Das Internet: Nicht nur Chance, sondern auch Risiko


Startseite › Politik › Mehr Internetbetrug: Wie Kriminelle die C

Neuer Enkeltrick: Wie Betrüger nun Hochrisikopersonen ausnutzen

Die Corona-Pandemie markiert eine Zäsur, auch für Kriminelle. Betrüger versuchen, die Ausnahmesituation auszunutzen. Während Einbrüche in Zeiten von Homeoffice abnehmen, blüht der Betrug im Internet – und nicht nur da.

10.04.2020, 10:28 Uhr

MESSENGERDIENST

FIESE BETRUGSMASCHE: DAS IST DER NEUE ENKELTRICK BEI WHATSAPP

Stand: 24. November 2022, 17:42 Uhr

Die Polizei warnt vor einer neuen Betrugsmasche bei Messengerdiensten. Unbekannte geben sich bei WhatsApp als Sohn oder Tochter aus, deren Handy kaputt sei und bitten um Geld. Was Sie dazu wissen sollten.

"Hallo Mama. Mein Handy ist kaputt gegangen. Das ist meine neue Nummer" - mit WhatsApp-Nachrichten wie diesen beginnt der neue "Enkeltrick". Denn dreiste Betrüger haben sich vom Telefon auf Messenger-Dienste verlagert, da immer mehr Senior


Rentner aufgepasst: Verbraucherzentralen warnen vor neuer Betrugsmasche

Erstellt: 12.08.2022, 14:29 Uhr
Von: Patricia Huber

Kommentare Teilen

Mit einer neuen Masche wird derzeit versucht, Rentner um über hundert Euro zu betrügen. Verbraucherzentralen erklären, was im


/ Oberallgäu/Kempten / Bad Hindelang / Polizei

4. November 2022, 12:28 Uhr • 1.047× gelesen •
Redaktion all-in.de

FIESE BETRUGSMASCHE!

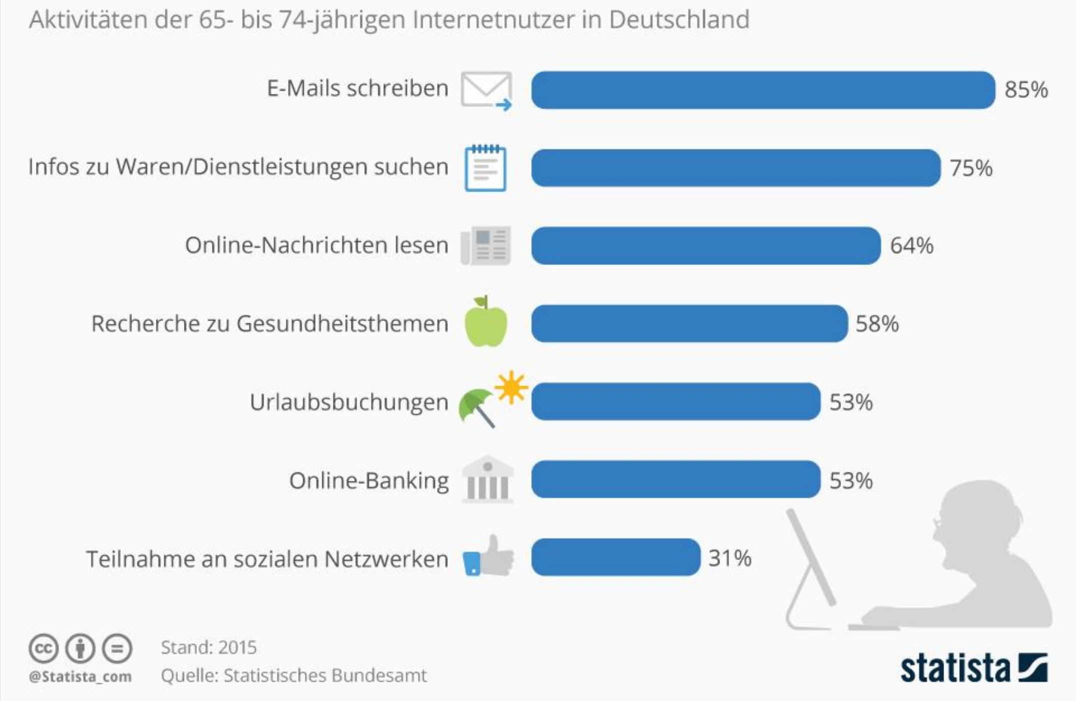
"Phishing"-Anruf: Betrüger erbeuten vierstellige Summe von Oberallgäuer Senior

Betrugsmasche "Phishing": Datenklau, zum Beisp Onlinebanking, richtet jedes Jahr viel Schaden a (Symbolbild) • Foto: vicky gharat auf Pixabay • hochgeladen von Holger Mock

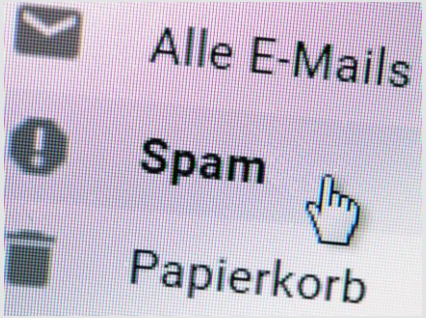
Ein älterer Herr aus dem Oberallgäu von Online-Betrügern. Die Unbekann ten bei dem Senior eine vierstellige


E-Mail-Konto gehackt, was tun? In nehmen Täter gern ältere Mensch Hier gibt das LKA Schleswig-Holst gegen Betrug im Internet.

Wozu Senior*innen das Internet nutzen



1. Betrugsmaschen - Spam-Mails



❖unerwünschte Spam-Mails verfolgen immer die gleiche Zielsetzung:

- ■ großflächige Werbung
- ■ persönliche Daten abgreifen
- ■ durch Betrug an Geld kommen

!!! es fallen noch immer sehr viele Menschen auf diesen Betrug rein!!!

❖ Spam-Mails lassen sich in kürzester Zeit, kostenlos und in einer riesigen Anzahl versenden (inzwischen sind über die Hälfte aller Mails „Datenmüll", vgl. Verbraucherzentrale)

❖ diese Mails sind nicht nur nervig, sondern können auch gefährlich werden

-können Viren oder schädliche Programme enthalten

-können Links zu betrügerischen Websites enthalten

1. Betrugsmaschen - Spam-Mails

Woher hat der Absender meine Mailadresse?

-Die Spammer verfügen über zufällig oder systematisch generierte Adressen

-Sehr verbreitet ist der Adressenhandel: Spammer kaufen oder mieten die gewünschten Daten von Adresshändlern

-Außerdem greifen Spammer auf verschiedene Programme zurück, die Web-Seiten systematisch nach E-Mail-Adressen durchsuchen oder existierende E-Mail-Adressen herausfiltern, indem willkürlich zusammengesetzte Buchstabenkombinationen und häufige Nachnamen getestet werden.

Woran erkenne ich Spam-Mails?

-nicht mehr so einfach, da häufig keine Rechtschreibfehler mehr enthalten sind

-häufig wird Zeitdruck gemacht / kurze Fristen zum Handeln gesetzt

-Daten sollen eingegeben oder Links angeklickt werden

-teils keine persönliche Anrede

1. Betrugsmaschen - Spam-Mails

Wie kann ich mich vor Spam-Mails schützen?

-besondere Vorsicht ist geboten, wenn die Spam-Mails persönliche Ansprachen oder Daten enthalten

-Vorschau-Funktion des Mail-Programms deaktivieren

-Spam-Mail niemals öffnen oder gar beantworten (dadurch wird ersichtlich, dass die Mailadresse existiert)

-Spam-Mails sollten immer zuerst in den Spam-Ordner verschoben und dann gelöscht werden (dadurch landen Mails vom selben Absender das nächste Mal automatisch im Spam-Ordner)

-Apps für Spammails verwenden

-die E-Mail-Adresse nur vorsichtig herausgeben

-zweite Mailadresse für Online-Einkäufe einrichten (diese kann gelöscht werden, falls zu viel Spam ankommt)

-Mails von blockierten Absendern können vorkommen, wenn der Absender seine Adresse so gefälscht hat, dass ein anderer Name im Feld „Von:" angezeigt wird

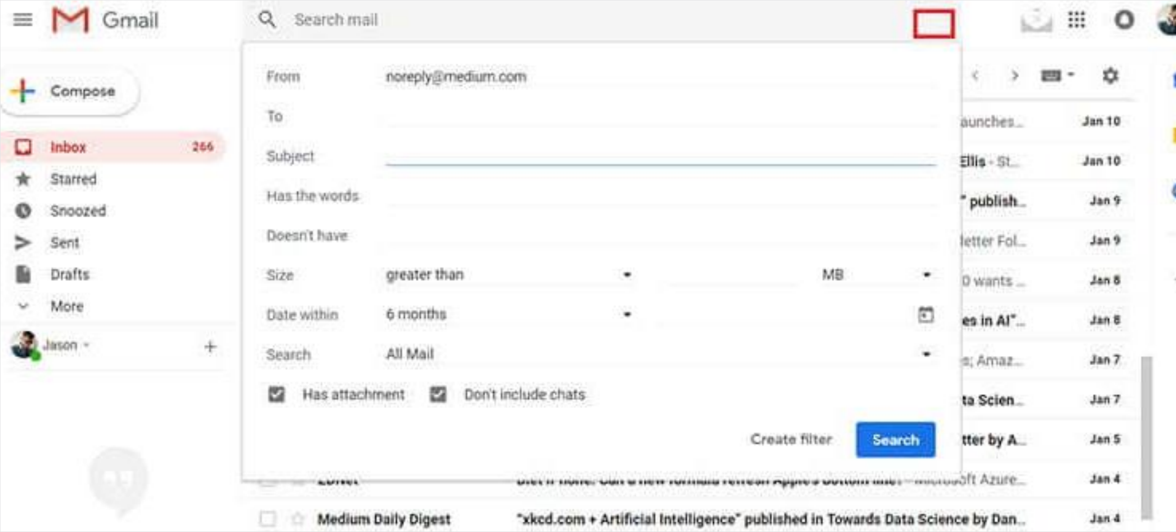
-Filtereinstellung des Mailprogramms checken

1. Betrugsmaschen - Spam-Mails

Wie kann ich unerwünschte E-Mails blockieren?
Bei allen gängigen E-Mail-Diensten können Sie Spam Filter einrichten, zum Schutz vor Spam Mail in Ihren Posteingang

Beispiel Einstellungen Gmail:
1.Öffnen Sie Ihren Gmail Posteingang.
2.Klicken Sie im Suchfeld auf den Abwärtspfeil, um auf die Einstellungen vom Spamfilter zuzugreifen.
3.Klicken Sie unten im Suchfenster auf Filter erstellen.

1.Wählen Sie aus, was der Spam Filter tun soll.
2.Klicken Sie auf Filter erstellen.



Achtung: Durch den Spam-Filter können auch legitime Mails gefiltert werden

1. Betrugsmaschen - Phishing

amazon.de

Datum: 03.02.2019

Sehr geehrter Herr [redacted]

auf Grund einer Gesetzesänderung sind Wir verpflichtet regelmäßig zu legitimieren ob Sie der rechtmäßige Inhaber des Kontos sind. Dieser Vorgang ist notwendig um noch stärker gegen Terrorismusfinanzierung vorzugehen.

Im rahmen der Überprüfung ist ein Datenabgleich erforderlich. Achten Sie hierbei auf die korrekte Angabe aller Informationen. Sollte es zu Abweichungen kommen sind wir auf Grund der Gesetzesänderung gezwungen ihr Amazonkonto bis zur Verifikation Ihrer Person einzuschränken.

Weiter zur Überprüfung

Wir entschuldigen uns für die Unannehmlichkeiten und bedanken uns bei Ihnen für Ihre Geduld

Mit freundlichen Grüßen
Ihr Team von Amazon

Dies ist eine automatisch versendete Nachricht.
Antworten Sie nicht auf dieses Schreiben, Diese Adresse wurde nur zum Versand von E-Mails eingerichtet

PayPal Support
21 January 2016 at 18:14:48 GMT+1
To: Recipients
Ihr PayPal Konto hat ein neues Endgerät

PayPal

Ihr PayPal Konto hat ein neues Endgerät

Guten Tag
Ihr letzter Einkauf in Höhe von **523,64 €** zzgl. Versandkosten bei dem Online-Anbieter **amazon.de** wurde zu Ihrer Sicherheit zunächst nicht ausgeführt. Hier gelangen Sie zum jeweiligen Produkt.

Scheinbar wurde Ihr Zugang von einem dritten Endgerät genutzt, welches uns nicht bekannt ist.

Wenn Sie diesen Einkauf **nicht** durchgeführt haben, bitten wir Sie über den unten aufgeführten Button Ihre Daten zu bestätigen und anschließend die Bestellung zu stornieren.

Für die Stornierung der Bestellung haben Sie eine Frist von **12 Werktagen**. Läuft diese ab und Sie beantragen keine Stornierung, wird die Transaktion automatisch genehmigt.

Stornieren Sie hier (zum Widerruf)

Vielen Dank für Ihre Zeit.

Phishing-Mails sind Spam-Mails, die auf den ersten Blick so aussehen, als kämen sie beispielsweise von der Hausbank, von Paypal oder Amazon. Sie wollen die Nutzer auf eine gefälschte Webseite lenken. Mails und Webseite sind dabei oft täuschend echt und auf den ersten Blick kaum als Fälschung zu erkennen. Das Opfer gibt deshalb die eigenen Benutzerdaten zum Beispiel fürs Onlinebanking ein – doch die landen eben nicht bei der Hausbank, sondern auf dem Computer der Kriminellen

1. Betrugsmaschen - Phishing

Wie kann ich mich vor Phishing schützen?

-stets vorsichtig sein

-häufig verwenden diese Mails allgemeine Anreden in Kombination mit Zeitdruck

-KEINEN Links in Mails folgen, Spam-Mails möglichst nicht öffnen und unverzüglich über den Spam-Filter löschen

-den Anbieter anrufen über die bekannte Telefonnummer (nicht über Kontaktdaten in der Mail oder auf einer Website (könnte ebenfalls Fake sein!)

-wenn ein Anruf eingeht (auch mit korrekter Telefonnummer inkl. Vorwahl) misstrauisch sein!

-NIEMALS Geheimzahlen, Passwörter etc. am Telefon bekanntgeben oder parallel nach Aufforderung eintippen

-E-Mail-Header lesen

-halten Sie Virenschutzprogramme auf Ihren Geräten aktuell

-Passwörter regelmäßig ändern und sichere Passwörter verwenden

Passwortsicherheit

In wenigen Schritten zum sicheren Passwort

Sie haben zwei Strategien zur Wahl

Langes und weniger komplexes Passwort

Nutzen Sie ein langes Passwort (mindestens 25 Zeichen), brauchen Sie nur zwei Zeichenarten, z.B. Groß- und Kleinbuchstaben.

Umsetzungsbeispiel: tisch_himmel_kenia_blau_pfannkuchenteig_lachen

Kürzeres und komplexes Passwort

Nutzen Sie ein kurzes Passwort (mindestens acht Zeichen), sollten Sie vier Zeichenarten kombinieren (Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen).

Umsetzungsbeispiel: q7yPv8!x§B

© Bundesamt für Sicherheit in der Informationstechnik

1. Betrugsmaschen – Online-Einkäufe

Für viele sind Online-Einkäufe inzwischen zum Standard geworden

⇨durch dieses routinierte Online-Shopping werden manche unvorsichtig und tappen in die Betrugsmasche

⇨insbesondere wenn man „schnell“ etwas einkaufen möchte, um die Lieferung noch rechtzeitig zu erhalten, werden manche leichtsinnig

⇨ebenso bei besonders verlockenden Preisangeboten

!!! Achtung !!!

-Immer vorsichtig bleiben

-das eigene Handeln stets kritisch hinterfragen

-auf das Bauchgefühl hören

1. Betrugsmaschen – Betrügerische Websites

-mit Fake-Websiten möchten Betrüger kriminelle Machenschaften vollziehen

-es handelt sich dabei um erfundene Websites oder Kopien von existierenden Seiten, häufig täuschend echt mit Prüfsiegel, Impressum und Callcenter

-es werden dazu beliebte legitime Shops wie z. B. Amazon genutzt, um das Vertrauen der Kunden zu missbrauchen

-durch den „Verkauf" von Artikeln möchten die Betrüger an persönliche Daten sowie Zahlungen kommen

1. Betrugsmaschen – Betrügerische Websites

Woran erkenne ich einen Fake-Shop?

- ☒ In der Adresszeile des Browser fehlt das Kürzel https://
- ☒ Die angebotenen Produkte sind extrem günstig (im Vgl. zum Wettbewerb)
- ☒ Die Kundenbewertungen auf der Website sind ausschließlich „Sehr gut“
- ☒ Schlechtes Deutsch in Rechtschreibung oder Grammatik auf der Website
- ☒ Impressum, Datenschutzerklärung und AGBs fehlen oder sind unvollständig
- ☒ Keine oder nur eingeschränkte Kontaktmöglichkeiten
- ☒ Bezahlung nur per Vorauskasse oder Direktüberweisung möglich

1. Betrugsmaschen – SMS und Handy

Derzeit sind betrügerische SMS im Umlauf:

■angebliche Paketdienste, in denen Empfänger auf einen Link tippen sollen. Die Folge können schädliche Apps, Massen-SMS und Abofallen sein. Diese Betrugsform ist als "Smishing" bekannt.

■SMS mit neuer Handynummer

!!!hier gilt äußerste Vorsicht!!!

Für die Internetnutzung mit dem Smartphone sind die Tipps zur Sicherheit gleichermaßen zu beachten

2. Tipps der MuT-Profis zur Sicherheit im Netz
-Online-Einkäufe-

-Domänenname von Websites prüfen (.net oder .org sind sehr viel weniger häufig als .de)

-häufig sind Auszeichnungen und Siegel kopiert (draufklicken, ob diese einen Link folgen)

-immer Vorsicht wahren bei der Bezahlung (v. a. bei Bezahlung mit Kreditkarte und Vorauskasse). Bestehen Sie auf sichere Zahlungsmethoden ➔häufig greifen Betrüger auf die Ausrede zurück, dass Überweisung etc. derzeit aufgrund technischer Probleme nicht zur Verfügung steht

-persönliche Kontodaten nur wenn unbedingt notwendig herausgeben

-Vorsicht: Ist es wirklich notwendig, dass manche Angaben als Pflichtfeld notwendig sind für den Einkauf?

-Überprüfen Sie den Online-Shop auf Seriosität, lesen Sie die Bewertungen (Nur positive? Könnte verdächtig sein)

-Informieren Sie sich über die Ware, seien Sie misstrauisch bei Schnäppchen

-Achten Sie auf Ihr Widerrufsrecht

-Achten Sie auf sichere Datenübertragung

-Wählen Sie sichere Passwörter

2. Tipps der MuT-Profis zur Sicherheit im Netz

-Verkaufsplattformen-

➢immer hinterfragen „würde ich im realen Leben so handeln?“ Wenn Ihre Antwort darauf Nein lautet, dann bitte auch online nicht machen

➢auch bei Privat(ver)käufen Vorsicht wahren, selbst wenn der Verkäufer sympathisch wirkt

➢Vorsicht wem Sie vertrauen (insbesondere bei Online-Bekanntschaften, Dating-Portalen, Bezahlung von Online-Käufen von privat etc.)

Fall 1: Der angebliche Kurierdienst möchte vor der Zustellung des Geldes eine Zahlung für eine Versicherung. Zu einer Geldübergabe oder Abholung kommt es jedoch nie.

Fall 2: Der Trick besteht darin, dass der Abholdienst schneller ist als das versandte Geld. Weigert man sich die Ware mitzugeben, wird man als Betrüger hingestellt, da der Käufer bezahlt hätte und das Geld nicht mehr zurückholen kann. Als Verkäufer bekommt man zudem auch gefakte Mails vom Kurierdienst, dass das Geld unterwegs sei.

Fall 3: Der Käufer lässt sich auf die IBAN-Überweisung ein und sendet einen Screenshot von der Überweisung. Wieder steht kurze Zeit später jemand vor der Tür, der die Waren abholen möchte

2. Tipps der MuT-Profis zur Sicherheit im Netz

-Online bezahlen-

◇◇◇◇◇

■für das Online Banking möglichst zwei Geräte nutzen (TAN)

■ TAN niemals am Telefon bekanntgeben oder parallel eingeben

➔Banken rufen NIEMALS an und verlangen den TAN oder Bankverbindungen etc.!!!

■Tageshöchstlimit für Überweisungen hinterlegen

■immer skeptisch bleiben

■bei Mails/Anrufen von der Bank bei dieser nachfragen

■Passwort / Zugangsdaten öfter ändern

■Passwörter nicht auf dem Computer oder Handy gesammelt speichern

(kann von Betrügern gehackt werden)

2. Tipps der MuT-Profis zur Sicherheit im Netz

-mobil bezahlen-

■kontaktloses Bezahlen ist eine vergleichsweise sichere Technologie, v. a. mit dem Smartphone

■Halten Sie die Gerätesoftware Ihres Smartphone oder Ihrer smarten Armbanduhr stets auf dem neuesten Stand und nutzen Sie automatische Updates

■ Um das ungewollte Auslesen von funkfähigen Karten wirklich ganz sicher zu verhindern, können Sie eine Schutzhülle verwenden, die Funkwellen zuverlässig blockiert.

■ Wenn Ihre funkfähige Karte oder Ihr Smartphone mit verwendbarer Bezahlfunktion verloren geht, sollten Sie sofort handeln. Lassen Sie Karten und Konten umgehend sperren. In den meisten Fällen hilft der zentrale Sperr-Notruf, der unter 116 116 rund um die Uhr zu erreichen ist, aus dem Inland gebührenfrei.

■ Kontrollieren Sie regelmäßig Ihre Abrechnungen und melden Sie falsche Abbuchungen umgehend Ihrer Bank.

■ Wer Bedenken hat, kann das kontaktlose Bezahlen bei einigen Banken und Sparkassen abschalten lassen. Fragen Sie ggf. Ihre Bank

■ nicht zum Online-Bezahlen in öffentliche Wlan-Netzwerke einwählen

3. Verhalten im Falle eines Betrug(verdacht)es

Beweise sichern:

-Heben Sie die Mails gut auf, in denen Sie der Anbieter auffordert, die Ware zu liefern oder eine Rücksendeadresse mitzuteilen

-Bildschirmfotos der betrügerischen Seiten machen und dann unverzüglich die Bank informieren

Schnell handeln:

-Passwort ändern

-Kontaktieren Sie Ihre Bank, das Kreditinstitut oder den Zahlungsdienstleister und bitten Sie um Rückerstattung

-Online-Überweisungen lassen sich innerhalb eines kurzen Zeitraums rückgängig machen (außer bei Sofortüberweisung), jedoch muss das empfangende Unternehmen zustimmen. Häufig schwierig, wenn die Überweisung ins Ausland geht!

-Auch bei geringen Beträgen sollte man Anzeige bei der Polizei erstatten

-wenn etwas merkwürdig vorkommt, dies mit einer Vertrauensperson besprechen

4. Tipps zur Sicherheit im Umgang mit dem Smartphone im Netz

Auch für das Smartphone gelten die genannten Tipps, insbesondere bei Verwendung von Einkaufs- oder Mail-Apps

1. Software aktuell halten
2. Virenschutz aktivieren
3. Apps nur aus sicheren Quellen
4. Browserwarnungen beachten
5. Fake-Warnungen erkennen
6. Illegale Inhalte meiden
7. Zwei E-Mail Adressen verwenden
8. Vorsicht bei Spam
9. Passwörter klug wählen
10. Erst Denken, dann klicken

Bei der Verbraucherzentrale gibt es noch weiterführende, hilfreiche Tipps zur Sicherheit sowie Information über aktuelle Tricks / gehäuftes Auftreten von Betrügen

Ebenso beim Bundesamt für Sicherheit in der Informationstechnik

4. Fazit – Sicherheit im Netz