# *Coronavirus als neue Betrugsmasche*

Kriminelle haben die Corona-Krise als erträgliche Einkommensquelle entdeckt und versuchen auf perfide Weise, ältere und gutgläubige Menschen zu betrügen. Dabei nutzen die Trickbetrüger die aktuellen Entwicklungen rund um die Corona-Pandemie geschickt aus, um ihren kriminellen Aktivitäten verstärkt nachzugehen. Es ist wahrscheinlich, dass in naher Zukunft weitere Betrugsmaschen auftauchen. Denken Sie immer daran: Die Trickbetrüger sind erfinderisch!



Die folgenden Beispiel-Fälle zeigen, welche Maschen die (Trick-) Betrüger anwenden und geben Tipps und Hilfestellungen, wie Sie sich schützen können.

# *1. Corona-Maschen am Telefon*

### Fall 1: Der Enkeltrick – Angst um Angehörige wird ausgenutzt

Bei Rainer F. klingelt das Telefon und sein vermeintlicher Enkel berichtet, er habe sich mit dem Coronavirus infiziert. Er läge im Krankenhaus und brauche dringend Geld für teure Medikamente. Ob ein Kurier bei Rainer F. das Geld abholen könne? Bei dieser Nachricht wurde der Rentner misstrauisch. Er rief seinen Enkel direkt an. Zum Glück. Der Enkel war kerngesund und bestätigte seinen Verdacht, dass Betrüger am Telefon zugange waren. Rainer F. notiert sich alle wichtigen Infos und beschwert sich bei der Verbraucherzentrale und informierte die Polizei. Zu Recht.

### Fall 2: Adressenklau am Telefon - Das Spiel mit der Gesundheit

Als Inge H. am Telefon erfuhr, dass sie sich möglicherweise bei einer Bekannten mit Corona infiziert habe, stieg ihr Puls auf 180. Die 92-jährige Seniorin gab dem vermeintlichen Mitarbeiter der Corona-Hotline die Nummer ihrer Schwiegertochter. Auch ihr wurde der Sachverhalt erklärt. Kurz darauf erhält die Schwiegertochter eine E-Mail, in der sie dazu aufgefordert wird, alle Kontaktpersonen der Schwiegermutter mit Namen, Anschrift und Telefonnummer in Formulare einzutragen. Sie wurde misstrauisch und fragte beim Gesundheitsamt nach. Die

daraufhin folgenden Ermittlungen der Polizei ergeben, dass es sich um eine fiese Betrugsmasche handelt, um an Anschriften potenzieller Opfer zu gelangen.

## Das sollten Sie wissen:

### Enkeltrick – Angst um Angehörige wird ausgenutzt Adressenklau am Telefon - Das Spiel mit der Gesundheit

Ein Anruf eines vermeintlichen Enkels mit der Bitte um Geld, eine angebliche Corona-Meldestelle informiert über eine mögliche Infizierung, das Ordnungsamt fordert telefonisch zur Zahlung eines Bußgeldes auf – die Spielarten des (Enkeltrick-) Betruges am Telefon sind vielseitig. Die Betrüger nutzen dafür sogar Telefonnummern von realexistierenden Hotlines oder Meldestellen, die im Zusammenhang mit Corona stehen. Deswegen ist bei unbekannten Anrufern, die Geld fordern oder sich für sensible Daten interessieren, stets Vorsicht geboten. Eine neue Form der Masche: Der vermeintliche Enkel ruft aus dem Ausland an, behauptet, er sitzt in Quarantäne wegen des Virus und benötige dringend Geld.

## Tipps zum Schutz vor betrügerischen Anrufen:

- Seien Sie immer misstrauisch, wenn Personen sich am Telefon als Verwandte oder Bekannte ausgeben, die Sie als solche nicht erkennen. Auch bei Ratespielchen wie „Rate mal, wer dran ist“, sollten Sie auf keinen Fall mitmachen und Namen nennen.
- Sollten Sie Zweifel an der Identität eines Anrufers hegen, der sich als Familienangehöriger oder Mitarbeiter des Gesundheitsamtes ausgibt, legen Sie auf und rufen Sie den angeblichen Bekannten/Verwandten oder das Gesundheitsamt selbst unter der Ihnen bekannten Nummer an.
- Rufen Sie die vermeintlich infizierte Bekannte an, um zu prüfen, ob diese wirklich an dem Coronavirus erkrankt ist und ob sie Ihre Kontaktdaten an das Gesundheitsamt weitergegeben hat.
- Telefonbetrüger verschaffen sich während dem Gespräch äußerst versiert Informationen über Sie, Ihr Umfeld und Ihre finanziellen Verhältnisse. Geben Sie niemals Ihnen unbekannten Personen Informationen (z.B. Adressen) über sich oder andere preis.
- Lassen Sie niemals Fremde in Ihre Wohnung und übergeben Sie niemals Geld an Ihnen unbekannte Personen, die ein Verwandter telefonisch angekündigt hat.
- Informieren Sie die Polizei, wenn Ihnen die Kontaktaufnahme verdächtig vorkommt und lassen Sie sich nicht einschüchtern und notieren Sie sich, wenn möglich, die Rufnummer.

## Fall 3: Teure Nachhilfe in Zeiten von Corona

Rolf W. klingelte es am Telefon. Eine Mitarbeiterin eines vermeintlichen Nachhilfe-Portals zählt ihm energisch die Vorteile ihres Nachhilfeunterrichts auf: Ein Gesamtpaket mit 80 Unterrichtseinheiten für nur 1235 EUR wäre in Zeiten von Corona ein unschlagbares Angebot. Rolf W. zögerte nur kurz. Zuhause mit zwei schulpflichtigen Kindern und seiner Frau und ihm im Homeoffice waren zu einer Herausforderung für die ganze Familie geworden. Das Angebot versprach eine Entlastung des neuen Familienalltags. Leider tauchte der angekündigte Nachhilfelehrer nie auf. Das Geld war weg.

### Das sollten Sie wissen:

#### Teure Nachhilfe in Zeiten von Corona

Arbeitsblätter, Lernvideos, Schulaufgaben – Homeschooling beschäftigt in Zeiten von Ausgangssperren viele Familien. Umso hilfreicher wirken da die Versprechungen von Online-Nachhilfeunterricht. Der erhöhte Bedarf ruft unseriöse Anbieter mit fragwürdigen Geschäftsmodellen auf den Plan. Betrüger verkaufen Eltern am Telefon überteuerte Nachhilfeangebote, bspw. 1200 EUR teure monatliche Abo-Verträge. Nach der Buchung kommen die Nachhilfelehrkräfte entweder nie vorbei oder die Qualität des Unterrichts lässt sehr zu wünschen übrig.

### Tipps zum Schutz vor überteuerter Nachhilfe:

- Sollten Ihnen das überteuerte Angebot am Telefon fragwürdig vorkommen, legen Sie auf. Wichtig: Nehmen Sie niemals Leistungen des Vertrags direkt am Telefon in Anspruch.
- Informieren Sie sich bei Interesse an Nachhilfeangeboten bei der Schule ihrer Kinder oder der Nachhilfeschule vor Ort. Hier bekommen Sie sicherlich hilfreiche Tipps.
- Lassen Sie sich auf keine Diskussion ein, denn die Betrüger verfügen in der Regel über einen reichen Erfahrungsschatz, dem der überraschte Bürger meist nicht gewachsen ist.

## Fall 4: Falsche Mitarbeiter der Landesbank

Hilde M. sucht hektisch nach ihrem TAN-Generator. Die angebliche Mitarbeiterin ihrer Landesbank erklärt am Telefon, dass eine Überprüfung ihres TAN-Generators anstehe und das müsse jetzt sofort und aufgrund der Corona-Maßnahmen am Telefon geschehen. Endlich, gefunden! Hilde M. steckt ihre EC-Karte in den TAN-Generator und folgt den Anweisungen am Telefon. „Geschafft“, denkt Hilde M. Mit Entsetzen stellt sie einige Tage später fest, dass auf ihrem Konto Überweisungen von Dritten getätigt wurden.

Das sollten Sie wissen:

### Falsche Mitarbeiter der Landesbank

Die vermeintliche Überprüfung des eigenen TAN-Generators stellt eine neue Masche von Telefonbetrügern dar. Dass diese Überprüfung durch Mitarbeiter einer Landesbank am Telefon stattfinden muss, ist in Zeiten von Corona ein nützliches Scheinargument. Steckt die Kreditkarte im Generator, diktieren die Betrüger ihren Opfern einen Startcode zur Eingabe in den TAN-Generator. Daraufhin erscheint ein neuer Code, den die Opfer den Kriminellen nennen sollen. Dieser Code dient den Betrügern als Zugang zum Onlinebanking der Betroffenen und sie können getätigte Transaktionen umleiten.

Tipps zum Schutz vor falschen Bankmitarbeitern:

- Geben Sie niemals ihre Zugangsdaten oder PINs zu Ihrem Online-Banking am Telefon heraus.
- Legen Sie auf, wenn Sie zur Herausgabe sensibler Daten aufgefordert werden.
- Hegen Sie Zweifel an der Identität des Bankangestellten: Rufen Sie Ihre Bank direkt an. Suchen Sie die Telefonnummer selbst heraus. Nutzen Sie nicht die Rückruftaste.

## Fall 5: Falsche Gewinnversprechen

Es klang zu schön um wahr zu sein. Michaela H., 68 Jahre alt, freute sich im ersten Moment riesig, als sie am Telefon von ihrem Geldgewinn erfuhr. Ein Notar und zwei Sicherheitsleute kommen vorbei, um den Gewinn zu übergeben. Als Michaela H. kurz darauf mitgeteilt wurde, dass die persönliche Übergabe wegen Corona nun doch nicht möglich sei und sie die Transportkosten des Gewinns in Höhe von mehreren Hundert Euro übernehmen müsse, wurde sie misstrauisch. Sie hatte an keinem Gewinnspiel teilgenommen. Warum sollte sie in Vorleistung gehen? Michaela H. notiert sich alle wichtigen Infos und leitet eine Beschwerde bei der Verbraucherzentrale ein. Zu Recht.

Das sollten Sie wissen:

### Falsche Gewinnversprechen

Ob Traumreise, Auto oder hohe Geldsummen in Zeiten von Corona – diese Betrugsmasche ist leider häufig anzutreffen und nun an die Situation mit Corona angepasst. Die Kriminellen geben sich häufig als Notare, Rechtsanwälte oder Staatsanwälte aus und fordern sehr überzeugend vom Gewinner eine Vorleistung. Der Geschädigte soll Geld in Form von Google-Play-Karten oder anderen Guthaben-Karten (Amazon, iTunes…) besorgen. Hat das Opfer die Karten besorgt, meldet

sich der Betrüger nach einer Stunde zur Übermittlung des Codes wieder.

### Tipps zum Schutz vor falschen Gewinnversprechen:

- Nur wer mitspielt, hat bei Gewinnspielen eine Chance: Bleiben Sie trotz Vorfreude skeptisch und weisen Sie unberechtigte Geldforderungen sofort zurück.
- Für Gewinne muss man nicht zahlen. Geben Sie niemals Geld aus, um an einen vermeintlichen Gewinn zu kommen.
- Lassen Sie sich nicht einschüchtern. Auch von angeblichen Amtspersonen wie Notaren nicht. Private Informationen bleiben privat.

## Fall 6: Abzocke durch angeblichen Homeoffice-Support

Martina B. Telefon klingelt. Gestresst nimmt sie den Hörer ab. Sie hat sich gerade erst halbwegs im Homeoffice eingerichtet. Der Mann am anderen Ende stellt sich als Mitarbeiter eines IT-Dienstleisters für Home-Office-Software vor. In gebrochenem Deutsch erklärt er Martina B., dass es mit dem Sicherheitszertifikat auf ihrem Firmenlaptop noch ein kleines Problem gibt und er nur kurz etwas installieren müsse. Genervt gibt Martina B. ihm Zugriff zu ihrem Rechner. Das hat ihr gerade noch gefehlt.

### Das sollten Sie wissen:

#### Abzocke durch angeblichen Homeoffice-Support

In Deutschland sitzen gerade unzählige Beschäftigte im Homeoffice. Für einige ist das eine neue und ungewohnte Situation, die Trickbetrüger als Einfallstor nutzen. Hier gilt es, besonders achtsam bei Anrufen angeblicher Homeoffice-Supports oder beim Öffnen unbekannter Phishing-Mails mit vermeintlicher Homeoffice-Software zu sein. Meist auf Englisch oder gebrochenem Deutsch rufen Kriminelle Menschen im Homeoffice an und kündigen an, eine Fernwartungs-Software auf ihre Rechner spielen zu müssen, da es Probleme mit dem Computersystem des Unternehmens gäbe. So gelingt es den Tätern, an sensible Daten zu kommen.

### So schützen Sie sich:

- Seriöse IT-Dienstleister melden sich nicht unaufgefordert bei Ihnen. Sollten Sie einen solchen Anruf erhalten: Legen Sie einfach den Hörer auf.
- Gewähren Sie unbekannten Anrufern niemals Zugriff auf Ihren Rechner.
- Haben Sie eine Mail zur Installation einer Homeoffice-Software bekommen? Wenden Sie sich direkt an ihren firmeneigenen IT-Dienstleister und fragen Sie im Zweifel nach, ob die Software in der angezeigten E-Mail die richtige ist.

### Fall 7: Abzocke durch angebliches Corona-Impfstoffpaket

Herbert G. war gerade von einem Spaziergang wiedergekommen, als sich ein angeblicher Mitarbeiter einer bekannten Impfstofffirma am Telefon meldet. Er habe die Möglichkeit Herrn G. ein erstes Corona-Impfstoffpaket zum Preis von 6.000 Euro anzubieten. Der Impfstoff soll nach der Zahlung per Post zugesendet werden. Das Geld sollte Herbert G. an der Tür einem Mitarbeiter der Impfstofffirma übergeben. Herbert G. überlegte, er selbst war Risikopatient und hatte in den Nachrichten gehört, dass der Impfstoff inzwischen in der EU zugelassen wurde. Dennoch ist er unsicher, ob der Impfstoff einfach per Post verschickt werden kann. Nach dem Telefonat informiert er sich beim Gesundheitsamt. Als ein vermeidlicher Geldabholer klingelte, war die Polizei bereits vor Ort.

#### Das sollten Sie wissen:

**Abzocke durch angebliches Corona-Impfstoffpaket**

Impfstofffirmen verkaufen ihre Impfstoffe, wie den für COVID-19, nicht über das Telefon oder an der Haustür. Daher ist bei Anrufern, die sich als Mitarbeiter von Impfstofffirmen ausgeben und Geld fordern oder sich für sensible Daten interessieren, stets Vorsicht geboten. Informieren Sie sich über aktuelle Entwicklungen bei seriösen Quellen, wie dem örtlichen Gesundheitsamt, dem Gesundheitsministerium oder dem Robert-Koch-Institut.

#### So schützen Sie sich:

- Lassen Sie sich nicht auf ein Gespräch am Telefon oder an der Haustür ein. Legen Sie den Hörer auf oder schließen Sie umgehend Ihre Wohnungstür und verständigen Sie die Polizei.
- Übergeben Sie kein Geld an Ihnen fremde Personen
- Informieren Sie sich beim örtlichen Gesundheitsamt oder bei offiziellen Stellen über die Impfstoffvergabe.

## *2. Corona-Maschen an der Haustür*

### Fall 1: Der Handwerker-Trick – Corona-Betrüger an der Haustür

Als es an der Wohnungstür klingelt, öffnet Hedwig B. und lässt einen vermeintlichen Handwerker in die Wohnung. Der junge Mann bietet an, die Räume als Schutz vor Corona zu desinfizieren. Während des Gesprächs schlüpft ein Komplize durch die angelehnte Haustür in die Wohnung und entwendet Bargeld und Wertsachen. Verärgert erstattet Hedwig B. Anzeige bei der Polizei.

#### Das sollten Sie wissen:

### Der Handwerker-Trick – Corona-Betrüger an der Haustür

Trickbetrüger schlüpfen in jede erdenkliche Rolle, um ältere Menschen an der Haustür zu betrügen. Bei diesen kriminellen Methoden überreden und überrumpeln sie ihr Gegenüber und geben sich bspw. als Handwerker, Mitarbeiter des Gesundheitsamtes oder des Katastrophenschutzes aus, um kostenpflichtige Corona-Tests, Wohnungsdesinfektionen u. ä. durchzuführen oder Spenden für Desinfektionsmittel zu sammeln. Die Unterschrift oder das Bargeld sind dabei ihr Ziel. Um an die Wertsachen zu gelangen, verschaffen sie sich unter einem Vorwand Zugang zur Wohnung. Während ein Betrüger das Opfer ablenkt, schleicht sich eine zweite Person in die Wohnung und raubt sie aus.

#### Keine Geschäfte an der Haustür

- Kaufen und unterschreiben Sie nichts an der Haustür. Lassen Sie sich nicht unter Druck setzen und überreden. Meist sind die Handwerkerleistungen geringwertig oder gar wertlos.
- Es werden keine unangemeldeten Corona-Tests an der Haustür durchgeführt. Diese müssen angeordnet werden und es wird nur in Abstimmung mit Ihrem Arzt oder dem Gesundheitsamt ein fester Termin zum Testen vereinbart.
- Lassen Sie keine Unbekannten in Ihre Wohnung. Das gilt auch für Handwerker, die nicht von der Hausverwaltung angekündigt wurden. Fragen Sie im Zweifel telefonisch nach.
- Reden Sie nicht darüber, wo Sie Ihr Geld oder Ihre Wertgegenstände aufbewahren.
- Falls Sie doch etwas kaufen möchten, dann zahlen Sie niemals im Voraus oder per Vorkasse, sondern immer mit Rechnung.

## Fall 2: Vermeintliche Einkaufshilfe – Betrug in der Nachbarschaftshilfe

Der junge Mann vor seiner Haustür bietet Stefan G. an, seine Einkäufe und den Gang zur Apotheke zu übernehmen. Er soll einfach Geld und Einkaufsliste aus hygienischen Gründen vor der Tür liegen lassen. Stefan G. nimmt die Hilfe des vermeintlichen Mitarbeiters von der Nachbarschaftshilfe dankend an. Er sah ihn und sein Geld nie wieder. Enttäuscht erstattet Stefan G. Anzeige bei der Polizei.

#### Das sollten Sie wissen:

### Vermeintliche Einkaufshilfe – Betrug in der Nachbarschaftshilfe

Seit Ausbruch des Coronavirus sind gerade Risikogruppen wie Seniorinnen und Senioren verstärkt auf Hilfe von außen angewiesen. Sie müssen ihren Alltag neu organisieren. Diese Notlage nutzen Betrüger unter dem Deckmantel der Nachbarschaftshilfe aus. Sobald Einkaufszettel und Geld vor der Tür abgelegt wurden, verschwinden die Trickbetrüger.

### Nachbarschaftshilfe – aber richtig!

- Lassen Sie sich nur von Menschen helfen, die Sie persönlich kennen und sprechen Sie die Hilfe vorher ab!
- Am besten bitten Sie über bekannte Institutionen (Kirche, Gemeinde, DRK…) um Hilfe und sprechen Sie mit der Organisation ab, wie Sie den Helfenden an der Haustür erkennen können (Name, Ausweis…).
- Aus Schutz vor dem Coronavirus: Nehmen Sie Einkäufe vor der Haustür entgegen.

## Fall 3: Falsche Vodafone-Mitarbeiter

Bei Susanne S. klingelte es an der Tür. Ein vermeintlicher Vodafone-Mitarbeiter informiert ihn, dass durch die Ausgangsbeschränkungen und das verstärkte Homeoffice das Netz stark überlastet sei, weshalb er kurz in die Wohnung müsse, um den Router auszutauschen und neue Leitungen zu legen. Susanne S. stimmt dem Vorschlag des Vodafone-Mitarbeiters zu und verschaffte damit nichtsahnend Betrügern Zugang zu seiner Wohnung. Bargeld und liebgewonnene Erbstücke wurden entwendet.

### Das sollten Sie wissen:

**Falsche Vodafone-Mitarbeiter**

Trickbetrüger finden immer neue Vorwände, wie sie sich Zugang zu der Wohnung von Opfern verschaffen können. Die Unterschrift oder das Bargeld sind dabei ihr Ziel. Während ein Betrüger das Opfer ablenkt, schleicht sich eine zweite Person in die Wohnung und raubt sie aus.

### So schützen Sie sich:

- Kaufen und unterschreiben Sie nichts an der Haustür. Lassen Sie sich nicht unter Druck setzen und überreden. Meist sind die versprochenen Leistungen geringwertig oder gar wertlos.
- Lassen Sie keine Unbekannten in Ihre Wohnung. Das gilt auch für Mitarbeiter von Vodafone, die nicht von der Firma angekündigt wurden. Fragen Sie im Zweifel telefonisch nach.

- Reden Sie nicht darüber, wo Sie Ihr Geld oder Ihre Wertgegenstände aufbewahren.
- Falls Sie doch etwas kaufen möchten, zahlen Sie es niemals im Voraus oder per Vorkasse, sondern immer mit Rechnung.
- Erstatten Sie Anzeige: Melden Sie solche Vorfälle unverzüglich bei der Polizei.

## 3. Corona-Maschen im Internet

### Fall 1: Verlogene Online-Shops – Betrug mit Atemschutzmasken

Um sich vor Corona zu schützen, bestellt Gabi W. Atemschutzmasken und Desinfektionsmittel in einem Online-Shop. So muss sie das Haus nicht verlassen. Bei Bestellung der Ware, muss sie eine Vorauszahlung tätigen. Doch die Ware wird nie geliefert und die Hotline des Anbieters meldet „Kein Anschluss unter dieser Nummer. Gabi W. wurde arglistig getäuscht. Sie wendet sich hilfesuchend an den WEISSEN RING.

#### Das sollten Sie wissen:

**Verlogene Online-Shops – Betrug mit Atemschutzmasken**

Kriminelle fälschen die Internetshops von bekannten und real existierenden Firmen. Unter einer dem Original ähnlichen Webadresse bieten sie angeblich hochwertige Markenartikel günstig an. Mit kopierten Produktbildern, Informationen und einem gefälschten Impressum gewinnen die Betrüger das Vertrauen der Nutzer. Bestellt der Kunde, werden seine Bank- oder Kreditkartendaten abgefragt. Oft versenden Fake-Shops minderwertige Ware (z. B. Atemschutzmasken) zu einem überhöhten Preis oder liefern nach einer Vorauszahlung nicht. Besonders problematisch: Neben dem erlittenen finanziellen Schaden werden in diesen Fake-Shops auch die Kontodaten der Betroffenen erbeutet.

#### Daran erkennen Sie seriöse Shops:

- Informieren Sie sich über Online-Shops und geben Sie deren Namen in eine Suchmaschine ein. Dadurch können Sie negative Erfahrungen anderer Kunden ausfindig machen.
- Vertrauenswürdige Shop-Anbieter stellen ihren Kunden eine Anbieterkennzeichnung mit vollständigem Impressum zur Verfügung.
- Auch Angaben zu den Allgemeinen Geschäftsbedingungen, Widerrufs- und Rückgaberechten sowie den Daten-

schutzbestimmungen geben Aufschluss über die Seriosität eines Online-Händlers.

- Es gilt: Vorsicht bei unbekannten Internet-Shops. Bei einem Verdacht auf Betrug wenden Sie sich umgehend an die Polizei und die Verbraucherzentralen.

Wahl des Zahlungswegs:

- Der Kauf auf Rechnung kann vor Betrug durch Fake-Shops schützen. Überweisungen können nur kurzfristig rückgängig gemacht werden. Beim Lastschriftverfahren können vorgenommene Abbuchungen noch nach einigen Tagen storniert werden. Zahlen Sie niemals per Vorkasse Geld an Anbieter.

## Fall 2: Fragwürdige Apps zu Corona

Lars W. ist sehr zufrieden. Er hat eine App entdeckt, die ihn in regelmäßigen Abständen über das Coroanvirus auf dem Laufenden hält. So bleibt er informiert und muss nicht aktiv selbst nach neuen Informationen im Netz suchen. Außerdem bietet die App Hilfestellungen an, sollte Lars W. Symptome an sich feststellen. Nachdem er die App gestartet hat, erscheinen plötzlich Lösegeldforderungen zur Entsperrung seines Geräts auf dem Bildschirm. Lars ist einer Fake-App für Covid-19 zum Opfer gefallen.

### Das sollten Sie wissen:

#### Fragwürdige Apps zu Corona

Das Informationsbedürfnis der Menschen zu Covid-19 auf dem Laufenden zu bleiben, nutzen Kriminelle aus, indem sie fragwürdige Covid-19 Tracker-Apps zum Download anbieten. Leider halten die Apps nach der Installation ihr Versprechen nicht. Sie vermitteln entweder (gefährliches) Halbwissen, Fake News (Google löschte gerade eine rechtsextreme App aufgrund von Fake News zum Coronavirus), zeigen nervige Werbeanzeigen an oder im Zweifel wird im Hintergrund sogar Schadsoftware heruntergeladen. Mithilfe der Ramsoftware erhalten Kriminelle Zugriff auf das Smartphone und können die Passwörter ändern. Sie fordern dann Geld zur Freischaltung des Geräts.

**Hinweis**: Die Corona-Datenspende-App des Robert Koch-Instituts soll helfen, die Ausbreitung des Coronavirus in Deutschland besser zu verstehen. Mit Erscheinen der neuen App könnte die Betrugsmasche mit fragwürdigen Apps in naher Zukunft an noch größerer Relevanz gewinnen. Mögliche Fake-Corona-Apps können für Betrüger ein Einfallstor darstellen.

### So schützen Sie sich:

- Die Corona-Datenspende-App ist kein Corona-Test! Installieren Sie keine Apps auf dem Smartphone oder Software auf dem Computer, die Ihnen Tests gegen den

Virus versprechen. Die App funktioniert pseudonymisiert, sie fragt nicht nach Ihrem Namen.

- Prüfen Sie vor der Installation von Apps die Vertrauenswürdigkeit des App-Anbieters. Ist das Impressum und die Datenschutzerklärung im Store vollständig und vertrauenswürdig? Herausgeber der Corona-Datenspende-App ist das Robert Koch-Institut.

- Laden Sie grundsätzlich Apps für Android nur aus dem Google Play Store und für iOS nur aus dem App Store von Apple herunter.

## 4. Corona-Maschen mit Phishing

### Fall 1: Phishing-E-Mails: Betrüger nutzen Corona-Pandemie aus

„Ihre Sicherheit und Ihre Gesundheit und auch die unserer Mitarbeiter liegt uns sehr am Herzen." - Klaus W. hat eine E-Mail von seiner Bank bekommen. Die kleine Filiale im Ort sei vorerst zum Schutz aller Beteiligten geschlossen. Zur Gewährleistung einer reibungslosen Kommunikation soll Klaus W. nur kurz auf einer Webseite seine Adresse(n), Telefonnummer(n), Passwort und seine E-Mail-Adressen aktualisieren. Die Mail und der externe Link kommen Klaus W. jedoch verdächtig vor. Er wendet sich an seine Bank, um die Echtheit der Mail zu überprüfen. Beinahe wäre er einer betrügerischen Phishing-E-Mail ins Netz gegangen. Die Nachricht leitet er an die Verbraucherzentrale weiter und löscht sie umgehend aus seinem Postfach.

Das sollten Sie wissen:

**Phishing-E-Mails - Betrüger nutzen Corona-Pandemie**

Bei Phishing-Mails (engl. frei übersetzt „nach Passwörtern fischen") haben es Kriminelle auf Passwörter, Konto- oder Kreditkarteninformationen und andere sensible Daten abgesehen. Das Vorgehen beim Phishing ist relativ einfach: über gefälschte E-Mails im Namen seriöser Kreditinstitute werden die Mailempfänger aufgefordert einem Link zu folgen. Auf der verlinkten Seite werden anschließend aus vermeintlichen Sicherheitsgründen, zum Datenabgleich oder anderen Vorwänden, sensible Informationen abgefragt. Diese landen jedoch bei Betrügern, die die entsprechenden Daten zum Missbrauch und zur Schädigung der Opfer nutzen. In Zeiten von Corona nutzen Betrüger das Bedürfnis der Bevölkerung nach gesicherten Erkenntnissen zur aktuellen Lage schamlos aus. Kriminelle schreiben gefälschte Mails im Namen der WHO, der Gesundheitsämter oder anderen Institutionen.

So schützen Sie sich vor Phishing-Mails

- Seien Sie skeptisch bei unbekanntem Absender, Rechtschreibfehlern, unbekanntem Link –auf solche Nachrichten nicht antworten und keine Dateianhänge oder Links öffnen!
- Kontaktieren Sie im Zweifel den Absender, um sich über die Echtheit der Nachricht zu vergewissern. Suchen Sie die Kontaktdaten selbst heraus. Nutzen Sie nicht die in der Mail angegebenen Telefonnummern.
- Vertraulichen Daten (PINs, TANs, Passwörter, ...) werden von seriösen Banken grundsätzlich nicht per E-Mail, Telefon oder Post bei Ihnen abgefragt. Im Zweifel kontaktieren Sie Ihre Bank.
- Veränderungen im Ablauf des Online-Bankings sollten Sie misstrauisch machen. Geben Sie persönliche Daten nur bei gewohntem Verlauf innerhalb des Online-Banking an. Kommt Ihnen etwas seltsam vor, beenden Sie die Verbindung und versuchen Sie es erneut.
- Nutzen Sie möglichst eine Zwei-Faktor-Authentisierung. Durch die Absicherung mit einem zweiten Faktor bei der Identifizierung können Kriminelle Ihre Daten nicht abgreifen, auch wenn sie bereits Ihr Passwort erbeutet haben.

## Fall 2: Phishing mit Fake-Websites für Soforthilfeanträge

„Sie erhalten bis zu 30.000 Euro Soforthilfe vom Staat ohne Rückzahlung.“ Norbert H. ist erleichtert, als er das auf der Website des Soforthilfeprogramms der Bundesregierung las. Endlich kann der Unternehmer einen Kredit für Soforthilfe in Zeiten der Corona-Pandemie beantragen. Eine Mitarbeiterin des Soforthilfeprogramms hatte ihn sogar angerufen und ihn darauf aufmerksam gemacht, dass die Beantragung nun online auf dieser Website möglich ist. Er müsse nur kurz das vermeintliche Antragsformular auf der Website ausfüllen und hochladen. Was Norbert H. erst zu spät merkt: Er ist von der Anruferin auf eine Fake-Seite gelotst worden, das Fake-Formular dient dem Klau von Unternehmensdaten, um später damit Missbrauch zu begehen.

### Das sollten Sie wissen:

#### Phishing mit Fake-Websites für Soforthilfeanträge

Betrüger haben es auch auf die in Not geratenen Wirtschaftsunternehmen abgesehen. Bei Phishing (engl. frei übersetzt „nach Passwörtern fischen“) mit Fake-Websites und Fake-Formularen haben es Kriminelle wie bei Phishing-Mails auf Passwörter, Konto- oder Kreditkarteninformationen und andere sensible Daten von Unternehmen abgesehen. Das Vorgehen ist relativ einfach: Die Betrüger*innen lotsen Unternehmen auf ihre Fake-Websites, bspw. indem sie sich am Telefon

als Mitarbeiter*innen der Abwicklungsstelle für Soforthilfen ausgeben, um die Unternehmen gezielt auf die Fake-Formulare aufmerksam zu machen. Sobald die Unternehmen ihre Daten in die Formulare eingeben und hochladen, können sie mit diesen Daten Missbrauch betreiben.

In jüngster Zeit sind noch weitere Fälle von Fake-Websites bekannt geworden. So kursiert weltweit laut Bundesamt für Sicherheit in der Informationstechnik (BSI) eine englischsprachige Website mit einer sogenannten „**Corona-Karte**“, die in Echtzeit die Infektionen aktualisiert. Durch das Öffnen der Karte wird im Hintergrund Spyware heruntergeladen, die wie bei Phishing-Mails sensible Daten wie Passwörter und Zugangsdaten auslesen. Aktuelle Ereignisse eignen sich für Kriminelle sehr gut, um die Glaubwürdigkeit von Spam-Mails oder Websites zu erhöhen.

### So schützen Sie sich:

- Achten Sie bei der Antragsstellung für Soforthilfe genau darauf, ob Sie wirklich auf der offiziellen Website des zuständigen (Wirtschafts-)Ministeriums oder der Landesförderbanken (KfW) gelandet sind.
- Wenn Sie sich unsicher sind, rufen Sie selbst die entsprechende Stelle unter der offiziellen Nummer an und fragen Sie dort nach.
- Aktualisieren Sie regelmäßig Updates und achten Sie auf eine sichere Verbindung zum Browser: Neben dem https:// ist auch das Schlosssymbol in der Adressleiste ein Hinweis auf eine sichere Verbindung. Ist es geschlossen ist die Internetverbindung gesichert, ist es geöffnet, besteht keine sichere Verbindung.
- Seriöse Websites verfügen immer über ein vollständiges Impressum und eine Datenschutzerklärung. Diese fehlen bei Fake-Websites häufig oder es sind Adressen aus dem Ausland angegeben.

## Fall 3: Erpressermails mit Corona-Spam

Thomas F. traut seinen Augen kaum. Er hat eine E-Mail bekommen, in der ihm gedroht wird, dass er und seine Familie mit dem Coronavirus infiziert werden, sollte er innerhalb der nächsten 24 Stunden keine 4000 US-Dollar in Bitcoin überweisen. Besonders irritierend: Der Absender kannte einzelne Passwörter von Thomas F. Hilfesuchend wendet er sich an die Verbraucherzentrale.

### Das sollten Sie wissen:

### Erpressermails mit Corona-Spam

Phishing-Mails rund um Corona kursieren in vielen Formen. Die Erpresserbotschaft mit drohender Sars-CoV-2-Infizierung ist eine abgewandelte Form. Dahinter verstecken sich leere Drohungen, die vermeintlich „echten“ Passwörter stammen laut heise.de häufig aus früheren Passwort-Leaks und werden für solche Zwecke missbraucht. Die E-Mails werden wahllos an einen Personenkreis geschickt – manchmal mit persönlicher Anrede, manchmal ohne – mit dem Ziel durch Panikmache die Bereitschaft zur Lösegeldzahlung zu erhöhen.

So schützen Sie sich:

- Zahlen Sie niemals Geld an Kriminelle! Leiten Sie solche Erpressungsversuche umgehend an Polizei und Verbraucherzentralen zur Kenntnis weiter.
- Ändern Sie Ihr Passwort, sollte Ihr echtes Passwort in solch einer Mail auftauchen.
- Seien Sie skeptisch bei unbekanntem Absender oder Rechtschreibfehlern: Solche Mails arbeitet zurzeit mit griechischen Buchstaben, um Spam-Filter zu umgehen.

## 5. Was tun, wenn Sie Opfer wurden?

Bei aller Vorsicht am Telefon, an der Haustür oder im Netz kann es trotzdem passieren, dass Personen Betrügern zum Opfer fallen. Dann können folgende Tipps helfen, weitere Schäden zu vermeiden.

### Widerrufsrecht

Wenn Sie einen Vertrag an der Haustür oder am Telefon abgeschlossen haben, können Sie diesen innerhalb von 14 Tagen ohne Angabe von Gründen widerrufen. Das Widerrufsrecht gilt jedoch nicht, wenn Sie den Vertreter selbst bestellt haben oder wenn es sich um ein Bagatellgeschäft (bis 40 Euro) handelt.

### Fake-Shops

- Zahlung rückgängig machen: Sollten Sie bereits Geld für Ihren Kauf überwiesen haben, versuchen Sie die Zahlung bei Ihrer Bank rückgängig zu machen. Dies ist innerhalb eines bestimmten Zeitraums in der Regel noch möglich. Bei anderen Zahlungsarten kontaktieren Sie sofort den Dienstleister und lassen ihn die Transaktion stoppen.

- Beweise sichern: Bewahren Sie alle Belege für Ihren Kauf, wie zum Beispiel E-Mails auf. Drucken Sie diese aus.

- Erstatten Sie Anzeige: Auch wenn die strafrechtliche Verfolgung von Internetbetrügern oft schwierig ist, sollte trotzdem Anzeige erstattet werden. Nur so können die Behörden gegen Fake-Shops vorgehen.

### Phishing-Mails, -Websites und Homeoffice-Support

- Sie haben auf den Link geklickt – und jetzt? Sollten Sie Geldforderungen zur Entsperrung ihres PCs von Unbekannten bekommen: Zahlen Sie kein Geld an Kriminelle! Kontaktieren Sie die Polizei, Verbraucherzentralen oder Hilfsorganisationen wie den WEISSEN RING.

- Schadsoftware ist auf Ihrem Rechner installiert? Nehmen Sie Ihren Rechner umgehend vom Netz und fahren ihn herunter. Ändern Sie alle Passwörter über einen nicht infizierten Rechner.

- Sie befürchten, dass Ihre Daten abgeschöpft wurden: Ändern Sie Ihr Passwort und erstatten Sie Anzeige! Übergeben Sie den infizierten Rechner in professionelle Hände, z.B: an das IT-Team Ihrer Firma und lassen Sie die schädliche Software entfernen.

- Kontrollieren Sie Ihr Konto. Sollten Sie hierbei Auffälligkeiten feststellen, können Sie schnell reagieren, ihre Bank informieren und das Konto gegebenenfalls sperren lassen.

**Weitere Informationen zu dem Thema:**

- Bundeskriminalamt
- ProPK Polizeiliche Kriminalprävention
- Robert-Koch-Institut
- Bundesamt für Sicherheit in der Informationstechnik