Vorsicht, Betrug!

Hohe Rendite, schnelles Geld, vermeintlich harmlose Mails und Jobangebote von der BaFin: Betrüger versuchen alles Mögliche, um Geld oder Daten von Verbraucherinnen und Verbrauchern abzugreifen. Wie Sie sich schützen können.

Betrug am Finanzmarkt hat viele Gesichter und fängt oft harmlos an:

- Die Rentnerin Ilse Meier erhält ungewollt einen Anruf eines Finanzberaters, der ihr die einmalige Chance bietet, aus einer sofortigen Investition von ein paar hundert Euro ganz einfach und ohne Risiko mehrere tausend Euro zu machen.
- Die Studentin Luisa Schneider wird per E-Mail aufgefordert, einem Link auf die Website einer Bank zu folgen und dort sofort ihren Online-Banking-Zugang zu aktualisieren.
- Der arbeitssuchende Hans Wagner wird im Internet auf ein lukratives Jobangebot als Finanzagent im Treuhandservice aufmerksam.

Die hier benannten Personen sind fiktiv, ihre Probleme Realität.

Welche Gefahren für Verbraucher am Finanzmarkt lauern, auf welche Warnsignale Sie achten sollten, wie Sie sich schützen können und was zu tun ist, wenn Sie Opfer eines Betrugs geworden sind, erfahren Sie in diesem Artikel.

Achtung, Anlagebetrug!
Der Anruf des Finanzberaters bei Frau Meier ist gleich in mehrfacher Hinsicht alarmierend:

Unerbetener Anruf? Nein danke!
Auf einen unaufgeforderten Anruf sollten Sie erst gar nicht eingehen. Denn Wertpapierunternehmen und anderen Finanzdienstleistern sind solche Lockanrufe, im Englischen auch als Cold Calling bekannt, untersagt. Wer Verbraucher wahllos anruft, ist schlichtweg unseriös und sein Angebot ist mit hoher Wahrscheinlichkeit eine Abzocke.

Es ist nicht alles Gold, was glänzt. Kritisch bleiben!
Unseriöse Anbieter versuchen, Verbraucher nicht nur telefonisch, sondern auch per E-Mail, in sozialen Netzwerken, auf seriös präsentierten Websites und über vielversprechende digitale Werbeanzeigen zu ködern. Betrüger benutzen auch gerne bekannte Persönlichkeiten oder Unternehmen ohne deren Wissen als Referenz in der Werbung. Die Investitionsangebote werden zumeist aggressiv als heißer Anlagetipp in angesagte Anlageobjekte oder Branchen beworben. Darunter fallen Edelmetalle, Kryptowährungen, Start-ups oder regenerative Energien.

Hohe Rendite und kein Risiko? Gibt es nicht!
Ungewöhnlich hohe Zins- oder Renditeversprechen, die weit über dem üblichen Marktniveau liegen, können für sich genommen ein Hinweis auf ein unseriöses Angebot sein.

> Hinweis
>
> Grundsätzlich gilt: Je höher der versprochene Gewinn, desto höher ist in der Regel auch das Risiko, das eingesetzte Kapital zu verlieren.

© ronstik/stock.adobe.com

Nur jetzt und sofort?
Wenn ein Anbieter Druck ausübt und Sie sich sehr schnell entscheiden müssen, dann ist das häufig ein Trick. Lassen Sie sich nie drängen, denn seriöse Angebote gibt es nicht nur heute, sondern auch morgen.

Seriöse Geldanlage oder falsche Versprechungen? Prüfen Sie nach!
Die Maschen von Betrügern sind vielfältig. Manche Unternehmen, häufig ohne Geschäftstätigkeit und mit Sitz außerhalb der Europäischen Union (EU), werden einzig zu dem Zweck gegründet, Anleger abzuzocken. Informieren Sie sich daher im Vorfeld genau über den Anbieter und worin Ihr Geld konkret investiert werden soll.

Unseriöse Anbieter nutzen auch gerne illiquide, also wenig gehandelte Aktien, oder solche, die nur im Cent-Bereich notieren, im Englischen Penny Stocks genannt, um sie als vermeintliche Schnäppchen anzubieten. Häufig sind das Aktien oder andere Wertpapiere aus dem Freiverkehr einer Börse. Denn in diesem Segment bestehen nur geringe Informationspflichten. Betrüger erzeugen mit einer aggressiven Verkaufsstrategie eine künstliche Nachfrage nach solchen illiquiden oder wertlosen Aktien, um den Kurs in die Höhe zu treiben. Dafür nutzen sie oft soziale Netzwerke.

> Hinweis
>
> Was Sie bei Anlagetipps in sozialen Medien beachten müssen, erfahren Sie hier.

Die Betrüger oder dritte Personen, mit denen sie zusammenarbeiten, haben die Aktien zuvor längst zu einem niedrigen Kurs erworben, um sie nach einer Kurssteigerung gewinnbringend zu verkaufen. Danach stürzt der Kurs ins Bodenlose und die ahnungslosen Anleger müssen herbe Verluste hinnehmen oder gehen sogar leer aus. Bei dieser Masche handelt es sich um eine strafbare Marktmanipulation, das Scalping (englisch für skalpieren).

Schnelles Geld für alle? Augen auf!
Eine weitere bekannte Betrugsmasche ist das Schneeballsystem. Hierbei wird Anlegern ebenfalls eine gewinnbringende Geldinvestition vorgetäuscht. In Wirklichkeit werden die Einlagen neuer Investoren aber zum Teil als Scheingewinne an andere Investoren ausgezahlt, der Rest fließt in die Tasche der Anbieter. Neue Investoren erhalten häufig zur Vertrauensbildung schnell erste Renditen ausbezahlt. Dann ruft der Anbieter seine Opfer an und schlägt vor, mehr Geld einzusetzen. Irgendwann bricht das System zusammen, spätestens wenn nicht mehr genügend neue Investoren angeworben werden können. Das eingesetzte Kapital der ahnungslosen Anleger geht auch hier verloren.

Genau hinschauen!
Schneeballsysteme oder ähnliche Betrügereien findet man in erster Linie am illegalen, dem Schwarzen Kapitalmarkt. Darunter fallen alle Anbieter am Finanzmarkt, die

erlaubnispflichte Finanzgeschäfte unerlaubt anbieten oder sogar verbotene Geschäfte machen. Die Gefahr, dass Anleger bei Geschäften mit solchen Anbietern vollständig ihr Geld verlieren, ist sehr hoch.

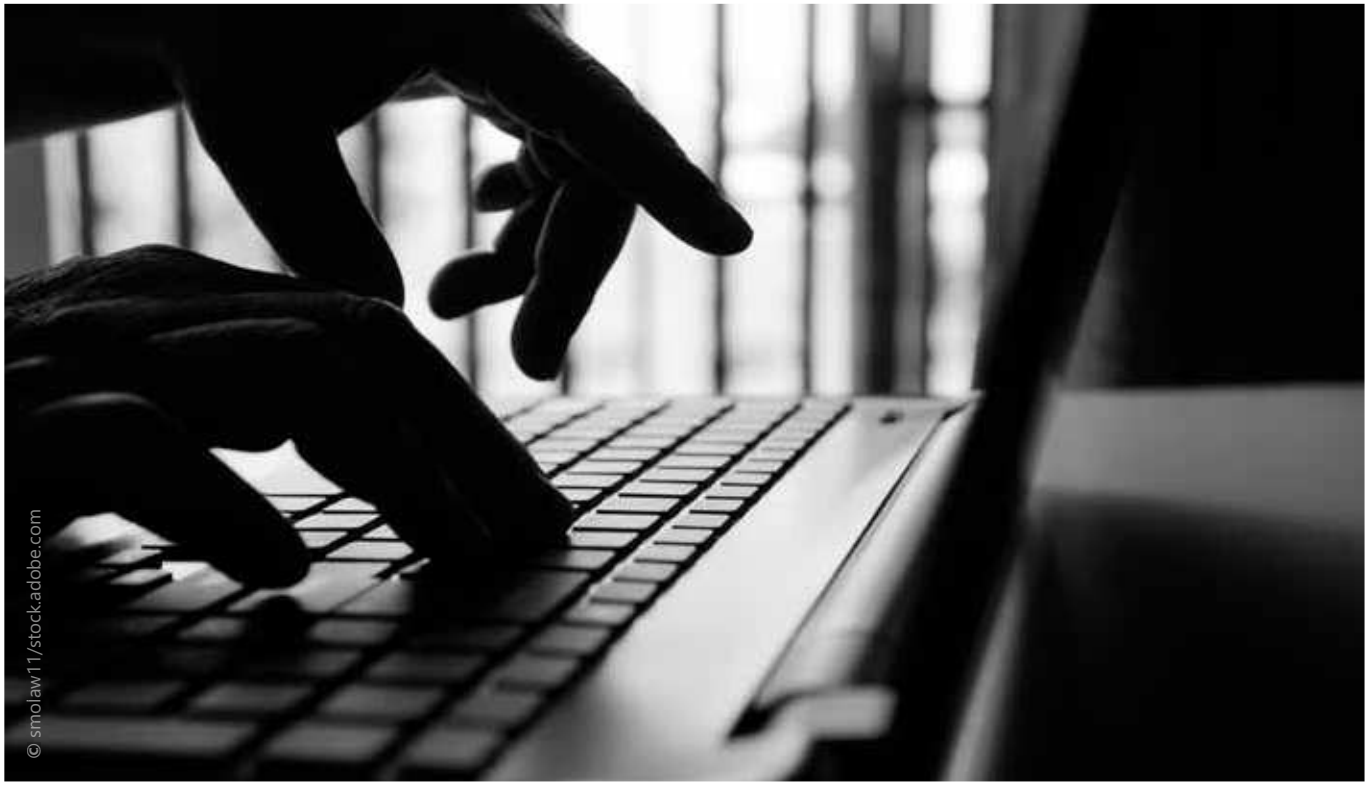
> Hinweis
>
> Warnungen vor solchen unerlaubt tätigen Unternehmen, gegen die die BaFin formell eingeschritten ist, finden Sie auf der Website der BaFin. Dort warnt die BaFin auch vor Marktmanipulationen oder Verletzungen der Prospektpflicht.

Bei Angeboten am Grauen Kapitalmarkt sollten Sie ebenfalls vorsichtig sein. Man spricht vom Grauen Kapitalmarkt, wenn Anbieter für den Vertrieb ihrer Produkte keine Erlaubnis der BaFin benötigen und nicht unter der laufenden Aufsicht der BaFin stehen. Das ist etwa bei Unternehmensbeteiligungen, Direktinvestments (zum Beispiel in Container, Holz, Edelmetalle), Genussrechten, Nachrangdarlehen und vielen Crowdfunding-Angeboten der Fall. Nicht alle Angebote am Grauen Kapitalmarkt sind unseriös. Sie sollten aber in solche Produkte nur dann investieren, wenn Sie deren Funktionsweise und Risiken verstehen und von dem Unternehmen und seinem Geschäftsmodell hundertprozentig überzeugt sind.

Unter staatlicher Aufsicht

In Deutschland erteilt die BaFin Finanzinstituten, die Bank-, Finanzdienstleistungs- und Versicherungsgeschäfte betreiben wollen, eine Erlaubnis und überwacht die Einhaltung der jeweiligen Aufsichtsgesetze.

> Hinweis
>
> Listen der Unternehmen, die die BaFin zugelassen hat, finden Sie auf der Website der BaFin. Dort können Sie auch nach hinterlegten Prospekten und Informationsblättern für Wertpapiere und Vermögensanlagen suchen.

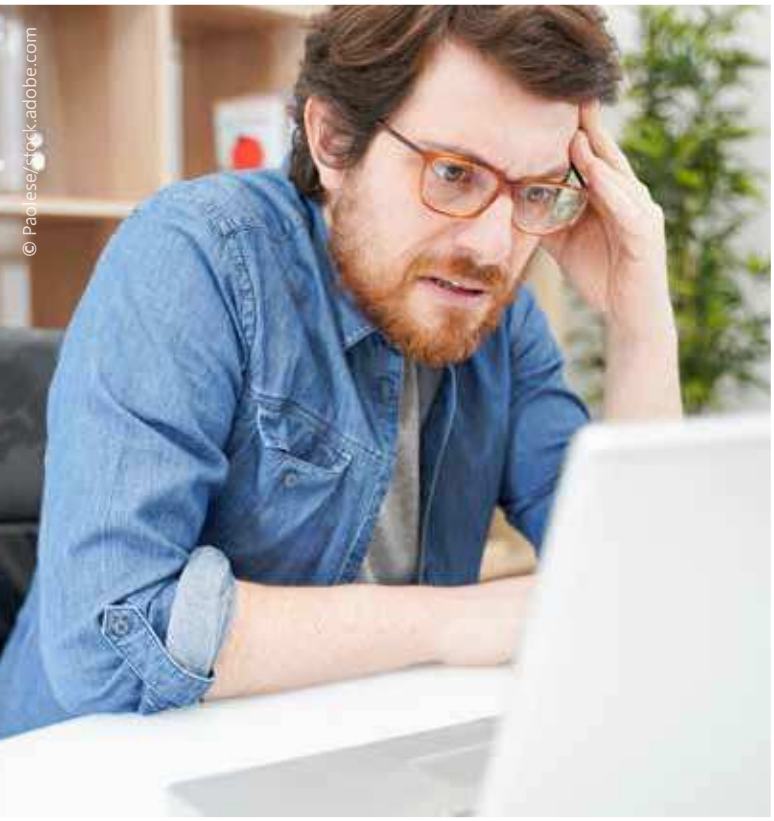


© smolaw11/stock.adobe.com

Werbung mit der BaFin – ein Gütesiegel?
Lassen Sie sich nicht dadurch blenden, dass ein Anbieter damit wirbt, von der BaFin beaufsichtigt zu werden oder einen von ihr gebilligten Prospekt zu haben. Die Aufsicht und die Prospektprüfung durch die BaFin unterliegen rechtlichen Grenzen. Abgesehen davon ist die Werbung eines Anbieters mit der BaFin grundsätzlich unzulässig.

Selbst wenn ein Unternehmen sich an alle Regeln hält, können Sie bei einer Geldanlage, je nach Produkt und vertraglicher Regelung, Verluste erleiden oder Ihr Geld vollständig verlieren. Informieren Sie sich vor Abschluss eines Geschäfts daher selbst, wie und wann Sie Ihren Anlagebetrag zurückerhalten und inwieweit ein vertraglicher Rückzahlungsanspruch besteht.

Bleiben Sie wachsam!
Es gibt ein paar einfache Regeln, wie Sie sich vor unseriösen Angeboten am Finanzmarkt schützen können:

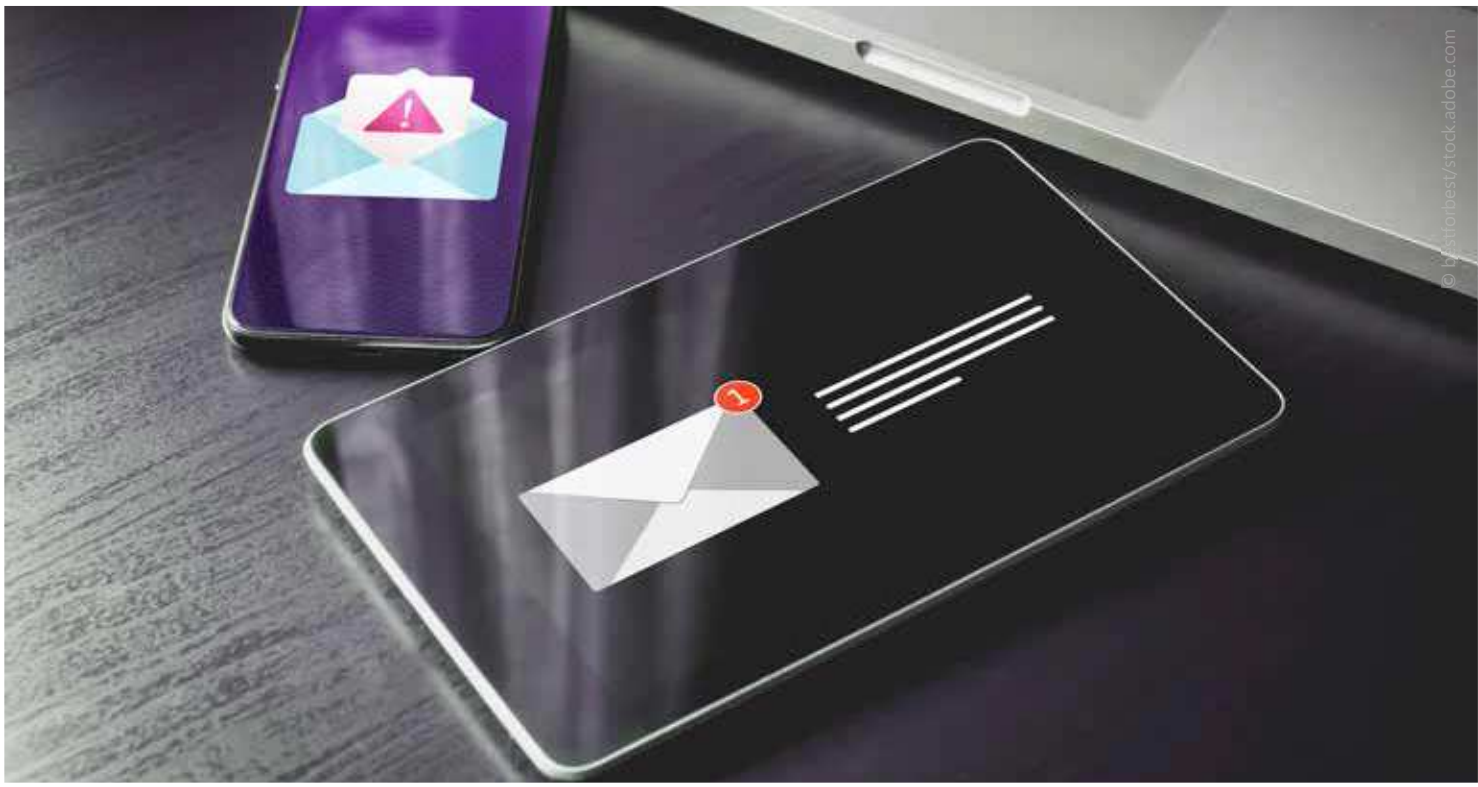


- Lassen Sie sich nicht drängen!
  Nehmen Sie sich ausreichend Bedenkzeit und beraten Sie sich gegebenenfalls mit einer Vertrauensperson.
- Machen Sie keine Geschäfte mit Anbietern, die keine transparenten Informationen zur Verfügung stellen.
  Wenn Sie das Vertragswerk nicht verstehen, lassen Sie die Finger von dem Angebot.
- Prüfen Sie vor Abschluss eines Geschäftes genau, inwieweit ein Rückzahlungsanspruch vertraglich festgelegt ist.
- Haben Sie Zweifel, dann investieren Sie nicht!
  Können die Zweifel auch bei einer Beratung nicht beseitigt werden, investieren Sie unter keinen Umständen!

> Hinweis
>
> Die BaFin hat auf ihrer Webseite verschiedene Broschüren für Verbraucher veröffentlicht, zum Beispiel zu den Themen „Geldanlage – Wie Sie unseriöse Anbieter erkennen“ und „Achtung Marktmanipulation“.

Cyberkriminalität
Straftaten mithilfe moderner Informationstechnik oder im Internet werden als Cyberkriminalität bezeichnet. Die kann zum Beispiel mit einer E-Mail beginnen, wie sie Frau Schneider erhielt.

Woher kommt die E-Mail?
Bei solchen betrügerischen E-Mails handelt es sich um das Phishing (im Deutschen: fischen). Die E-Mails werden von automatischen Programmen an alle möglichen Buchstaben- bzw. Vor-/Nachnamen-Kombinationen bei bekannten E-Mail-Providern versendet. Als Absender werden zum Beispiel Banken angegeben. Die Empfänger, wie Frau Schneider, können auf den ersten Blick oft nicht erkennen, ob es sich um eine echte Nachricht ihrer Bank oder einen Betrugsversuch handelt. Der Betreff (zum Beispiel „Ihre Überweisung“) wird so gewählt, dass die Empfänger neugierig werden, die E-Mail öffnen und die gewünschten Daten angeben, wie etwa die PIN und TAN aus dem Internet-Banking, die die Betrüger dann abfischen.



Eine andere Variante der Phishing-Mail sind Banking-Trojaner. Die E-Mails enthalten dabei einen Link oder eine angehängte Datei mit Schadsoftware, die sich nach Anklicken oder Download auf dem Rechner oder mobilen Endgerät des Empfängers installiert. Diese täuscht beispielsweise eine Log-in- oder Eingabe-Maske der Hausbank vor, greift Daten ab oder arbeitet im Hintergrund und manipuliert Überweisungen so, dass das Geld an das Konto der Betrüger umgeleitet wird. Diese Risiken bestehen ebenfalls beim Bezahlen im Internet oder beim Onlinekauf und -verkauf.

Kann man dieser Nummer vertrauen?

Das Vishing („Voice"=Stimme und „Phising"=fischen) ist eine Mischung aus technischer und emotionaler Manipulation. Betrüger manipulieren die Internettelefonie-Technologie (Voice-over-IP), um ihre Identität und Rufnummer zu verschleiern. Dies führt dazu, dass auf dem Telefon der angerufenen Person die vermeintlich echte Telefonnummer beispielsweise einer Bank erscheint, in Wahrheit aber ein Betrüger anruft. Dieser denkt sich eine für das Opfer augenscheinlich verständliche Geschichte aus, womit er die Person unter Druck setzt und zu einem sofortigen Handeln, wie der Weitergabe von sensiblen Daten, bewegen will.

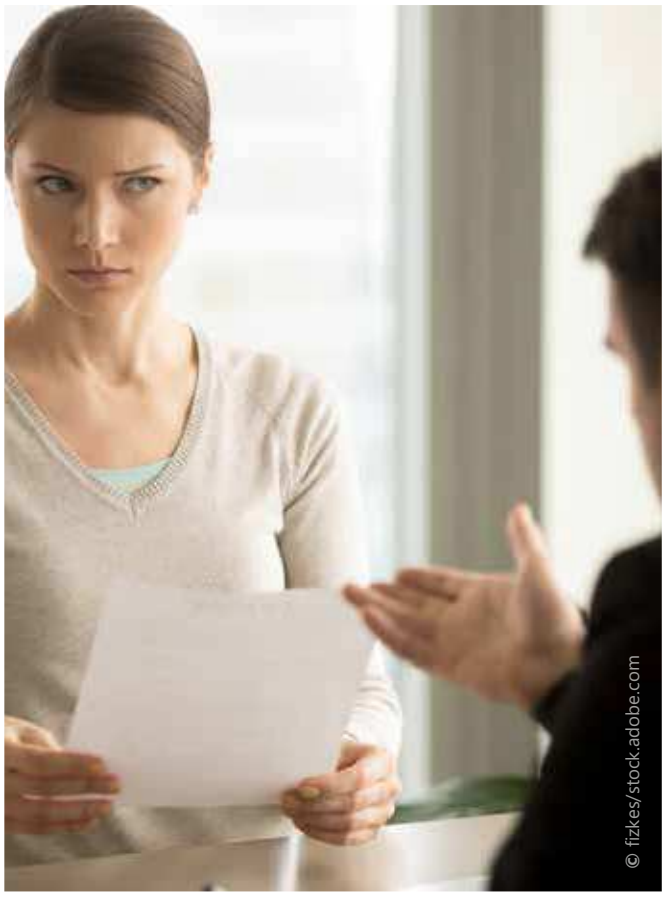
Hier ein Beispiel: Ein Betrüger gibt sich als Mitarbeiter einer Bank aus und versucht mittels geschickter Gesprächsführung die angerufenen Personen dazu zu bewegen, höhere Geldbeträge auf meist ausländische Bankkonten zu transferieren oder Onlinebanking-Daten preiszugeben. In diesen Fällen wird häufig behauptet, dass das Geld der Opfer durch kriminelle Organisationen oder Bankschließungen in Gefahr sei.

Bei einer andere Variante hinterlassen Betrüger eine Nachricht auf dem Anrufbeantworter oder der Mailbox oder senden eine SMS (Smishing). In dieser wird beispielsweise mitgeteilt, dass das Bankkonto der kontaktierten Person von einem Hackerangriff betroffen sei und um Rückruf gebeten. Ruft der Kontaktierte zurück, wird dann anhand einer Bandansage von ihm verlangt,

dass er Bankdaten bzw. Kreditkartendaten benennen soll.

Ist die Seite wirklich echt?
Betrüger imitieren auch immer wieder Websites, zum Beispiel von Banken, so detailgetreu, dass sie nur schwer von Originalseiten unterschieden werden können. Diese Betrugsmasche wird häufig mit dem Phising kombiniert. Dabei erhalten Verbraucher eine E-Mail, über die sie auf die gefälschte Website der Bank geführt werden, damit die Betrüger dort sensible Daten abfischen oder Zahlungen umleiten können.

Darüber hinaus betreiben Betrüger gefälschte Online-Shops (Fake-Shops), auf denen sie Kunden mit hochwertigen Artikeln zu absoluten Dumpingpreisen locken. Die bestellten Waren werden nach der Eingabe von sensiblen Daten und der Bezahlung (meist nur per Vorkasse) aber niemals ausgeliefert. Die Opfer fallen bei dieser Methode auf einen doppelten Betrug herein, da das Geld weg ist und sensible Daten preisgegeben beziehungsweise abgefischt wurden.


© fizkes/stock.adobe.com

Kontoeröffnung beim Bewerbungsgespräch? Passt das zusammen?
Bei dieser Betrugsmasche suchen Betrüger anhand von gefälschten Firmen über Stellenangebote – ausschließlich online – zum Beispiel nach flexiblen Teilzeitbeschäftigten. Die Firmen werben dabei meist mit einem guten Verdienst und großzügigen Home-Office-Möglichkeiten. Das Unternehmen verlangt beim Auswahlverfahren die Eröffnung eines Kontos (welches im Nachgang gelöscht werden soll) und die Bestätigung der Identität anhand eines Video-Ident-Verfahrens. Oder es stellt für die Gehaltszahlung ein Verrechnungskonto bereit, bei dem der Bewerber sich mit seinen persönlichen bzw. sensiblen Daten bei der Digitalbank verifizieren lassen muss. Auf das neu erstellte Konto haben anschließend ausschließlich die Betrüger Zugriff, die es zum Beispiel für die Zahlungsabwicklung von Fake-Shops oder zur Geldwäsche verwenden.

Betrug mit dem Namen der BaFin
Auch bei dem vermeintlichen Jobangebot im Internet, auf das der eingangs erwähnte Herr Wagner gestoßen ist, handelt es sich um eine Variante des Job-Scamming (Jobbetrug), diesmal mit dem Namen der BaFin. Bei einem Job im Treuhandservice sollen Verbraucher über ihr eigenes Konto Gelder weiterleiten, die aus kriminellen Handlungen stammen.

> Hinweis
>
> Achtung: Verbraucher, die im Treuhandservice agieren, können sich selbst strafbar machen.

Immer wieder wird auch der Name der BaFin von Betrügern missbraucht, um sensible Daten von Verbrauchern abzuschöpfen, an deren Geld zu gelangen oder sie für Straftaten zu missbrauchen. Häufig handelt es sich um Phising-Methoden, indem gefälschte E-Mails mit dem Absender „BaFin“ versendet werden.

Betrüger bedienen sich aber auch der Vishing-Methode, indem sie sich als BaFin Mitarbeiter ausgeben.

Eine weitere Betrugsmasche ist das Versenden von gefälschten BaFin-Rechnungen sowohl in deutscher als auch englischer Sprache an Privatanleger.

Sie sollten sehr misstrauisch sein, wenn Sie von der BaFin oder einem vermeintlichen BaFin-Mitarbeiter persönlich kontaktiert werden.

In Wirklichkeit gibt es diese Form der Kontaktaufnahme nicht. Denn die BaFin wendet sich nicht von sich aus an einzelne Personen.

> Hinweis
>
> Die BaFin veröffentlicht regelmäßig Warnungen auf ihrer Internetseite, wenn sie erfährt, dass ihr Name missbräuchlich verwendet wird.

Wie können Sie sich vor Cyberkriminalität schützen?

- Öffnen Sie keine Anhänge, Links oder Bilder in E-Mails, ohne den Absender genau zu kennen oder geprüft zu haben.
- Kontaktieren Sie Ihre Bank oder Sparkasse, wenn Sie unsicher sind und nutzen Sie dafür nicht die Kontaktdaten aus E-Mails.
- Geben Sie den Link zu Ihrer Bank manuell ein.
- Geben Sie keine Bankdaten, TAN-Nummern oder Login-Daten preis.
- Lassen Sie sich nicht unter Druck setzen, unterbrechen Sie und erkundigen Sie sich selbst woanders.
- Nutzen Sie sichere Internetseiten (z.B. „https“) und verschlüsselte Verbindungen.
- Halten Sie Browser, Betriebssystem und Virenschutz auf dem aktuellen Stand.
- Überprüfen Sie Online-Händler, zum Beispiel anhand von Bewertungen und Erfahrungsberichten.
- Achten Sie beim Online-Shopping darauf, welche Zahlungsweisen angeboten werden und bezahlen Sie nicht per Vorkasse bei unbekannten Händlern.
- Überprüfen Sie regelmäßig Ihre Kontoumsätze.

Opfer, und was jetzt?
Wenn Sie Opfer eines Betruges geworden sind oder dies vermuten, informieren Sie Ihre Bank oder Sparkasse und lassen Sie Ihre Karte sperren.

Alternativ können Sie eine Sperrung Ihrer Karte über die Rufnummer 116 116 veranlassen.

Erstatten Sie außerdem Anzeige bei der Polizei. ■

Verfasst von
Thomas Müller
Dennis Stahl
Referat VBS 12