months ago.
You entered a password on one of the sites you visited, and I intercepted it.
This is your password from webmaster@wc on moment of hack: ass

Of course you can will change it, or already changed it.
But it doesn't matter, my malware updated it every time.

Do not try to contact me or find me, it is impossible, since I sent you an email from your account.

Through your email, I uploaded malicious code to your Operation System.
I saved all of your contacts with friends, colleagues, relatives and a complete history of visits to the Internet resources.
Also I installed a Trojan on your device and long tome spying for you.

**So schützt Ihr Euch:**

# So geht’s leichter | Stoppt Phishing und Passwortklau

- Klickt in diesen E-Mails auf keinen Link und öffnet keine Anhänge: Die Wahrscheinlichkeit ist hoch, dass sich darin Schadsoftware befindet.

## Ransomware: Verschlüsselter Rechner

Deutlich schlimmer ist es, wenn Ihr Euch eine Ransomware (einen Verschlüsselungstrojaner) eingefangen habt. Das ist eine Schadsoftware, die Dateien auf dem PC verschlüsselt und diese nur gegen Zahlung einer teils heftigen Gebühr wieder entschlüsselt. Zumindest ist das das Versprechen, was die Ransomware in der Meldung auf Eurem Bildschirm anzeigt. So geschehen beispielsweise im Oktober 2022 bei der Zeitung „Heilbronner Stimme“.

Stimme Mediengruppe

Über uns Philosophie Geschäftsfelder Produkte Karriere Neuigkeiten

### Cyberangriff auf die Heilbronner Stimme

**14. Oktober 2022**

Wegen eines Cyberangriffs sind die Systeme der Heilbronner Stimme sowie weiterer Unternehmen der Stimme Mediengruppe, darunter das echo, RegioMail und der Stimme Pressedruck, seit dem Freitagmorgen weitgehend lahmgelegt. Die Mediengruppe ist seither nicht mehr erreichbar – weder telefonisch noch per E-Mail. Alle Systeme sind bis auf Weiteres blockiert und eine Zeitungsproduktion, sowie E-Paper Produktion sind nicht möglich. Ein interner Krisenstab untersucht gemeinsam mit der Polizei und Cyberexperten die Vorgänge. Bei den mutmaßlichen Tätern handelt es sich um eine bekannte Cyber-Tätergruppe. Eine Lösegeldforderung ist nicht eingegangen. Das genaue Ausmaß des Cyberangriffs ist bislang noch unklar. Inwieweit Daten von Privat- und Geschäftskunden betroffen sind, lässt sich zum aktuellen Zeitpunkt nicht sagen. Es wird mit Hochdruck an der Abwehr und Schadensbegrenzung gearbeitet.

Auf stimme.de und echo24.de wird weiterhin aktuell von allen anfallenden Terminen und Ereignissen berichtet. Darüber hinaus konnte gemeinsam mit der Brettener Woche in Bretten eine sechsseitige Notfallausgabe produziert werden, welche in Karlsruhe gedruckt und am morgigen Samstag an alle Haushalte im Stadt- und Landkreis Heilbronn sowie im Hohenlohekreis verteilt wird.

Wir werden Sie über unsere Website kontinuierlich auf dem Laufenden halten. Darüber hinaus ist unsere Servicenummer ebenfalls unter 07131/615615 erreichbar.

# So geht's leichter | Stoppt Phishing und Passwortklau

Eine Garantie dafür habt Ihr nicht, und ein allgemeingültiges Verfahren gibt es auch nicht.

Zuerst aber die gute Nachricht: Die meisten Antivirenprogramme haben auch einen Schutz gegen Ransomware integriert. Die Wahrscheinlichkeit einer Infektion ist also begrenzt.

## Identifikation der Ransomware

Programmierer eines Virus oder einer Ransomware sind meist mitteilsam: Sie wollen zeigen, wie gut sie sind. Natürlich nicht so, dass Ihr die Person dahinter identifizieren könnt, aber eines könnt Ihr immer machen: Die Infotexte mit der Suchmaschine Eurer Wahl finden.

Das geht in den allermeisten Fällen, weil der Natur der Erpressung nach der Browser benötigt wird, damit die Überweisung in Bitcoins ausgeführt werden kann. Wenn Ihr die Ransomware identifizieren konntet, dann findet Ihr in der zugehörigen Fundstelle oft eine wichtige Empfehlung: Ob Ihr den Rechner herunterfahren oder ihn laufen lassen sollt.

Bei einem Teil der Ransomwares findet die Verschlüsselung erst nach einem Neustart des Rechners statt. Bei anderen solltet Ihr den Rechner schnellstmöglich herunterfahren.

## Beheben der Schäden

Um weitere Hilfe zu bekommen, könnt Ihr auch einen Screenshot der Lösegeldforderung oder eine bereits verschlüsselte Datei bei dem kostenlosen Dienst ID Ransomware hochladen und bekommen Informationen über die Malware inklusive der ersten Tipps, was Ihr als Nächstes machen solltet.

# So geht’s leichter | Stoppt Phishing und Passwortklau

Auch die Seite NoMoreRansom.com ist eine gute Anlaufstelle. Sie bietet für immer mehr Ransomwares Entschlüsselungssoftware an, die die Dateien entschlüsselt und wieder zugänglich macht.

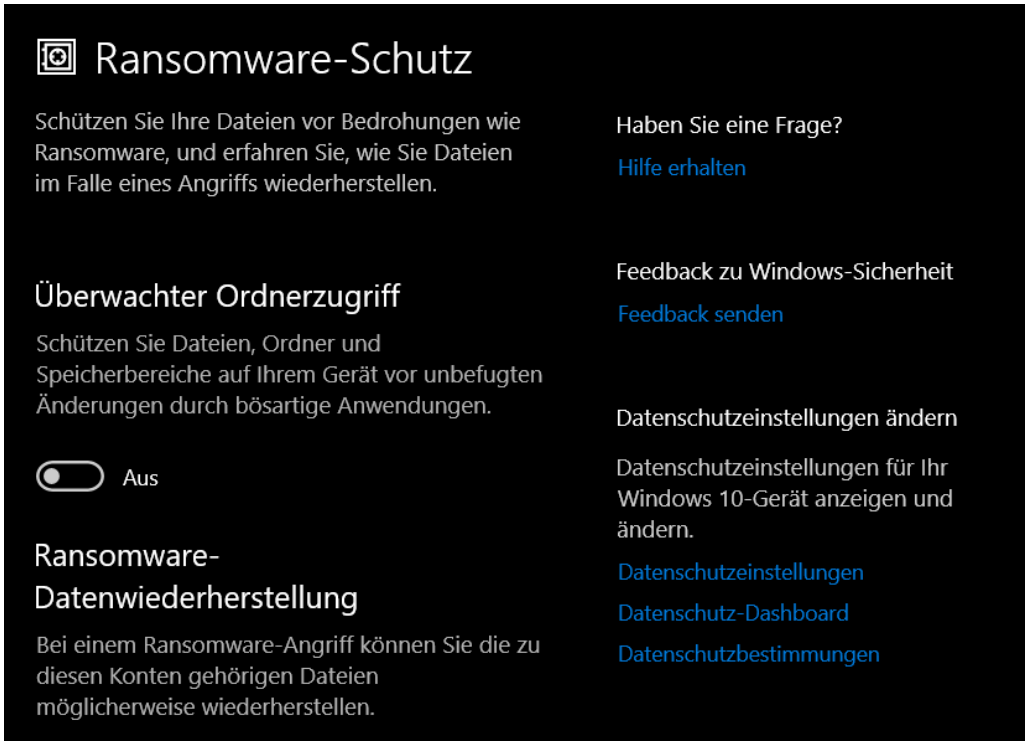
Das alleine ist allerdings nur ein Teil der Gegenmaßnahmen. Dieser nützt nur kurzfristig, wenn Ihr die Ransomware selber nicht loswerdet. Das kann durch eine Antivirensoftware geschehen, die Ransomware als Virus erkennen sollte.

Um sicherzugehen, installiert Windows/macOS komplett neu! Das Einspielen eines Backups über eine Systemwiederherstellung (Windows) oder Time Machine (macOS) macht nur Sinn, wenn Ihr Euch sicher seid, dass zu dem Zeitpunkt der Sicherung die Infektion noch nicht erfolgt war.

## Schutz vor Ransomware in Windows 11

Windows 11 hat einen eigenen Ransomware-Schutz integriert. Dieser ist nur dann verfügbar, wenn keine Sicherheitssoftware erkannt wird, die diese Funktion übernimmt.

# So geht’s leichter | Stoppt Phishing und Passwortklau




- Klickt auf **Einstellungen** > **Datenschutz und Sicherheit** > **Windows-Sicherheit** > **Viren- & Bedrohungsschutz**
- Dort könnt Ihr in den Einstellungen den **Überwachten Ordnerzugriff** aktivieren. Ihr könnt darin festlegen, welche Ordner überwacht werden sollen und welche Programme in diesen Ordnern Veränderungen an Dateien vornehmen können sollen.
- Das ist kein absoluter Schutz, verringert das Risiko der Verschlüsselung der Daten aber signifikant.

# So geht's leichter | Stoppt Phishing und Passwortklau

## Richtig mit Passwörtern umgehen

Das Hauptrisiko, einer Phishing-Attacke aufzusitzen, ist der Verlust Eurer Zugangsdaten. Wenn ein Angreifer Benutzernamen und Kennwort hat, dann kann er sich am entsprechenden Dienst/der entsprechenden Webseite anmelden und so tun, als sei er Ihr. Mit allen Konsequenzen: Vom Abfluss Eurer Daten, Bestellungen über Euer Konto bis hin zu einem Diebstahl der Identität. Klingt übertrieben? Die Journalistin Tina Groll hat das am eigenen Leib erfahren. Nach einem erst einmal unbemerkten Diebstahl ihrer Identität ist sie am Ende in eine Spirale aus Mahnungen, Vollstreckungsanordnungen und sogar Haftbefehlen gerutscht. Nur, weil Unbekannte nur mit ihrem Namen und ihrem Geburtsdatum ein Konstrukt aus Scheinidentitäten und Wohnadressen bauen und Waren dahin liefern lassen.

Nun stellt Euch vor, Euer E-Mail-Konto wird übernommen. Das, was zur Passwortwiederherstellung von Facebook genutzt wird.

- Hat der Angreifer Zugriff auf das Postfach, dann kann er das Passwort ändern und Euch ausschließen.
- Dann kann er beispielsweise über Facebook eine Passwortrücksetzung anfordern: Die Wiederherstellungs-E-Mail geht ja an das Postfach, auf das er Zugriff hat.
- Mit dem Zugriff auf Euer Facebook-Konto kann er dann alle Anmeldungen an Webseiten verwenden, bei denen Ihr Facebook als Anmeldemethode gewählt habt.

Dieses Horror-Szenario lässt sich beliebig fortsetzen, lässt sich aber vermeiden, wenn Ihr Euch deutlich mehr Gedanken über Eure Passwörter macht, als nur immer einen Zähler zu erhöhen. Hier findet Ihr einige Tipps:

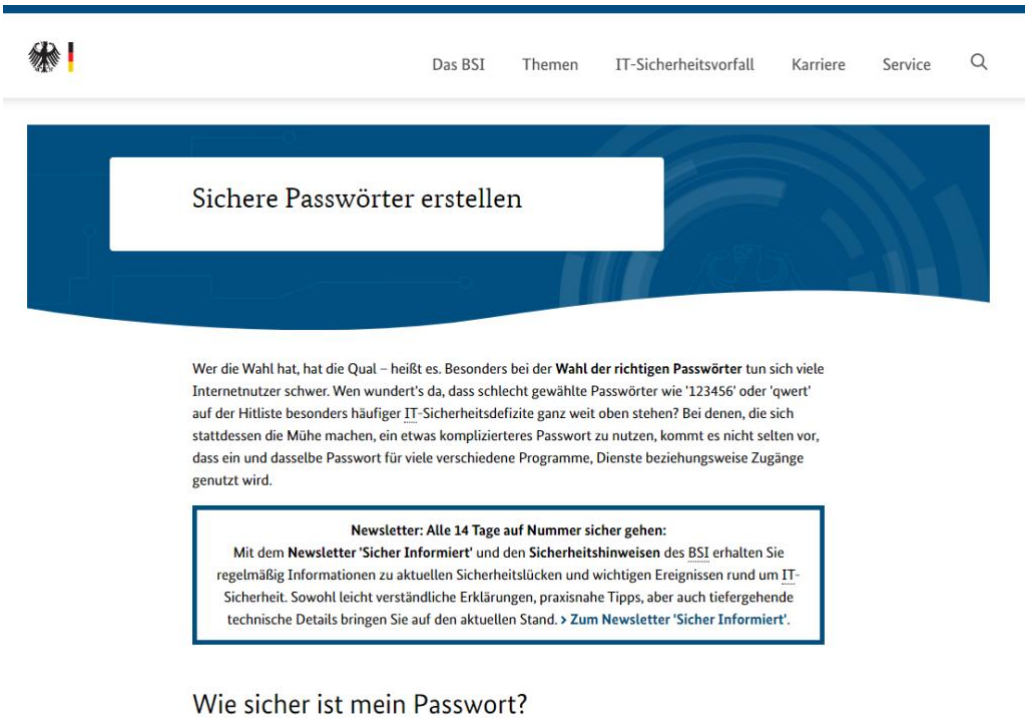
# So geht's leichter | Stoppt Phishing und Passwortklau

## Das sichere Passwort

Eigentlich ist der Begriff irreführend. Ein „sicheres" Passwort ist ebenso theoretisch wie ein Perpetuum Mobile, denn mit genügend Rechenpower und Zeit lässt sich wohl jedes Passwort irgendwann herausfinden. Ihr könnt den Aufwand aber zumindest so hochtreiben, dass die Wahrscheinlichkeit, dass das passiert, gegen null geht.

Was ist nun ein sicheres Passwort? Das Bundesamt für Sicherheit in der Informationstechnik (BSI) gibt unter https://www.bsi-fuer-buerger.de im Bereich **Passwort** einige Hinweise:

1. **Es sollte einfach zu merken sein:** Je schwerer ein Passwort zu merken ist, desto höher ist die Wahrscheinlichkeit, dass Ihr es Euch aufschreibt. Das widerspricht dem Anspruch, dass es nur Euch selbst bekannt sein soll. Das so beliebte kleine, gelbe Post-it als Zwischenspeicher ist eben nicht sicher!



# So geht's leichter | Stoppt Phishing und Passwortklau

2. **Es sollte mindestens 8 Zeichen haben:** Je komplexer es aber wird, desto schwerer wird es zu merken. Das BSI empfiehlt: Lieber ein mäßig komplexes Passwort, dass Ihr Euch merken könnt und nur einmal verwendet, als ein überkomplexes, dass Ihr aufschreibt oder wiederverwendet.

3. **Nutzt Sonderzeichen, Groß- und Kleinschrift und Ziffern:** Je komplexer das Passwort ist, desto schwerer ist es auch herauszubekommen. Wichtig dabei auch:

4. **Verwendete keine über Euch bekannten oder herauszufindenden Daten als Passwort:** Namen von Familienmitgliedern, Haustieren, Freunden, Geburtstage, Hochzeitstage etc. eignen sich nicht als Passwort. Auch keine Wörter, die in einem Wörterbuch vorkommen, oder Zeichen- oder Ziffernfolgen, die auf- oder absteigend sind wie *123456* oder *abcdef*.

Verliert nicht den Mut: Diese Anforderungen lassen sich tatsächlich umsetzen.

- Passwörter müssen nicht lesbar sein oder aus tatsächlich vorhandenen Begriffen bestehen, damit Ihr Euch daran erinnern können.

- Der Ausgangspunkt zu einem guten Passwort kann beispielsweise ein für Euch ganz persönlich leicht zu merkender Satz oder eine Zeile aus einem Lied. „Ich habe im Sommer 2022 den Motorradführerschein gemacht!" beschreibt ein Ereignis, an das Ihr Euch sicherlich noch lange erinnern werden.

- Nehmt davon nur die Anfangsbuchstaben (unter Beachtung der Groß- und Kleinschrift) und lasst die Ziffern und Satzzeichen an

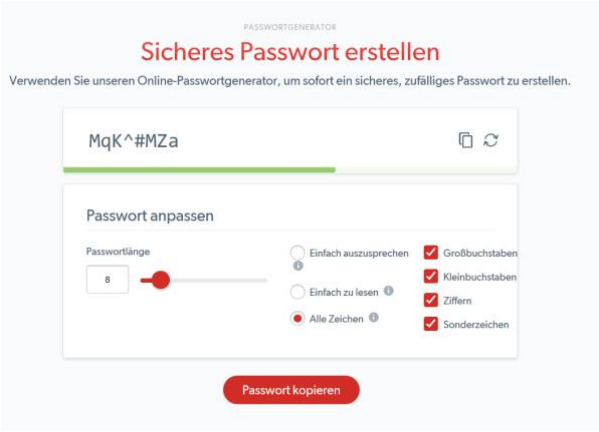
# So geht's leichter | Stoppt Phishing und Passwortklau

ihrem Platz, und schon habt Ihr *IhiS2022dMg!* als Passwort. Dieses Passwort errät niemand, der nicht den speziellen Satz kennt.

- Wichtig ist, dass Ihr möglichst kein Passwort zweimal verwendet. Ihr habt nachher keinen Überblick mehr, bei welchen Shops und Webseiten Ihr ein Konto angelegt habt.
- Wenn Ihr tatsächlich nur einmal dort bestellen wollt, dann nehmt Euch ein Einmalpasswort. iOS und macOS schlagen das direkt vor. Einmalpasswörter sind so kryptisch, dass niemand darauf kommt.

## Verwendung eines Passwortgenerators

Eine weitere Alternative ist die Verwendung eines Passwortgenerators, also eines Programms bzw. einer Webseite, die nach bestimmten Vorgaben sicher Passwörter generiert. Kostenlos findet Ihr dies beispielsweise unter https://www.lastpass.co/de/password-generator




Wählt die gewünschte **Passwortlänge** ein, wählt, ob **Großbuchstaben**, **Kleinbuchstaben**, **Ziffern** und/oder **Sonderzeichen** verwendet werden sollen. Auf Wunsch könnt Ihr dann das Passwort noch für das **Lesen** oder **Sprechen** optimieren, diese Einstellungen beeinflussen die Verwendung von Sonderzeichen bzw. leicht verwechselbaren Zeichen im Passwort.

# So geht's leichter | Stoppt Phishing und Passwortklau

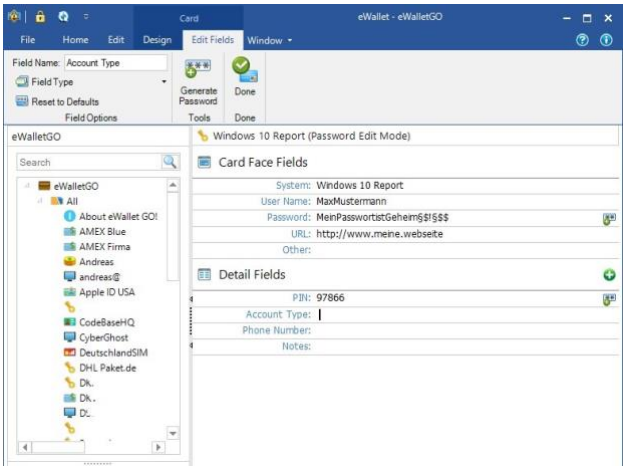
Aus LastPass könnt Ihr das Kennwort dann über das Symbol mit den beiden Seiten oben rechts in die **Zwischenablage** kopieren und vor dort aus weiterverwenden.

## Speichern von Passwörtern in einem Safe

Es bedarf keiner langen Erklärung, dass das Aufschreiben von Passwörtern keine wirklich gute Idee ist. Auch wenn es kaum zu glauben ist: Viele erfolgreiche Angriffe auf Systeme kommen nicht über einen technischen Einbruch über das Internet oder interne Netzwerk, sondern über kleine, gelbe Klebezettelchen, auf denen Anwender ihre Passwörter aufschreiben und „ganz geheim" am Monitor oder unter der Schreibtischauflage verstecken. Auch eine Excel-Tabelle ist nur eine bedingt gute Idee!

Natürlich fordert Euch der Anspruch, komplexe und unterschiedliche Passwörter zu verwenden und sich diese auch noch zu merken, aber auch dafür gibt es sichere Lösungen: Die sogenannten Passwortsafes.

Dies sind Programme, in denen Ihr Eure Passwörter speichern könnt und die die Datei, in denen diese abgelegt werden, verschlüsselt und so vor unberechtigtem Zugriff schützt.




Bekannte Passwort-Safes sind zum Beispiel 1Password (https://1password.com) und KeePass (https://keepass.info). Wenn Ihr mit verschiedenen Plattformen auf Desktop,

# So geht’s leichter | Stoppt Phishing und Passwortklau

Tablet und Smartphone arbeiten, dann ist Ilium´s eWallet (https://www.iliumsoft.com/) eine gute Wahl.

eWallet bietet die Synchronisation der (256bit-verschlüsselten) Passwortdatei mit verschiedenen Online-Speichern an und hat für alle großen Plattformen (Windows, macOS, iOS, Android) einen entsprechenden Client. Diese kosten zwar jeweils knapp EUR 10,-, lösen aber die Herausforderung, dass Ihr die Passwörter synchron halten und von überall her darauf zugreifen können.  Eine einmal eingegebene Passwort-Karte ist nach Beendigung des Speichervorgangs sofort auf den anderen Geräten verfügbar, bei Änderungen verhält es sich ebenso.

## Passwörter regelmäßig checken

Immer wieder kommen Datenlecks und -pannen in die Nachrichten: Durch Sicherheitsvorfälle werden E-Mail-Adressen, Nutzernamen und Passwörter gestohlen und im Internet verkauft. Der Käufer hat dann so lange theoretisch Zugriff auf all Eure Benutzerkonten, wie Ihr das Passwort nicht geändert habt.


Die bekanntesten Sicherheitsvorfälle (zumindest die, die bekannt geworden sind), sind auf der Seite https://haveibeenpwned.com/ zusammengefasst. Dort könnt Ihr nach Eingabe Eures Passwortes sehen, ob und bei welchem Hack Eure Zugangsdaten erbeutet wurden.

Wenn Ihr betroffen seid, dann ändert so schnell wie möglich das Passwort, und wiederholt dies häufiger.

# So geht's leichter | Stoppt Phishing und Passwortklau

Wenn Ihr ein neues Passwort vergeben wollt, dann könnt Ihr dieses auf der Webseite https://checkdeinpasswort.de überprüfen lassen. Die berechnet, wie lange ein herkömmlicher PC brauchen würde, um dieses durch Berechnungen und stumpfes Ausprobieren zu erraten.

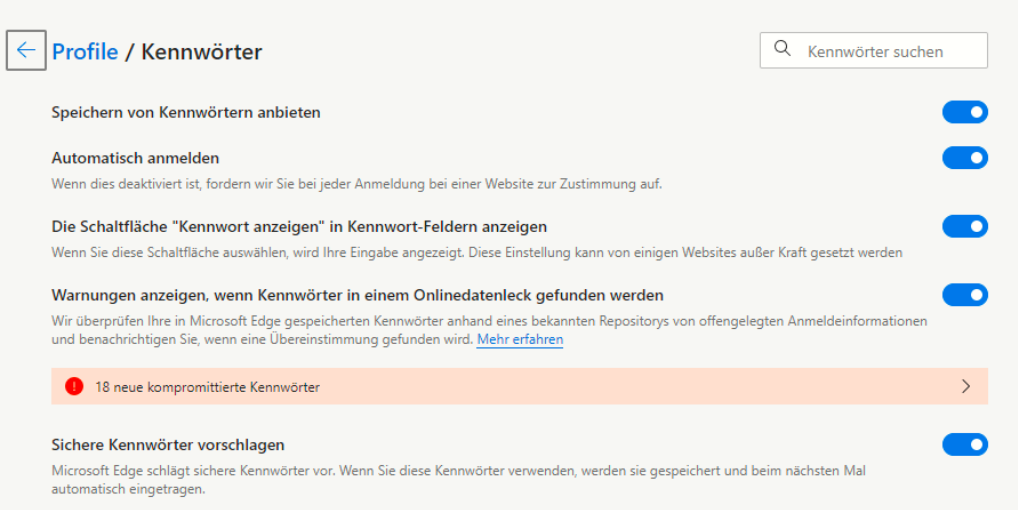

## Passwörter in Edge überprüfen lassen

Kennwörter sind immer noch der Kern der Sicherung der Zugänge zu Webseiten, Online-Konten und anderen Diensten. Das bringt mit sich, dass die Zugangsdaten auf allen möglichen Servern gespeichert sind. Werden durch Sicherheitslücken diese Daten Angreifern verfügbar gemacht, dann sind die Login-Daten schnell in Datenbanken wie Collection #1 frei verfügbar. Gerade bei nicht häufig genutzten Konten denkt Ihr oft nicht an dieses Risiko. Lasst Euch durch Microsoft Edge unterstützen!

- In den aktuellen Versionen von Edge bekommt Ihr beim ersten Start die Nachfrage angezeigt, ob Ihr Eure Kennwörter schützen wollt.

# So geht's leichter | Stoppt Phishing und Passwortklau

- Wenn Ihr dies aktivieren wollt, dann führt der Browser bei jeder Anmeldung an eine Webseite eine Überprüfung durch, ob Benutzername/ Kennwort in einem Datenleck gefunden wurde.
- Klickt auf **Kennwortschutz an**, um die Funktion zu aktivieren.




- Wenn Ihr das nachträglich machen wollt, dann klickt in Edge auf die **drei Punkte** oben rechts, dann auf **Einstellungen** > **Profile** > **Kennwörter** und aktiviert **Warnungen anzeigen, wenn Kennwörter in einem Onlinedatenleck gefunden werden**.

Ein solcher Hinweis sagt nicht zwingend aus, dass das Konto, an Ihr Euch gerade anmeldet, kompromittiert ist. Allerdings wurde die Kombination Benutzername/Kennwort in einem Leck gefunden. Ihr solltet die Zugangsdaten also umgehend ändern.

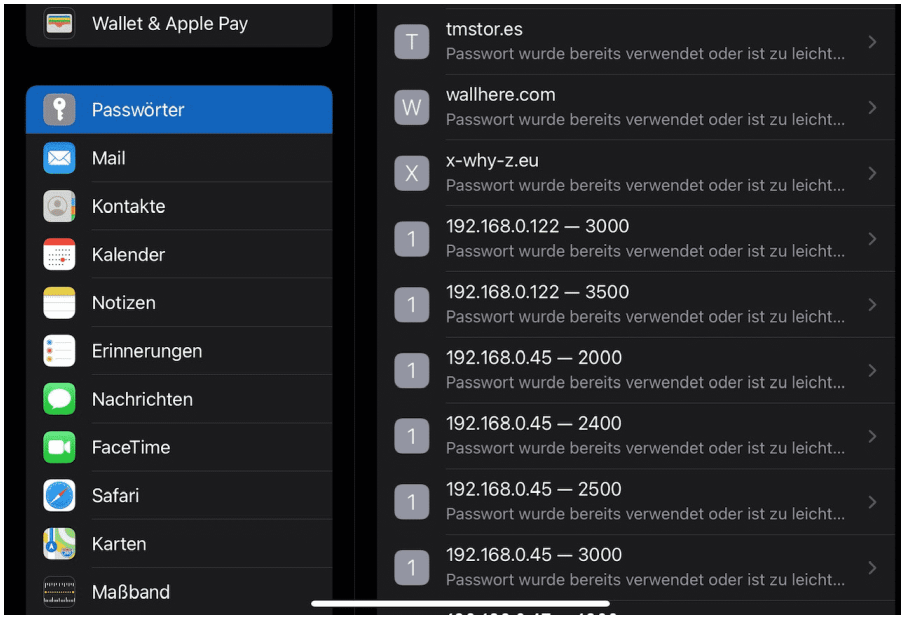
## Passwortcheck in iOS

So schön es ist, dass immer mehr Dinge online auch mit dem Smartphone durchgeführt werden können, einen Nebeneffekt hat das Ganze: Ihr müsst immer mehr Benutzerkonten anlegen und dafür natürlich auch Passwörter vergeben. iOS 15 bietet hier eine zentrale

# So geht’s leichter | Stoppt Phishing und Passwortklau

Stelle, an der die entstehenden Risiken kontrolliert und verringert werden können.

iOS speichert die Passwörter im Schlüsselbund. Das ist die interne, sichere Passwort-Datenbank von iOS.




- Unter **Einstellungen** > **Passwörter** findet Ihr direkt die Informationen zu den Konten/Webseiten, den verwendeten Passwörtern und der Bewertung, warum das Passwort nicht geeignet scheint oder ein Risiko beinhaltet.
- Tippt auf einen Eintrag, dann könnt Ihr direkt auf die Webseite wechseln, um das Kennwort zu ändern.
- Alternativ könnt Ihr das Passwort aus dem Schlüsselbund löschen. Das macht Sinn, wenn das Konto bereits gelöscht oder nicht mehr in Benutzung ist.

# So geht's leichter | Stoppt Phishing und Passwortklau

## Besser doppelt: Zwei-Faktor-Authentifizierung

Mit Netz und doppeltem Boden, das ist die klassische Absicherung in vielen Bereichen des täglichen Lebens. Eine alleinige Kombination aus Benutzername und Passwort ist anfällig:  Kommt ein Fremder in deren Besitz, weil er sie aus einem Datenleck bekommen, von Euren Fingern abgelesen oder erraten hat, dann kommt er ohne weitere Schritte an das betroffene Konto.

Eine Lösung ist die Zwei-Faktor-Authentifizierung (2FA). Hier unterscheidet man bei den Schutzmaßnahmen in **Wissen** und **Besitz**. Eine Kombination von Benutzername und Passwort fällt in den Bereich Wissen: Wer sich anmelden will, muss diese wissen. Eine Anmeldung ist von jedem Ort der Welt möglich, unabhängig davon, ob Ihr es seid.

Der zweite Faktor sollte also anders beschaffen sein. Man setzt gerne eine zweite Authentifizierungsschicht ein, die den Besitz von etwas voraussetzt. Beispielsweise die SMS eines Zahlencodes an eine vordefinierte Telefonnummer oder ein sogenanntes Token, das eine ständig wechselnde Zahlenkombination anzeigt. Nach der Anmeldung mit Benutzername und Passwort müsst Ihr dann noch diesen Zahlencode eingeben.


Für eine erfolgreiche Anmeldung müsst Ihr also nicht nur die Zugangsdaten **kennen**, sondern zusätzlich auch noch das Smartphone oder Token **besitzen**, in der Hand haben. Ist das eine kompromittiert,

# So geht's leichter | Stoppt Phishing und Passwortklau

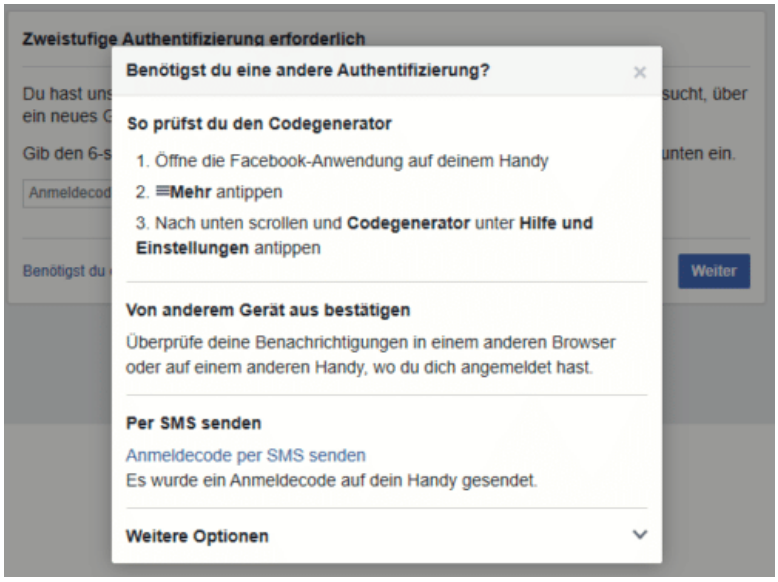
dann hilft das dem Dieb oder Finder nicht. Erst beide Informationen erlauben den Zugriff auf das so geschützte Konto.

## 2FA bei Facebook

Facebook trifft es immer wieder hart. Oder besser: Die Benutzer trifft es hart. Datenlecks, offen zugängliche Passwörter, Sicherheit sind offensichtlich kein Unternehmensziel. Es macht also Sinn, das selber in die Hand zu nehmen. Facebook bietet die Möglichkeit der Zwei-Faktor-Authentifizierung (2FA). Kommt ein Unbefugter an das Passwort, dann kann er damit nichts anfangen, denn zur Anmeldung wird dann ein immer wieder wechselnder Code angefordert. Die Einrichtung geht schnell und einfach.

- Unter **Einstellungen** > **Sicherheit und Login** könnt Ihr die Zwei-Faktor-Authentifizierung **unter Zweistufige Authentifizierung** einschalten.
- Im Standard versucht Facebook, Euch von der Verwendung einer Authenticator-App zu überzeugen: Diese kann auf Eurem Smartphone installiert werden und zeigt dann immer den richtigen Code an.
- Unabhängiger seid Ihr, wenn Ihr Euch den Code per SMS schicken lassen. Wenn die Facebook-Anmeldung (auf der Webseite oder der App) den Code abfragt, dann klickt auf **Benötigst Du eine andere Authentifizierung**.

# So geht’s leichter | Stoppt Phishing und Passwortklau




- Ein Klick auf **Anmeldecode per SMS** senden löst dann eine SMS mit dem Anmeldecode an die Eurem Konto hinterlegte Handynummer aus.

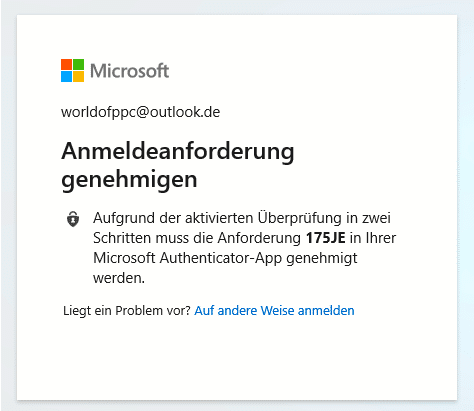
## 2FA bei Outlook

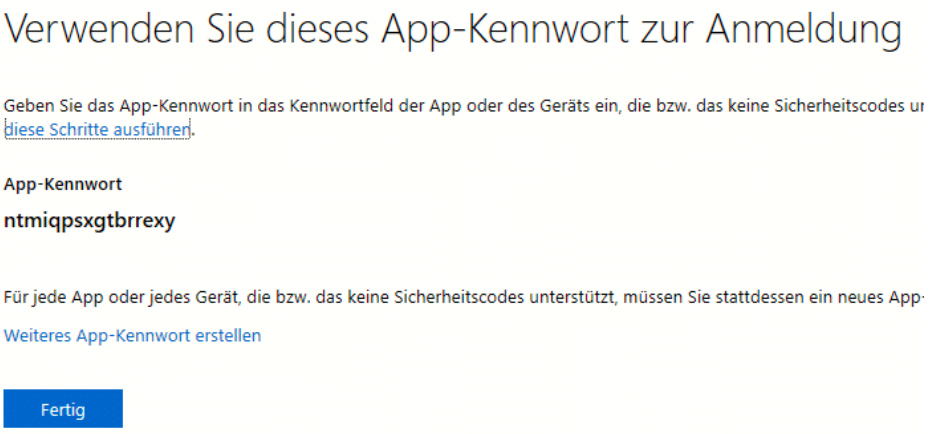
Die Zwei-Faktor-Authentifizierung funktioniert wunderbar, wenn der Zugriff über den Webbrowser stattfindet. Greift Ihr aber mit einem Programm auf das Outlook-Postfach zu, dann kann das Vorgehen von Programm zu Programm abweichen. In der Regel trefft Ihr dabei aber nur auf zwei Möglichkeiten. Einmal eingerichtet, ist auch die Mail-Abfrage auf dem PC abgesichert.

- Im idealen Fall ist Eure E-Mail-Software in der Lage, mit der Anforderung eines zweiten Faktors direkt umzugehen und sie zu verarbeiten. Outlook 2016 und 365 wie auch die interne E-Mail-App gehören dazu.

# So geht’s leichter | Stoppt Phishing und Passwortklau

- Bei den aktuellen Versionen von Windows wird der Authentifizierungscode der App nur einmalig abgefragt. Direkt danach schaltet sich Windows Hello ein und fordert einmalig die Anmeldung über eine der in Windows hinterlegten Methoden (wie Fingerabdruck, Gesicht oder Token) an. Wenn Ihr die ausgeführt habt, dann wird Windows Hello bei jeder Anmeldung am Postfach als zweiter Faktor verwendet. Deutlich bequemer, als wenn Ihr immer Codes eingeben müssen!




- Ältere Versionen von Outlook, Smartphones und andere Programme, die nicht nativ den zweiten Faktor bei der Anmeldung anfordern können, könnt Ihr austricksen.
- Wechselt wieder in die Sicherheitseinstellungen des Microsoft-Kontos und klickt auf **Zusätzliche Sicherheitsoptionen**.

# So geht's leichter | Stoppt Phishing und Passwortklau

- Unter App-Kennwörter könnt Ihr ein **zufälliges App-Kennwort** erzeugen. Das besteht aus einer Kombination aus dem Passwort und einem zufälligen Code. Es ist weder lesbar noch von einem Fremden zu erraten.
- Gebt dieses Kennwort statt des Kontokennwortes ein. Das E-Mail-Programm fragt nicht mehr nach dem zweiten Faktor, ein Fremder, der nur Euer eigentliches Passwort hat, kommt aber nicht an die E-Mails.

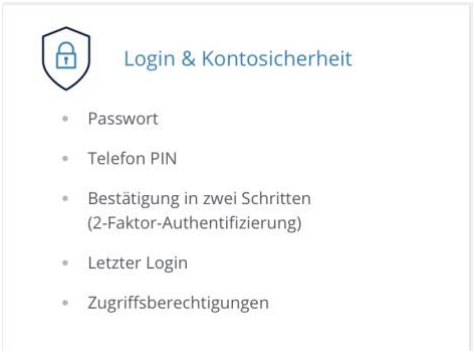
## 2FA bei Microsoft 365

- Ruft die Admin-Seite von Office 365 auf, dann klickt auf **Benutzer**.
- Setzt einen Haken bei dem Benutzer, den Ihr anpassen wollt und klickt ihn an.
- Unten rechts klickt dann auf **Mehrstufige Authentifizierung**. Office 365 öffnet den Benutzer und erlaubt unten rechts die Aktivierung der **Mehrstufigen Authentifizierung**.
- Bei jeder Anmeldung müsst Ihr nun neben dem Passwort einen Code eingeben. Diesen bekommt Ihr entweder per SMS, per E-Mail oder über die Microsoft Authenticator-App.

# So geht’s leichter | Stoppt Phishing und Passwortklau

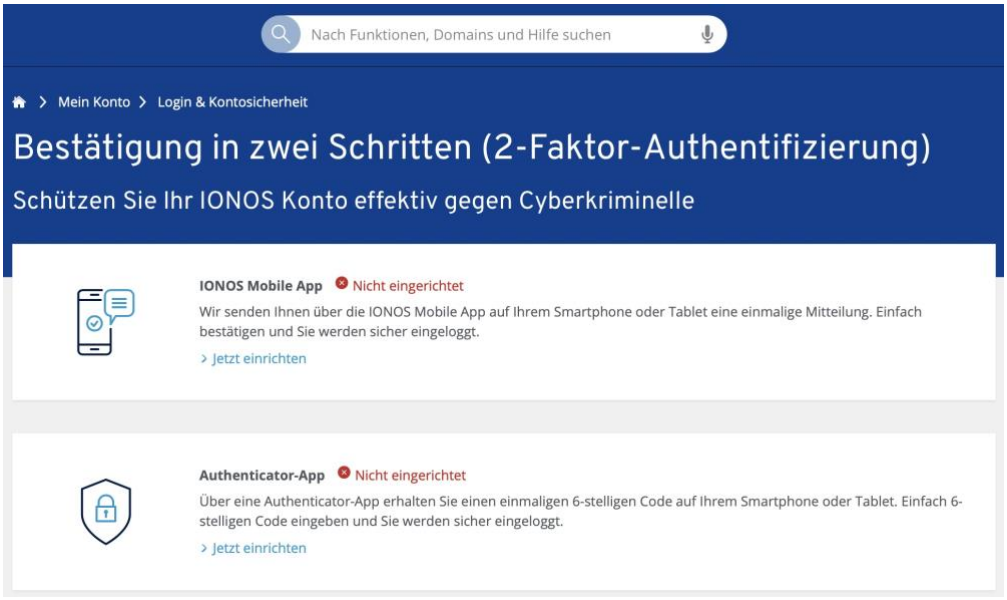
## 2FA für Webseiten

Passwort-Leaks, Phishing-Attacken, Social Engineering, die Möglichkeiten, das Passwort an Übeltäter zu verlieren, sind unzählbar. Das ist bei E-Mail- und Dienstkonten schon eine Katastrophe, bei einer Webseite sind die Auswirkungen noch einmal andere. Das Defacing, das Ersetzen der Inhalte der Seite durch Nachrichten der "Eroberer", hat eine direkte Außenwirkung. Dieser Fall kann eintreten, wenn ein Angreifer die Zugangsdaten erbeutet. Das Anmelden am Hosting-Konto und das Ändern der FTP- oder Wordpress-Zugangsdaten ist dann ein Klacks. IONOS/1&1 als einer der verbreitetsten Hoster bietet als Schutz dagegen die Zwei-Faktor-Authentifizierung bei der Anmeldung an die Administrationskonten an.




- Um die einzurichten, meldet Euch (noch nur mit dem Passwort) an der Admin-Oberfläche an und klickt dann auf **Euren Namen** > **Mein IONOS** > **Login & Kontosicherheit** > **Bestätigung in zwei Schritten**.

# So geht’s leichter | Stoppt Phishing und Passwortklau

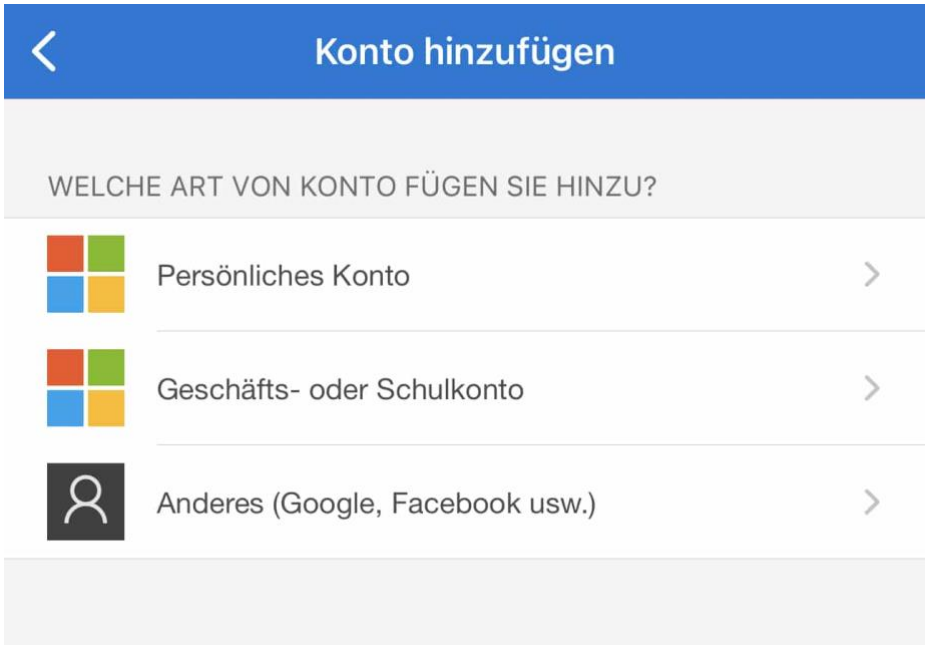



- IONOS bietet zwei verschiedene Möglichkeiten für den zweiten Faktor an: Zum einen die IONOS Mobile App, die unter anderem auch Einstellungen zum Hostingkonto erlaubt.
- Die zweite Möglichkeit ist die Verwendung einer normalen Authenticator-App, die dann auch für andere Konten verwendet werden kann.
- Egal, welche der beiden Lösungen gewählt wird: Nach Eingabe des Passwortes fordert die Admin-Konsole von IONOS/1&1 dann die Ziffernfolge ab, die die installierte App gerade anzeigt. Wer Euer Smartphone nicht in seinem Besitz hat, der bleibt außen vor!

## Authenticator-Apps

Weitere Alternativen zu SMS oder E-Mail als zweitem Faktor sind die kostenlose Authenticator-App von Microsoft und der ebenfalls kostenlose Google Authenticator, denn die benötigen im Vergleich zu SMS oder E-Mail keine Datenverbindung!

# So geht’s leichter | Stoppt Phishing und Passwortklau




- Nach Installation der App könnt Ihr Eure Microsoft-Konten, aber auch diverse Konten von anderen Anbietern (wie Facebook, Google, GMX etc.) einbinden.
- Dazu scannt den vom Anbieter für die Authenticator-App angegebenen Barcode in der Kontokonfiguration unter **Zwei-Faktor-Authentifizierung**.
- Das Konto erscheint dann in der App und zeigt bei Auswahl den jeweils aktuellen Code an, der nach Eingabe des Passwortes bei der Anmeldung in einem separaten Fenster eingegeben werden muss.

Beim Google Authenticator gibt es noch eine Besonderheit: Wenn Ihr das Telefon wechselt, dann müsst Ihr die eingerichteten Konten nicht manuell übertragen, sondern könnt das über einen automatisierten Prozess machen.

# So geht’s leichter | Stoppt Phishing und Passwortklau

- Klickt in der App oben rechts auf die drei Punkte und dann auf **Konten übertragen**.
- Die App erzeugt einen QR-Code, den Ihr mit der App auf dem neuen Handy scannen müsst.
- Auf dem neuen Handy tippt nach der Installation auf **Konten importieren > QR Code scannen**.
- Die Konten werden nun automatisiert übertragen und sind direkt nutzbar. Einzige Voraussetzung: Die Mobilfunknummer in beiden Geräten muss dieselbe sein!