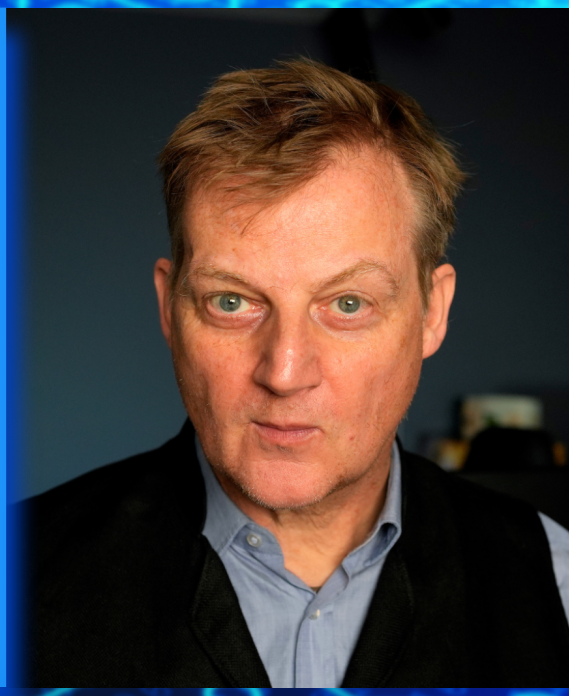
So geht's leichter...



Enkeltrick & Co: Schützt Euch!

- So funktionieren Enkeltricks
- Die Maschen der Betrüger erkennen
- Phishing erkenne und abwehren
- Trainiert Eure Fähigkeiten
- Sicherheit und Passwort ABC

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 | Enkeltrick&Co: Schützt Euch!

Inhalt

DEU 09:00 Schieb.de

So geht's leichter | Enkeltrick&Co: Schützt Euch!

DEU 09:00 Schieb.de

So geht’s leichter | Enkeltrick&Co: Schützt Euch!

Enkeltrick & Co.: Schützt Euch!

Der Enkeltrick ist eine betrügerische Masche, die seit vielen Jahren, vor allem in Deutschland, aber auch in anderen Ländern für Schlagzeilen sorgt. Ziel des Betrugs ist es, meist ältere Menschen um ihr Geld oder ihre Wertsachen zu bringen.

Die Täter gehen dabei psychologisch raffiniert vor: Sie rufen bei ihren Opfern an, geben sich als deren Enkel oder andere nahestehende Personen aus und behaupten, in einer Notsituation zu stecken. Sie bitten um Geld, oft mit dem Versprechen, es schnellstmöglich zurückzuzahlen.

Der Trick ist dabei die Erzeugung eines emotionalen Drucks. Die Anrufer spielen auf die Hilfsbereitschaft und das Vertrauen der Senioren an und setzen sie unter Zeitdruck.

Sie erzählen beispielsweise, dass sie einen schweren Unfall hatten, eine hohe Kaution zahlen müssen oder eine dringende Investition tätigen wollen, für die schnell Geld benötigt wird. Die Betrüger sind häufig so überzeugend, dass viele der Angerufenen nicht den Verdacht schöpfen, es könnte sich um einen Betrug handeln.

Typischerweise wird das Opfer angehalten, das Geld einem Boten zu übergeben, der angeblich im Auftrag des vermeintlichen Familienmitglieds handelt. Auf diese Weise hinterlässt der Täter selbst keine Spuren.

Der Enkeltrick ist ein klassisches Beispiel dafür, wie Betrüger die Schwächen des menschlichen Verhaltens ausnutzen, insbesondere das Vertrauen in Familienmitglieder und die Bereitschaft, in Notfällen zu helfen.

DEU 09:00 Schieb.de

So geht’s leichter | Enkeltrick&Co: Schützt Euch!

Es ist ein ernstes Thema, das zeigt, wie wichtig Aufklärung, insbesondere unter älteren Menschen, über solche Betrugsmethoden ist. Banken, Polizei und Verbraucherzentralen warnen regelmäßig vor dieser Form des Betrugs und raten zu Misstrauen bei Geldforderungen am Telefon.

Zwar hat es schon immer Betrug gegeben, auch an der Haustür, doch durch Internet und moderne Kommunikation wie Messenger bekommen die Betrüger neue Möglichkeiten an die Hand. Wir kommunizieren kaum noch von Angesicht zu Angesicht. Was auf der einen Seite das Leben deutlich vereinfacht, weil wir mit Menschen in Nah und Fern kommunizieren können, erleichtert auf der anderen Seite leider auch Betrügern das Umsetzen ihrer perfiden Maschen.

DEU 09:00 Schieb.de

So geht’s leichter | Enkeltrick&Co: Schützt Euch!

Das verborgene Netz der Täuschung: Wenn Betrüger anklopfen

In der schillernden Welt des Internets, wo sich Möglichkeiten und Wunder praktisch hinter jeder Ecke verbergen, gibt es auch jene dunklen Gassen, die uns vor Herausforderungen stellen.

Diese Gassen sind nicht immer sofort sichtbar, und oft sind sie kunstvoll mit den leuchtenden Pfaden des Netzes verwoben. Sie führen uns in die Welt der Internet-Abzocke, wo geschickte Betrüger ihre Netze auswerfen, um ahnungslose Opfer zu fangen.

Es ist faszinierend und zugleich beunruhigend, wie einfallsreich und überzeugend diese Betrüger sein können. Sie nutzen unsere Neugier, unser Mitleid und manchmal auch unsere Ängste, um uns in ihre Falle zu locken.

Oft beginnt es mit einer unschuldig wirkenden Nachricht oder einem Anruf. Ein vermeintlicher Enkel in Not, ein verlockendes Geschäftsangebot oder eine dringende Warnung vor einem angeblichen Virus auf unserem Computer.

Die Maschen dieser Betrüger sind vielfältig, und sie alle haben eines gemeinsam: Sie setzen ihre Opfer unter Druck, oft durch Vortäuschung falscher Tatsachen, um sie zur Herausgabe von Geld oder wertvollen Informationen zu bewegen. Doch wie bei jedem Rätsel gibt es auch hier Schlüssel zum Verständnis. Mit Wissen und Achtsamkeit können wir uns schützen und sicher durch die digitale Welt navigieren.

DEU 09:00 Schieb.de

So geht’s leichter | Enkeltrick&Co: Schützt Euch!

Bevor wir uns tiefer in dieses Labyrinth der Täuschungen begeben, ist es wichtig zu verstehen, dass es nicht immer die Unwissenheit ist, die Menschen zu Opfern macht.

Es ist vielmehr oft die geschickte Manipulation von Emotionen und die schnelle, drängende Art der Betrüger, die selbst den Klügsten von uns in die Irre führen kann.

Doch keine Sorge, gemeinsam werden wir die Tricks dieser Betrüger entschlüsseln und lernen, wie wir uns vor ihnen schützen können. Begleiten Sie mich auf dieser Reise ins Innere des verborgenen Netzes der Täuschung. Es ist Zeit, Licht ins Dunkel zu bringen.

DEU 09:00 Schieb.de

So geht's leichter | Enkeltrick&Co: Schützt Euch!

Das kann sehr schnell zu sehr unschönen Ergebnissen führen: Ihr gebt Informationen über euch preis, die nur für die echte Person (und nicht für die Allgemeinheit) gedacht sind, und die ein Betrüger verwenden kann, um Schaden anzurichten.

Das muss nicht sein: Gegen den Enkeltrick und Co. gibt es genügend Mittel, die ihr leicht anwenden könnt, um nicht darauf reinzufallen!

Enkeltrick und „echte" Freunde

Der sogenannte „Enkeltrick" existiert schon seit vielen Jahren. Sein Name kommt daher, dass am Anfang dieser Masche vor allem ältere Menschen angegriffen wurden: Der Enkel ruft die Oma an (bei der die Anrede weniger unterschiedlich ist bei den Eltern, wo Mama, Mutti, Mutsch und alle möglichen andren Kombinationen möglich sind).

So geht’s leichter | Enkeltrick&Co: Schützt Euch!

Enkeltrick im Netz: Eine moderne Variante eines alten Betrugs

Der Enkeltrick ist eine bekannte Betrugsmasche, bei der sich Betrüger am Telefon als Verwandte oder Freunde ausgeben und ältere Menschen um Geld bitten. Im Zeitalter des Internets hat dieser Trick jedoch eine neue Form angenommen. Hier ist eine anschauliche Erklärung, wie der Enkeltrick im Netz funktioniert:

1. Identitätsdiebstahl auf Social Media: Die Betrüger beginnen oft, indem sie Profile von jüngeren Familienmitgliedern auf sozialen Netzwerken wie Facebook oder Instagram ausspionieren. Sie sammeln Informationen wie Fotos, Namen, Geburtstage und andere Details, die ihnen helfen, sich überzeugend als das Familienmitglied auszugeben.

2. Erstellen eines gefälschten Profils: Mit den gesammelten Informationen erstellen die Betrüger ein neues, gefälschtes Profil, das dem echten Profil des Familienmitglieds sehr ähnlich sieht. Sie können auch versuchen, das echte Profil zu hacken und direkt von dort aus zu agieren.

3. Kontakt mit dem Opfer aufnehmen: Die Betrüger nehmen über das gefälschte Profil Kontakt zum älteren Familienmitglied (dem Opfer) auf, oft per Direktnachricht. Sie geben vor, in einer Notlage zu sein – z.B. einen Unfall gehabt zu haben, im Ausland festzusitzen oder dringend Geld für eine medizinische Behandlung zu benötigen.

4. Emotionale Manipulation: Die Betrüger spielen auf die Emotionen des Opfers an, betonen, wie dringend sie Hilfe benötigen und dass sie sich schämen, andere um Hilfe zu bitten. Sie betonen oft, dass es ein Geheimnis bleiben muss.

DEU 09:00 Schieb.de

So geht’s leichter | Enkeltrick&Co: Schützt Euch!

5. Geldtransfer: Das Opfer wird dazu gedrängt, Geld zu überweisen, oft über Online-Banking oder über Dienste wie PayPal. Manchmal werden sie auch dazu aufgefordert, Gutscheincodes von Online-Shops zu kaufen und diese weiterzugeben.

6. Schnelle Flucht: Sobald die Betrüger das Geld erhalten haben, brechen sie den Kontakt ab und das gefälschte Profil wird oft gelöscht. Das Opfer bleibt zurück und realisiert erst später, dass es betrogen wurde.

Präventionstipps:

- Seien Sie immer skeptisch, wenn Sie unerwartete Geldanfragen über das Internet erhalten, auch wenn sie von Familienmitgliedern oder Freunden zu kommen scheinen.
- Überprüfen Sie solche Anfragen immer persönlich, indem Sie die betreffende Person direkt anrufen – nutzen Sie dafür nicht die im Nachrichtendienst angegebene Nummer, sondern eine Nummer, die Sie selbst gespeichert haben oder aus einem Verzeichnis entnehmen.
- Schützen Sie Ihre Privatsphäre in sozialen Netzwerken und teilen Sie persönliche Informationen nur mit Personen, denen Sie vertrauen.

Dieser moderne Enkeltrick nutzt die Anonymität des Internets und die Naivität vieler Menschen, insbesondere älterer Menschen, die nicht so vertraut mit den Gefahren des Internets sind. Es ist wichtig, stets wachsam zu sein und Informationen über solche Betrugsmaschen weiterzugeben, um andere zu schützen.

Schon von Anfang an geht es um die Informationsgewinnung: Da der Enkeltrick meist kein gezielter Angriff auf eine Person ist, sondern meist

So geht’s leichter | Enkeltrick&Co: Schützt Euch!

allgemeine Quellen wie Telefonverzeichnisse verwendet, meldet der Anrufer sich nicht mit Namen (im Zweifel erfunden), sondern mit einer allgemeinen Phrase wie „Hi, weißt du, wer hier ist?“.

Durch die vertrauliche Anrede und den meist schnell zurückgegebenen Namen ist schon eine Basis für den Verlauf des Gesprächs geschaffen. Der Angerufene denkt, er hat den Enkel/die Enkelin drin.

Und die kann dann schnell weiter ihre Geschichte spinnen: Es ist ein Unfall passiert, eine Sicherheitsleistung ist nötig, damit die Polizei nicht eingeschaltet wird. Oder die Geldbörse ist verloren gegangen und nur noch heute kann die Semestergebühr entrichtet werden.

Oder eine Rechnung ist angeblich überfällig, und wenn diese nicht direkt bezahlt wird, dann kommt die Pfändung. Oft wird der Anruf dann noch unterbrochen und in kurzen Abständen wiederholt. Nur aus dem Grund, dass der Angerufene kaum einen ruhigen Gedanken fassen kann und durch den emotionalen Druck der vermeintlichen Situation nicht nachdenkt und hinterfragt.

Ist der Angerufene weichgekocht, dann geht es ans Eingemachte: Das Geld muss schnell übergeben werden. Das geht aber angeblich nur über eine Mittelsperson. Kein Wunder, der echte Enkel weiß ja gar nichts von seinem Pech!

Als Ziel sollen dann Geld oder Wertgegenstände übergeben werden oder immense Beträge an ausländische Kontonummern oder über sonderbare Zahlungsdienstleister transferiert werden. Wenig überraschend, dass die dann auf Nimmerwiedersehen verschwunden sind!

Der Trick hat Anfang der 2020er-Jahre eine Erweiterung erfahren: Hatte das Schauspiel nicht den gewünschten Erfolg, weil die Angerufenen

So geht’s leichter | Enkeltrick&Co: Schützt Euch!

misstrauisch geworden waren, dann melden sich in einem zweiten Schritt angebliche Polizisten oder Staatsanwälte.

Die haben den betrügerischen Anruf aufgefangen und wollen nun den Betrüger fassen. Natürlich mit Hilfe des Angerufenen, der der Glaubwürdigkeit wegen natürlich mit seinem Vermögen mitspielen werden soll. Das Ergebnis ist natürlich dasselbe: Das Geld ist weg.

Wie kann man darauf hereinfallen?

Wenn man vom Enkeltrick redet, dann ist die erste Reaktion meist “Das ist doch so offensichtlich: Wie kann man darauf hereinfallen?!”. Das mag für den ursprünglichen Enkeltrick gelten, nur entwickelt der sich immer und immer weiter.

Anrufe werden immer weniger, also verlagern sich die Angreifer auf die modernen Kommunikationsmedien: E-Mail, WhatsApp, SMS werden verwendet. Auch Deepfakes, bei denen geklonte Stimmen verwendet werden, die denen der vermeintlichen Opfer täuschend ähnlich sind, kommen immer häufiger vor.

Das Perfide an all diesen Maschen: Die Betrüger erzeugen Situationen, in denen Ihr unter Druck seid und vermeintlich schnell handeln müsst. So schnell, dass der Schreck und der vermeintliche Zeitdruck euer wichtigstes Gegenmittel deaktivieren: Euer Misstrauen.

Vertrauen ist gut, Kontrolle besser

Die allermeisten dieser Maschen könnt ihr in den Griff bekommen, wenn ihr wachsam seid. Dabei geht es gar nicht darum, niemandem mehr zu vertrauen. Und ihr seid auch nicht automatisch leichtsinnig, wenn ihr auf so eine Aktion hereinfallt.

DEU 09:00 Schieb.de

So geht's leichter | Enkeltrick&Co: Schützt Euch!

Wenn ein Familienmitglied in Not zu sein scheint, dann reagieren wir ohne großes Nachdenken. Das ist ein Urinstinkt. Wenn ein Kollege schreibt und einen Link schickt, dann klicken wir darauf, es wird schon wichtig sein.

Dabei ist es so einfach für Angreifer: Das Fälschen einer Absenderadresse in einer E-Mail, das Vorgaukeln einer falschen Telefonnummer in einer SMS, WhatsApp oder einem Anruf ist selbst für Amateure mit der richtigen App schnell gemacht und bietet keinerlei Sicherheit für euch.

Hat der Angreifer einmal Euer Vertrauen erschlichen, dann verleitet er euch leicht dazu, zum Beispiel

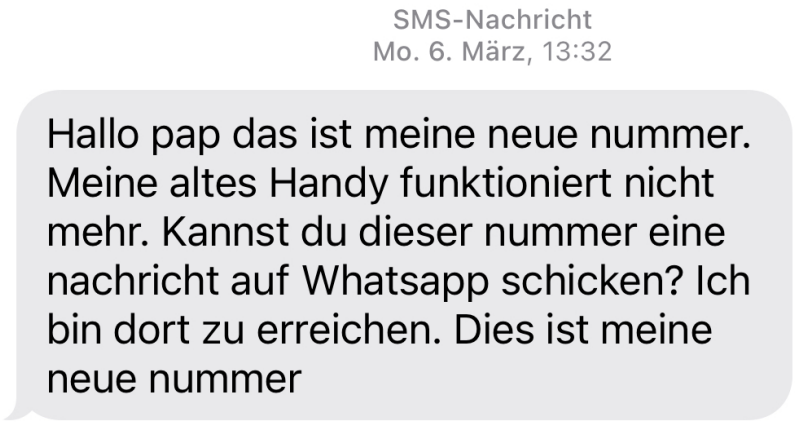
- geheime Daten wie Kontonummern, Vorlieben, Informationen über euer Umfeld preiszugeben,
- auf Links zu klicken und entweder auf Phishing-Seiten eure Benutzerdaten einzugeben oder
- unbewusst Malware herunterzuladen und zu installieren, die dann meist auch wieder Daten ausspäht und weiterleitet.

Mit den so erschlichenen Daten kann er dann in eurem Namen und auf eure Rechnung allen denkbaren Schaden anrichten.

Die neue Telefonnummer

Mittlerweile ein Klassiker: per SMS, iMessage (oder auch WhatsApp und Signal) bekommt Ihr über eine unbekannte Rufnummer die Nachricht, dass ein Familienmitglied eine neue Rufnummer hat. Meist sind es die Kinder oder Enkel, die dann mit „Papa" oder „Oma" für fast alle Opfer eine passende Anrede nutzen.

So geht’s leichter | Enkeltrick&Co: Schützt Euch!



Ihr werdet aufgefordert, die Rufnummer zu speichern. Was einfach geht: Ihr fügt sie einfach dem Kontakt des Kindes/Enkels hinzu. Damit aber passiert Folgendes: Wann immer die Nummer des Betrügers euch kontaktiert, zeigt euer Telefon euch den Namen an. Klar: Ihr habt die Nummer schließlich selbst dem echten Kontakt zugeordnet! Spätestens ab diesem Zeitpunkt glaubt Ihr allen Anrufen und Nachrichten des Betrügers!

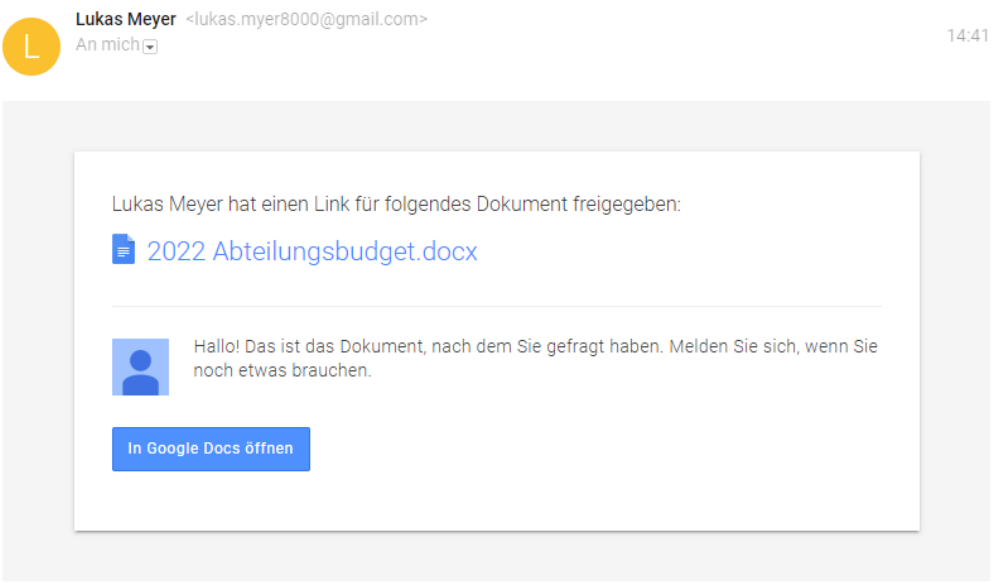
So schützt Ihr euch:

- Die Masche ist so verbreitet, dass ihr bei jeder so aussehenden Nachricht unbedingt den vermeintlichen Absender direkt kontaktieren solltet. Und zwar über einen vertrauenswürdigen Weg: Die bisher bekannte Rufnummer, per E-Mail, persönlich.
- Erst, wenn Ihr sicher seid, dass dieser Rufnummernwechsel wirklich echt ist, ändert die Rufnummer im Kontakt.
- Reagiert nicht auf die Anfrage über die Fake-Nummer!

So geht's leichter | Enkeltrick&Co: Schützt Euch!

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. Wenn dann der Absender auch noch eine gut bekannte Person ist, dann ist schnell Vertrauen hergestellt.



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-

So geht's leichter | Enkeltrick&Co: Schützt Euch!

Mail-Adresse nicht konsequent: Lukas Meyer und lukas.myer8000@gmail.com sind schon auffällig.

- 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, etwa 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 | Enkeltrick&Co: Schützt Euch!

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 einfach 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 | Enkeltrick&Co: Schützt Euch!

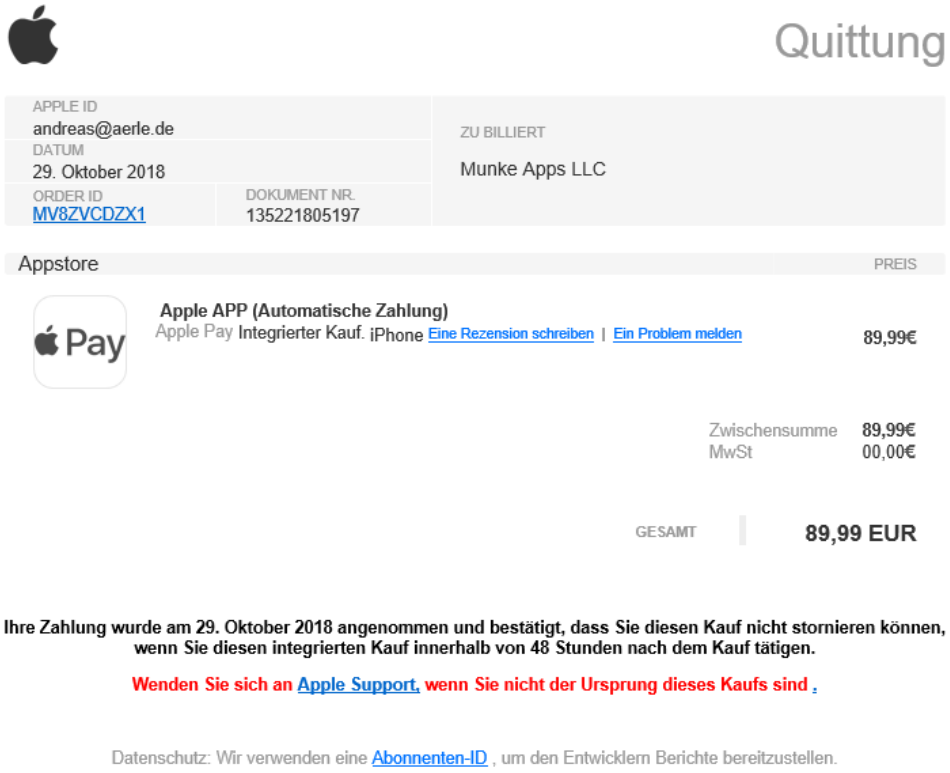
- Auch hier: Kontrolliert den Link, indem Ihr die Maus ohne zu Klicken darüber bewegt. Im Beispiel findet Ihr eine URL, die „mail.ru" enthält. Nie ein gutes Zeichen, und definitiv kein Link, den der echte Dienst nutzen würde.

Angebliche Bestell-E-Mails

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.

DEU 09:00 Schieb.de

So geht's leichter | Enkeltrick&Co: Schützt Euch!



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

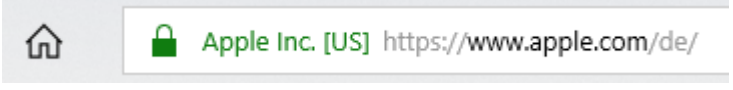
Ihre Zahlung wurde am 29. Oktober 2018 angenommen und bestätigt, dass Sie diesen Kauf nicht stornieren können, wenn Sie diesen integrierten Kauf innerhalb von 48 Stunden nach dem Kauf tätigen.

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.

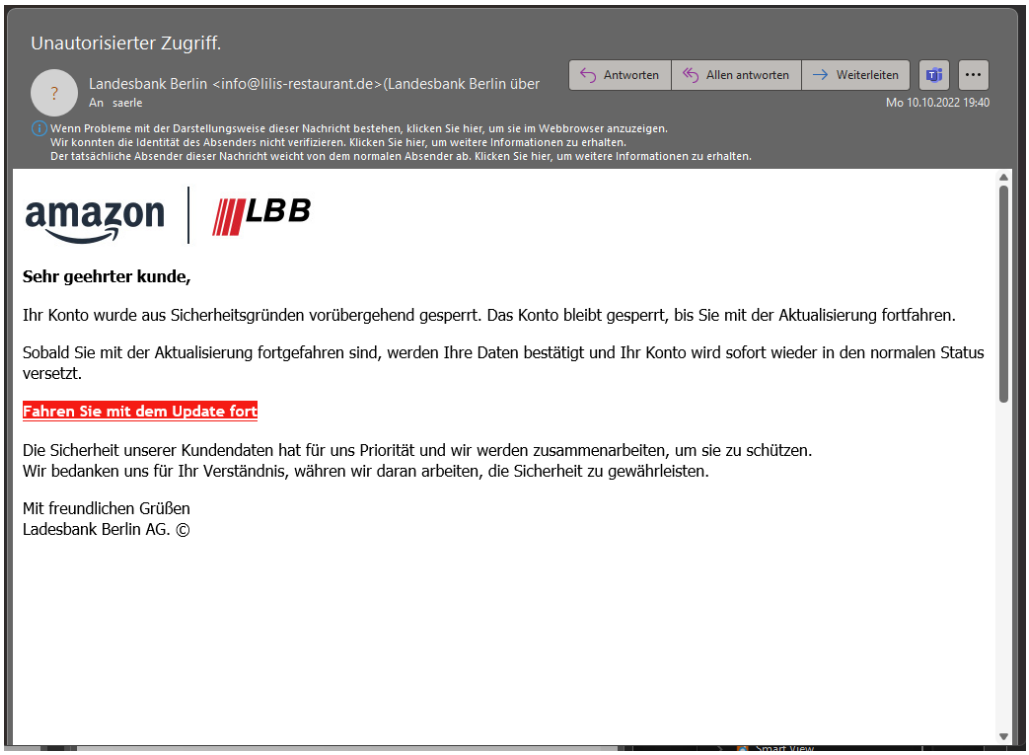


So geht’s leichter | Enkeltrick&Co: Schützt Euch!

- 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 | Enkeltrick&Co: Schützt Euch!

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

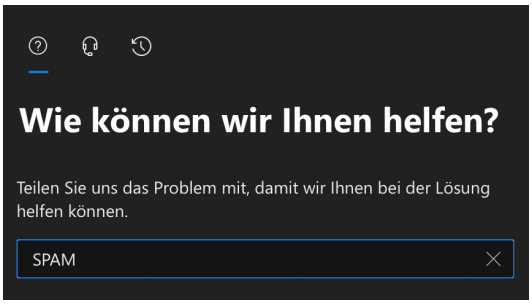
Eine ebenfalls gerne gewählte Masche, Zugriff auf einen fremden Rechner oder die Daten darauf zu bekommen, ist der Anruf eines freundlichen Servicemitarbeiters. In oft gebrochenem Deutsch ist angeblich Microsoft aufgefallen, dass es einen Defekt oder Virenbefall auf Eurem Rechner gibt und man bietet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

So geht’s leichter | Enkeltrick&Co: Schützt Euch!

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:

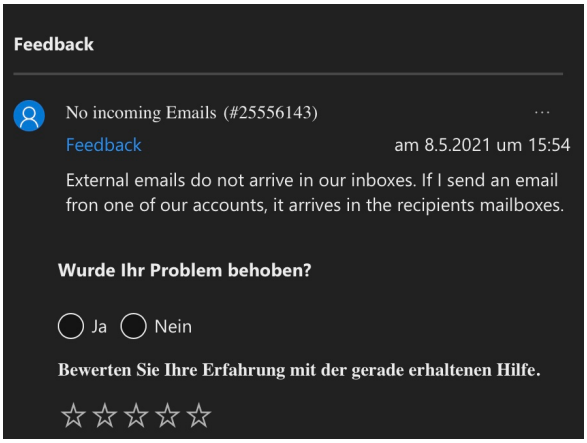
- Gerade im Beispiel von Microsoft ist ein Anruf immer ausgelöst von einem Ticket, das Ihr selbst selber öffnen müsst.



- 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 | Enkeltrick&Co: Schützt Euch!

- Erst dann erfolgt ein Anruf von Microsoft, und wenn Ihr das Ticket zu den deutschen Geschäftszeiten öffnet, 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 schützt Ihr Euch:

So geht’s leichter | Enkeltrick&Co: Schützt 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, 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.

Bei einer Phishing E-Mail geht es nicht darum, Eure Zahlungsinformationen zu validieren, sondern die abzugreifen. Ihr gebt

So geht's leichter | Enkeltrick&Co: Schützt Euch!

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.

Das gesperrte Bankkonto

Gerade wieder aktuell sehr verbreitet: Aufgrund einer ausstehenden Bestätigung eures Kontos bei der Targobank wird Euer Konto angeblich sehr zeitnah (meist im Bereich weniger Tage) gesperrt. Egal, ob ihr ein Konto bei der Targobank habt oder nicht. Diese Betrugsmasche gibt es in zwei Varianten: Entweder sollt ihr einen Link anklicken, der euch dann auf eine Seite schickt, bei der ihr eure Kontoinformationen des Online-Bankings preisgeben sollt. Oder könnt das Ganze mit einer schnell zu leistenden Strafzahlung über EUR 79,95 abwenden. Auch wenn das Erste schlimmer ist als das Zweite, beides ist natürlich totaler Quatsch.

So schützt Ihr Euch:

- Habt Ihr überhaupt ein Konto bei der Bank? Wenn ja, dann meldet Euch nicht über den Link, sondern direkt über die euch bekannte Bank-Website an.

So geht’s leichter | Enkeltrick&Co: Schützt Euch!

- Bei dieser Mail findet Ihr mal wieder den ein oder anderen Tippfehler, auch das Datum der angeblichen Sperrung ist auffällig in einer falschen Schriftart.
- Wenn nein: Ignoriert die Mail einfach vollkommen.

TARGOBANK

Sehr geehrte Kunde,

Aus technischen Sicherheitsgründen war es nötig Ihr Konto zu sperren.

Da Sie den Bestätigungsprozess noch nicht durchlaufen haben, müssen wir seitdem **25.10.2023** alle Benutzerkonten zwischenzeitlich sperren.

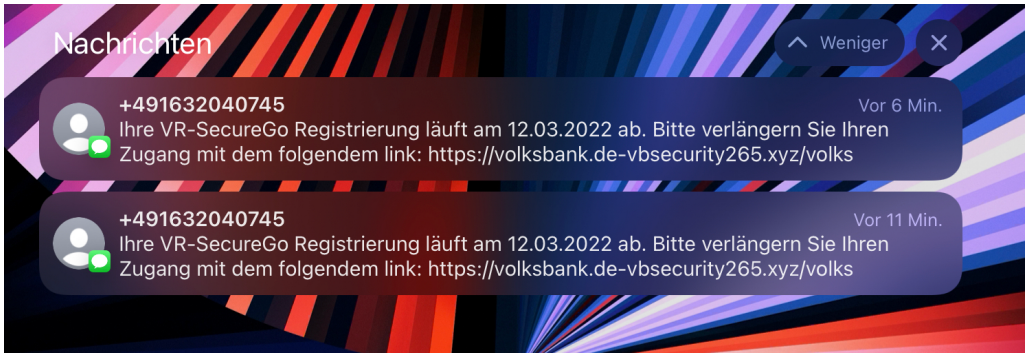
über den nachfolgend angezeigten Button können Sie den Bestätigungsprozess durchlaufen und Ihr Nutzerkonto wieder freischalten. Dieser Vorgang ist selbstverständlich kostenlos.

https://meine.targobank.de/

Phishing in sozialen Netzwerken/Messengern

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

So geht’s leichter | Enkeltrick&Co: Schützt Euch!

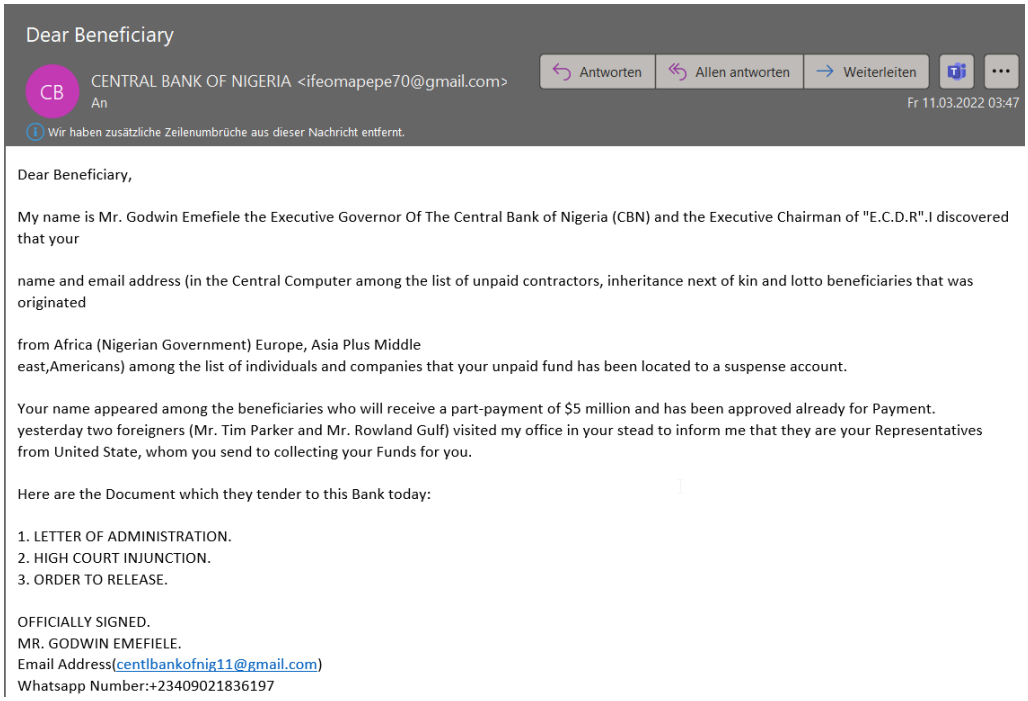


Eure Handynummer ist nicht ganz so geheim, wie sie es vielleicht sein sollte. Aus diversen Datenlecks ausgelesen wird sie verwendet, um Eure Daten zu kompromittieren.

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!

So geht’s leichter | Enkeltrick&Co: Schützt Euch!



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 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

DEU 09:00 Schieb.de

So geht's leichter | Enkeltrick&Co: Schützt Euch!

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.

DEU 09:00 Schieb.de

So geht's leichter | Enkeltrick&Co: Schützt Euch!

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.

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.

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

So geht's leichter | Enkeltrick&Co: Schützt Euch!

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.

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!

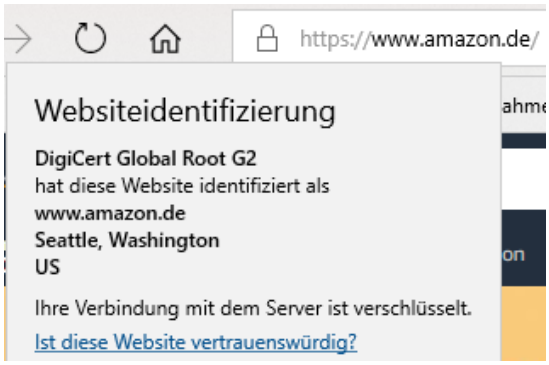
Sichere Webseiten

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

So geht's leichter | Enkeltrick&Co: Schützt Euch!

einen visuellen Eindruck verschaffen. Und vor allem könnt Ihr die Produkte anfassen und deren Qualität vorher beurteilen. Im Internet ist viel Vertrauenssache. Wenn Ihr kauft, dann könnt Ihr nur hoffen, auch die bestellte und meist vorbezahlte Ware zu bekommen.

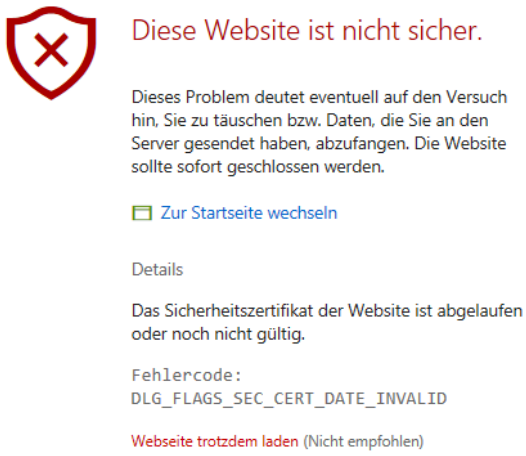
Einen Hinweis wenig bietet hier das Zertifikat der Webseite. Ein SSL-Zertifikat ist quasi ein Siegel, das die Organisation, der die Webseite gehört, und die Webseitenadresse miteinander in Verbindung bringen. Das Zertifikat ermöglicht es dann, die Kommunikation zwischen Eurem Rechner und dem Shop zu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

So geht's leichter | Enkeltrick&Co: Schützt Euch!

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 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.

So geht's leichter | Enkeltrick&Co: Schützt Euch!

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.

Vorsicht bei Anmeldung über Facebook § Co.

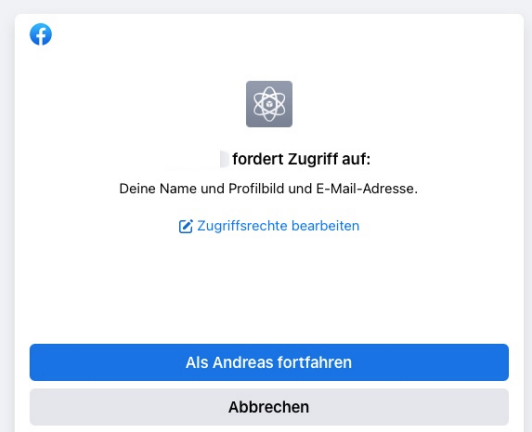
Fast jeder Shop oder Dienst im Internet erfordert ein Konto, in dem Ihr Eure Adress- und Zahlungsdaten hinterlegt. Das führt schnell dazu, dass Ihr Zugangsdaten mehrfach verwendet. Als Alternative bieten viele Anbieter daher die Anmeldung über soziale Netzwerke an. Hier solltet Ihr Vorsicht walten lassen!

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

So geht's leichter | Enkeltrick&Co: Schützt Euch!

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 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.

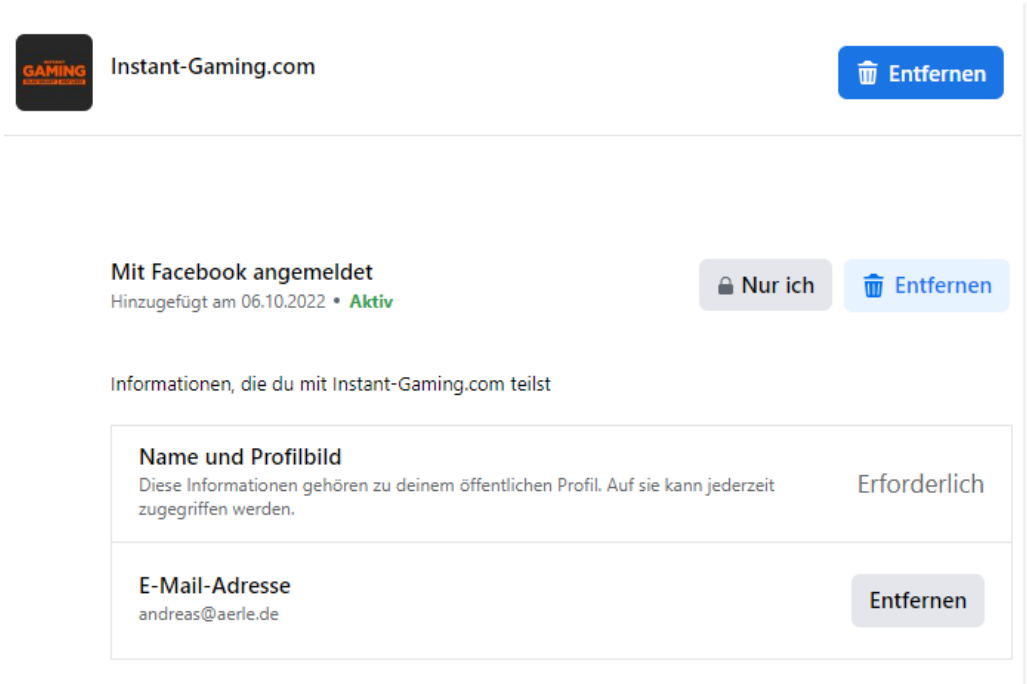
Übersicht über die Anmeldungen

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

So geht's leichter | Enkeltrick&Co: Schützt Euch!

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.

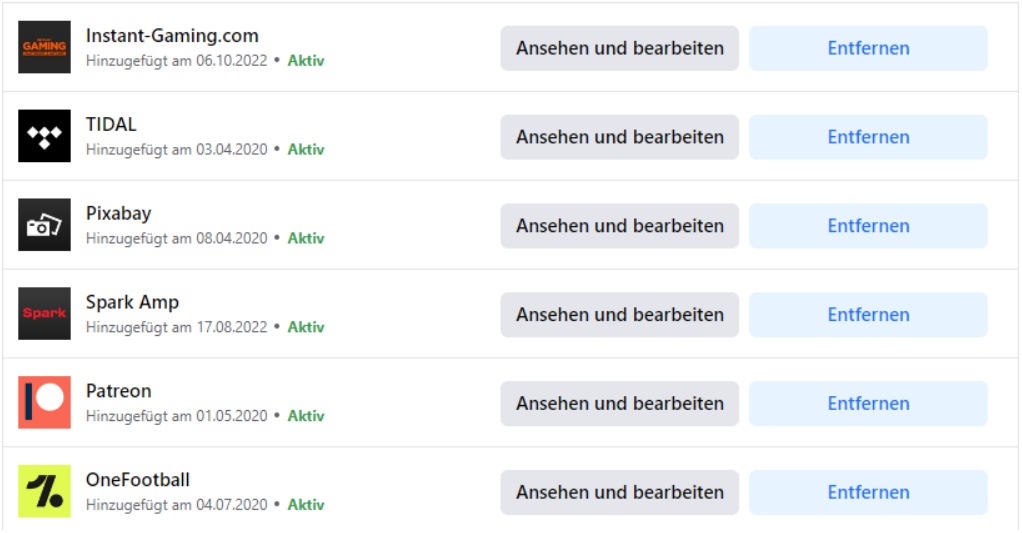


Löschen der Anmeldung per Facebook

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

So geht's leichter | Enkeltrick&Co: Schützt Euch!

natürlich dazu führen, dass bestimmte Funktionen nicht mehr funktionieren.



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.

Weitere Maßnahmen gegen Phishing

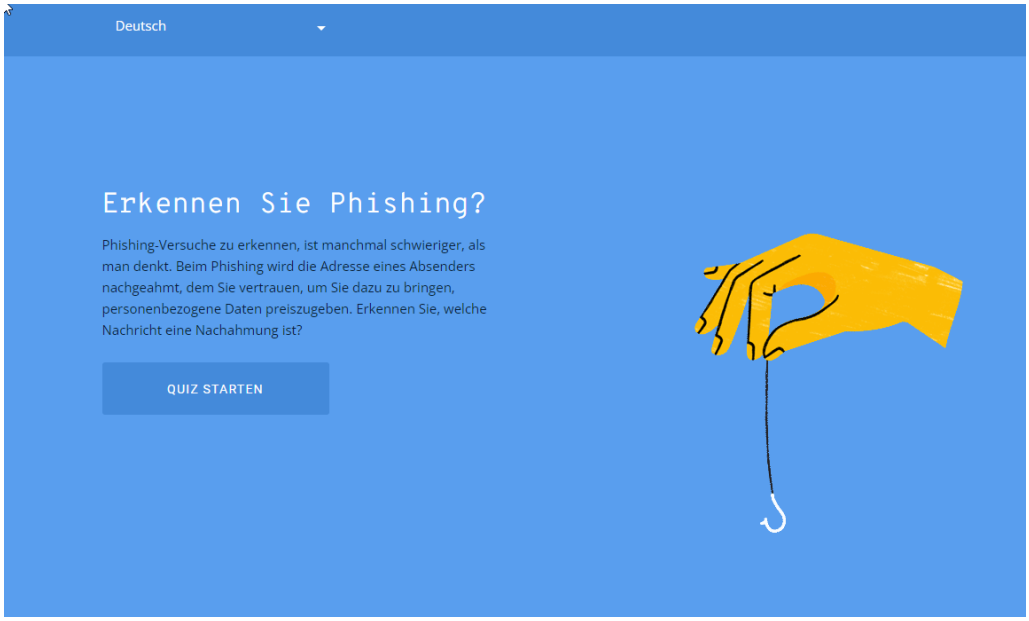
Ihr habt auf den vorangegangenen Seiten eines gemerkt: Phishing-Attacken sind vielfältig und immer anders. Es gibt keinen wirklichen Schutz, außer Euch immer und immer wieder damit zu beschäftigen, Euch zu trainieren, solche Mails und Nachrichten zu erkennen und gar nicht erst darauf zu reagieren.

So geht’s leichter | Enkeltrick&Co: Schützt Euch!

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

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?

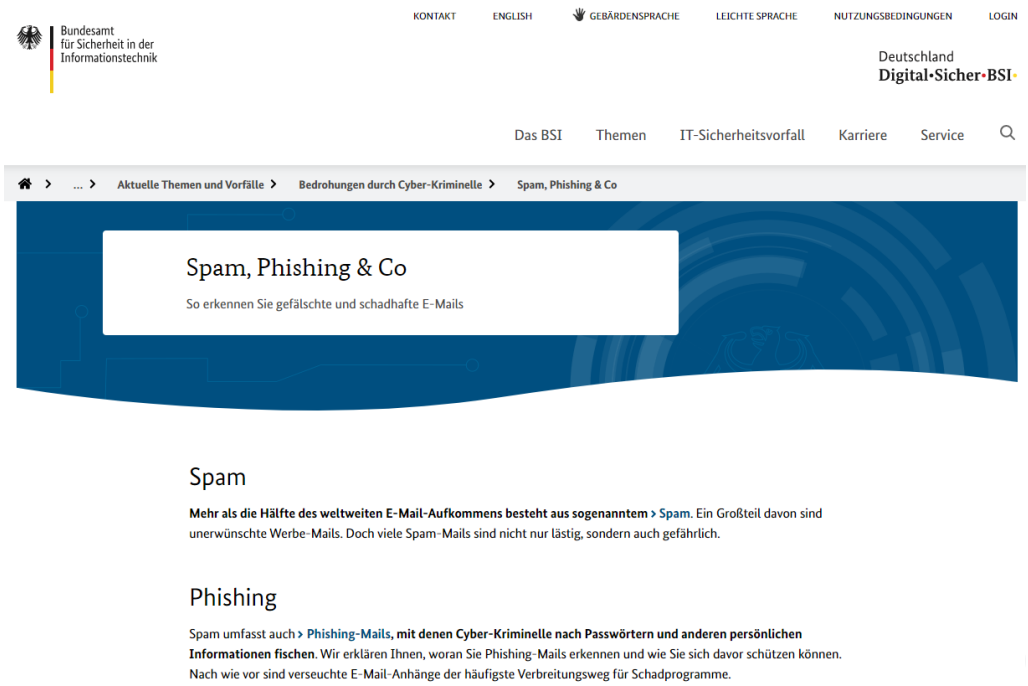
Keine Sorge: Weder werden Eure eingegebenen Informationen verwendet (die dienen nur dazu, die angezeigten E-Mails noch ein wenig realistischer zu machen), noch sind die Links in den Beispielen klickbar. Google will Euch ja schließlich nicht gefährden!

So geht’s leichter | Enkeltrick&Co: Schützt Euch!

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

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.

So geht's leichter | Enkeltrick&Co: Schützt Euch!

Phishing-Schutz im Browser aktivieren

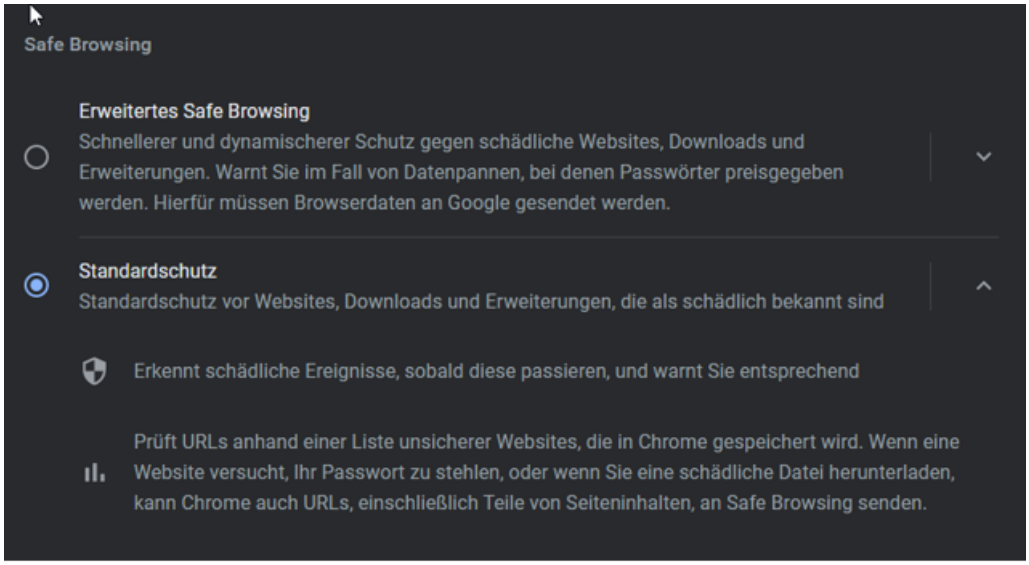
Hinter allen Browsern stehen große Hersteller, für die das Thema Sicherheit extrem wichtig ist. Darum haben sie Mechanismen an Bord, die Euch vor betrügerischen Webseiten und Phishingversuchen schützen sollen. Ihr müsst sie nur aktivieren und nutzen!

Microsoft Edge

Einmal mehr hat Microsoft es einfacher als andere Hersteller: Man nutzt einfach die Mechanismen, die sich auch für Windows als Betriebssystem bewährt haben.

- In Edge klickt auf die **drei Punkte** oben rechts > **Einstellungen** > **Datenschutz, Suche und Dienste**.
- Rollt ganz nach unten in den Bereich Sicherheit, dort finden sich zwei wichtige Optionen.
- **Microsoft Defender Smartscreen** nutzt den Cloud-Service von Microsoft, in dem Informationen von Benutzern aus der ganzen Welt zusammen laufen und aktuelle Phishing-Attacken sammeln, analysieren und die Browser der Benutzer dagegen wappnen.
- **Potenziell unerwünschte Apps blockieren** verhindert den versehentlichen oder absichtlichen Download von Apps, die Schaden verursachen oder das System instabil machen können.
- Aktiviert beide Optionen, um Euch zu schützen!

So geht's leichter | Enkeltrick&Co: Schützt Euch!



Mozilla Firefox

Auch Firefox bietet entsprechende Schutzfunktionen:

- Klickt auf das **Hamburgermenü** oben rechts > **Einstellungen** > **Datenschutz & Sicherheit**.
- Rollt ganz nach unten in den Bereich Sicherheit, dort befindet sich die Option **Gefährliche und betrügerische Inhalte blockieren**. Aktiviert darunter beide Punkte.
- Zusätzlich Aktiviert den **Zertifikatscheck**. Der sorgt dafür, dass die Zertifikate, die die Vertrauenswürdigkeit von Webseiten sicherstellen, noch einmal unabhängig bestätigt werden.

Google Chrome

Google Chrome nutzt wie Microsoft Edge die Chromium Engine als Basis, trotzdem sind die Anti-Phishing-Optionen ein wenig anders:

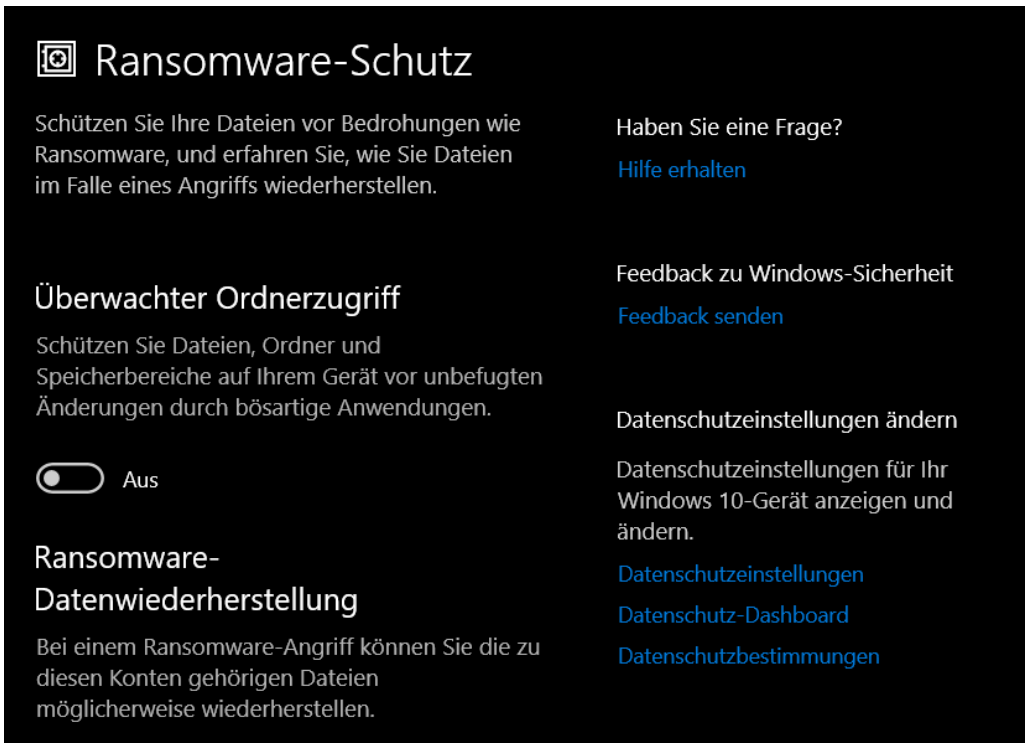
- Klickt auf die **drei Punkte** oben rechts > **Einstellungen** > **Datenschutz & Sicherheit**.

So geht's leichter | Enkeltrick&Co: Schützt Euch!

- Rollt nach unten zu **Safe Browsing**.
- Neben dem **Standardschutz** bietet Chrome auch noch das **Erweiterte Safe Browsing**, das ein Cloud-Lösung ähnlich dem SmartScreen von Microsoft, verwendet. Dazu müsst Ihr allerdings zustimmen, dass detailliertere Informationen an Google geschickt werden.

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 und schützt Euch vor den neben Phishing auch recht verbreiteten Angriffen durch Erpressersoftware.



- Klickt auf **Einstellungen** > **Datenschutz und Sicherheit** > **Windows-Sicherheit** > **Viren- & Bedrohungsschutz**

So geht's leichter | Enkeltrick&Co: Schützt Euch!

- 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.

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.

DEU 09:00 Schieb.de

So geht's leichter | Enkeltrick&Co: Schützt Euch!

- 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:

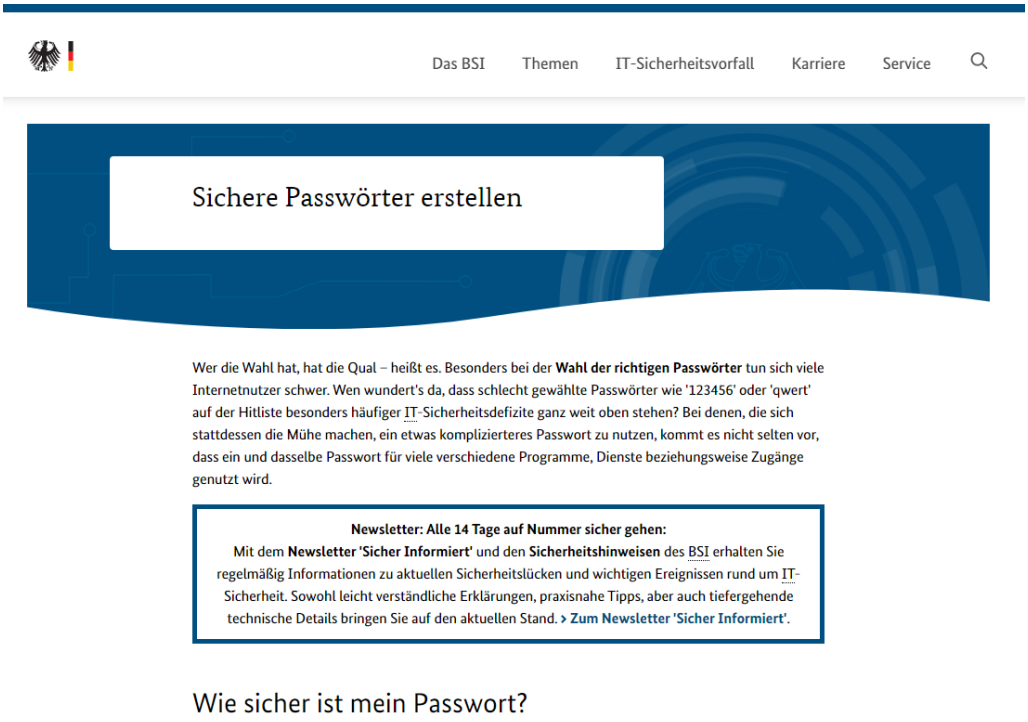
Das sichere Passwort

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 | Enkeltrick&Co: Schützt Euch!



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*.

So geht's leichter | Enkeltrick&Co: Schützt Euch!

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 Herbst 2023 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 ihrem Platz, und schon habt Ihr *IhiH2023dMg!* 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

So geht's leichter | Enkeltrick&Co: Schützt Euch!

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.

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

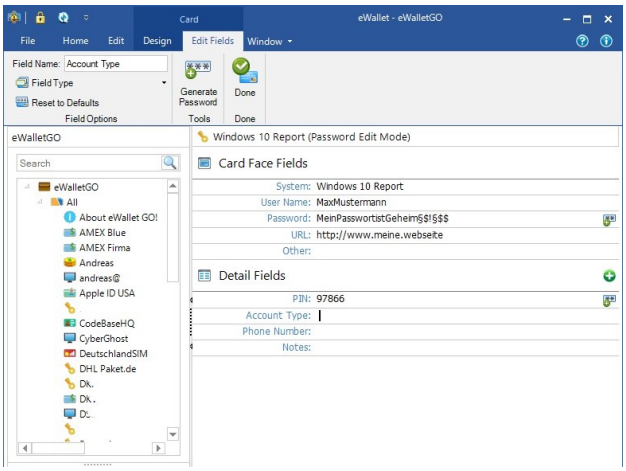
Es bedarf keiner langen Erklärung, dass das Aufschreiben von Passwörtern keine wirklich gute Idee ist. Auch wenn es kaum zu glauben ist: Viele erfolgreiche Angriffe auf Systeme kommen nicht über einen technischen Einbruch über das Internet oder interne Netzwerk, sondern über kleine, gelbe Klebezettelchen, 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.

DEU 09:00 Schieb.de

So geht’s leichter | Enkeltrick&Co: Schützt Euch!

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.



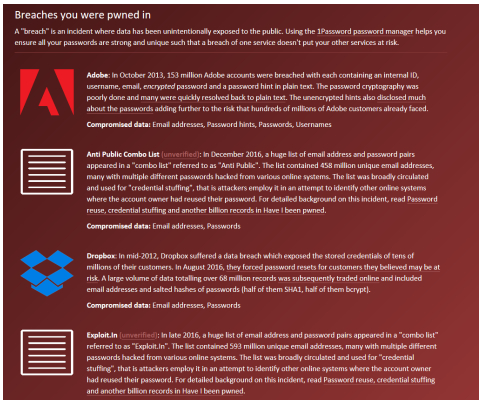
Bekannte Passwort-Safes sind zum Beispiel 1Password (https://1password.com) und KeePass (https://keepass.info). Wenn Ihr mit verschiedenen Plattformen auf Desktop, Tablet und Smartphone arbeiten, dann ist Ilium´s eWallet (https://www.iliumsoft.com/) eine gute Wahl.

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.

So geht's leichter | Enkeltrick&Co: Schützt Euch!

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.

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.

DEU 09:00 Schieb.de

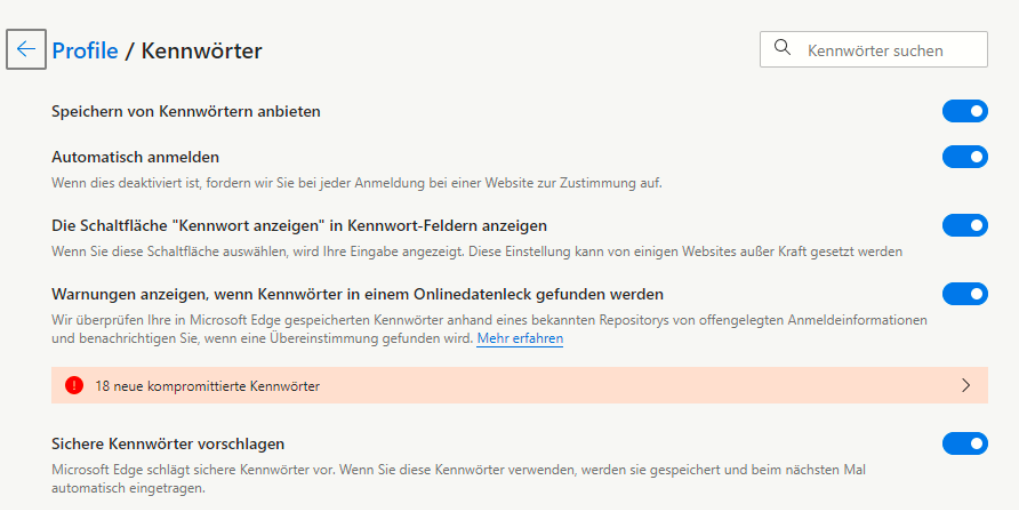
So geht's leichter | Enkeltrick&Co: Schützt Euch!

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.
- 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.

So geht's leichter | Enkeltrick&Co: Schützt Euch!



- 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**.

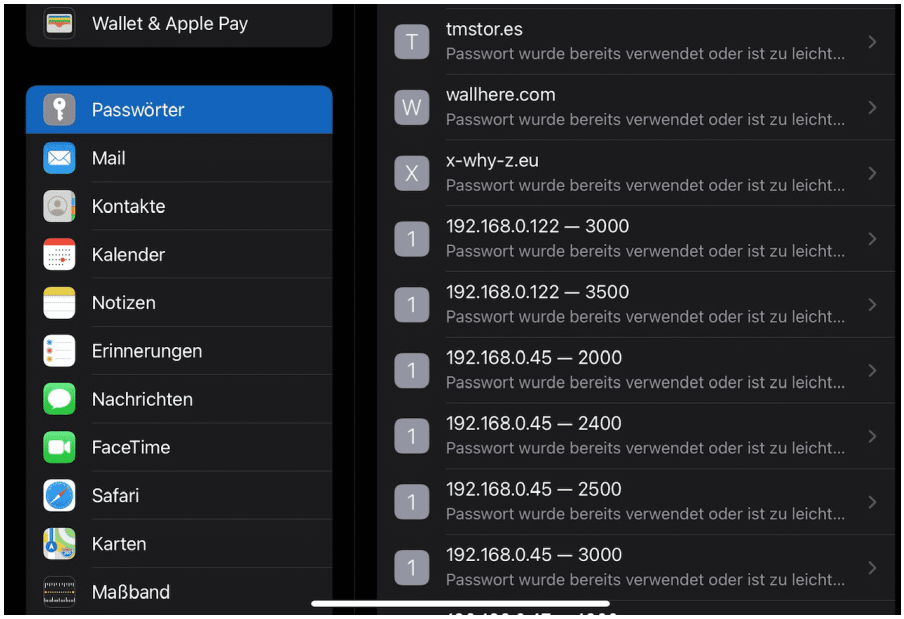
Ein solcher Hinweis sagt nicht zwingend aus, dass das Konto, an Ihr Euch gerade anmeldet, kompromittiert ist. Allerdings wurde die Kombination Benutzername/Kennwort in einem Leck gefunden. Ihr solltet die Zugangsdaten also umgehend ändern.

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 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.

So geht’s leichter | Enkeltrick&Co: Schützt Euch!



- 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.

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.

So geht's leichter | Enkeltrick&Co: Schützt Euch!

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

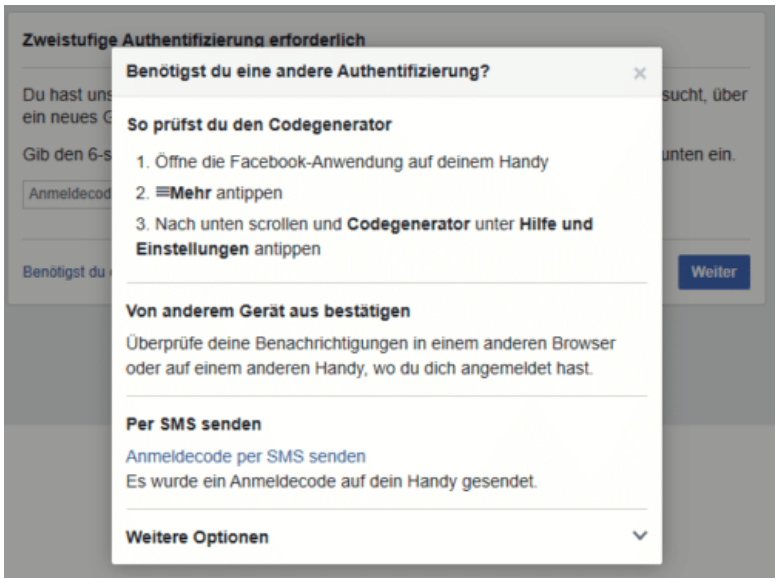
2FA bei Facebook

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

So geht’s leichter | Enkeltrick&Co: Schützt Euch!

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 | Enkeltrick&Co: Schützt Euch!

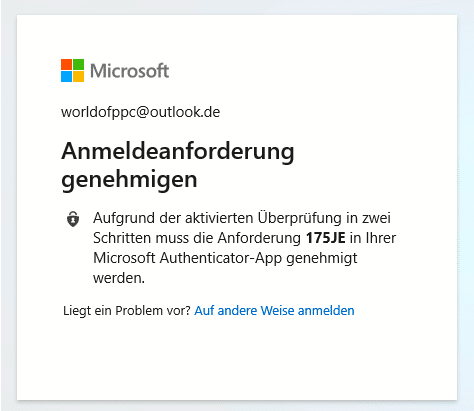
- Ein Klick auf **Anmeldecode per SMS** senden löst dann eine SMS mit dem Anmeldecode an die Eurem Konto hinterlegte Handynummer aus.

2FA bei Outlook

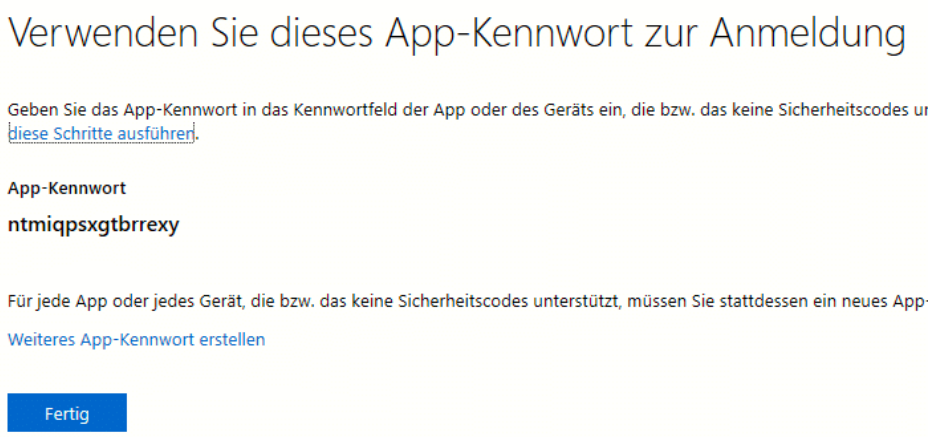
Die Zwei-Faktor-Authentifizierung funktioniert wunderbar, wenn der Zugriff über den Webbrowser stattfindet. Greift Ihr aber mit einem Programm auf das Outlook-Postfach zu, dann kann das Vorgehen von Programm zu Programm abweichen. In der Regel trefft Ihr dabei aber nur auf zwei Möglichkeiten. Einmal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

- 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!



So geht's leichter | Enkeltrick&Co: Schützt Euch!



- 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**.
- 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

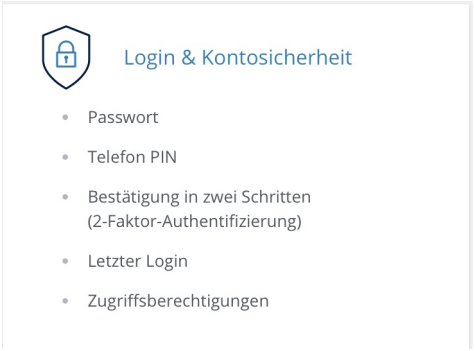
- Ruft die Admin-Seite von Office 365 auf, dann klickt auf **Benutzer**.

So geht's leichter | Enkeltrick&Co: Schützt Euch!

- 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.

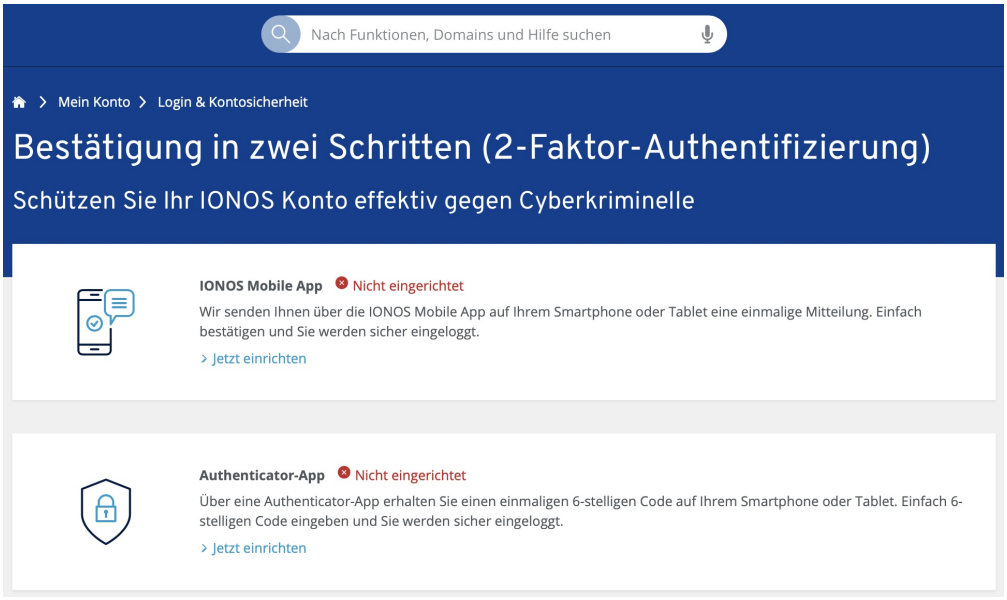
2FA für Webseiten

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 | Enkeltrick&Co: Schützt Euch!

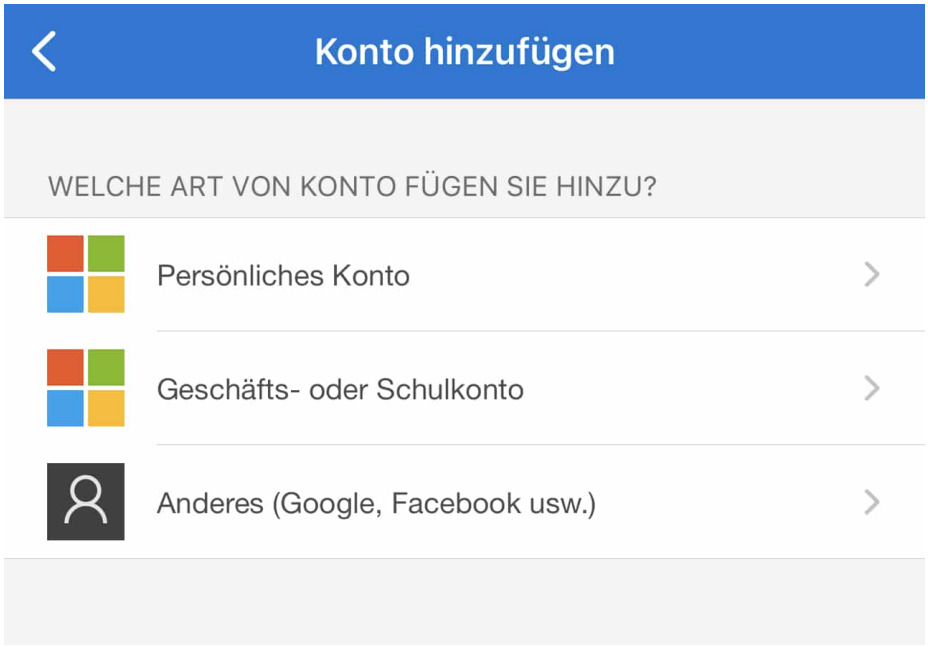


- IONOS bietet zwei verschiedene Möglichkeiten für den zweiten Faktor an: Zum einen die IONOS Mobile App, die unter anderem auch Einstellungen zum Hostingkonto erlaubt.
- Die zweite Möglichkeit ist die Verwendung einer normalen Authenticator-App, die dann auch für andere Konten verwendet werden kann.
- 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 | Enkeltrick&Co: Schützt Euch!



- 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 | Enkeltrick&Co: Schützt Euch!

- 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!