Achtung: Phishing!

Betrug mit Förderprogrammen und „Inflationsschutz“

Die Verbraucherzentrale Bremen informiert

Dr. Annabel Oelmann

Aktuelle Entwicklungen machen sich Kriminelle schnell zunutze. So ist es auch beim Thema Inflation und Energiekrise: Der Betrug kommt per SMS, E-Mail oder auf falschen Internetseiten. In diesem Artikel warnen wir vor verschiedenen aktuellen Betrugsmaschen. Annabel Oelmann, Vorständin und Finanzexpertin der Verbraucherzentrale Bremen, erläutert, wie die Betrüger vorgehen, und gibt Tipps zum Schutz.

Betrügerische E-Mails sehen oft täuschend echt aus. Der Absender klingt seriös, die Nachricht ist nicht völlig abwegig. Misstrauisch sollten Sie jedoch immer sein, wenn Sie aufgefordert werden, persönliche Daten anzugeben, um sich ganz schnell Vorteile zu sichern. Dann könnte es sich um eine Phishing-Mail handeln. Phishing ist ein Kunstwort, das sich aus Passwort und Fishing zusammensetzt. Der Absender „fischt“ nach vertraulichen Da-

ten, um z. B. Zugang zu Ihrem Onlinebanking zu erhalten oder in Ihrem Namen und auf Ihre Kosten Ware im Internet zu bestellen. Derzeit werden u. a. Phishing-Mails verschickt, in denen Sie aufgefordert werden, bestimmte Maßnahmen zur Entlastung in der gegenwärtigen Finanzsituation zu beantragen.

Angebliches Förderprogramm „NextGenerationEU“

Mit einem Bundesadler und den Farben der deutschen Flagge versehen, kommt ein Betrugsversuch per E-Mail, in dem Kriminelle als Absender das Bundesfinanzministerium vorgaukeln. Angeblich könne man im Rahmen eines 750 Milliarden Euro umfassenden Maßnahmenpakets namens „NextGenerationEU“ eigenes Kapital in einen „digitalen Euro“ umschichten. Das werde mit einer Förderung von 29 Prozent auf die getätigte Einlage unterstützt und solle die Kaufkraft erhalten. Bei dieser Behauptung nutzen die Kriminellen den Namen eines tatsächlich existierenden Wiederaufbauprogramms der EU aus, dichten ihm aber weitere Funktionen hinzu.

Angeblich sei das Förderprogramm exklusiv für „sorgfältig ausgewählte Teilnehmer“. Deshalb ist am Ende der E-Mail eine Kombination aus Zahlen und Buchstaben als „persönlicher Zugangsschlüssel“ angegeben. Der ist allerdings bisher in allen an uns weitergeleiteten E-Mails der gleiche.

Der Link in der E-Mail führt auf eine Internetseite, die optisch so gestaltet ist, dass sie tatsächlich eine Seite des Finanzministeriums sein könnte. Jedoch weist die Internetadresse „bundesminsiterium-der-finanzen.com“ auf den Betrug hin. Der Tippfehler im Wort „Bundesministerium“ ist in der tatsächlichen Adresse der Betrugsseite vorhanden.

Wir raten wie üblich dazu, die E-Mail nicht zu beachten. Antworten Sie nicht darauf und klicken Sie nicht auf enthaltene Links! Weitere Details zu diesem Betrugsversuch finden Sie im Online-Ratgeber Internetkriminalität des Landeskriminalamts Niedersachsen: https://www.polizei-praevention.de, Menüpunkt: Aktuelles

Hallo [redacted]

Aufgrund der anhaltenden Inflation in Deutschland, die im Oktober 2022 die Zehn-Prozent-Marke überschritten hat, möchten wir Ihnen im Rahmen des 750 Milliarden Euro schweren "NextGenerationEU" Maßnahmenpakets ein Sonder-Förderprogramm für den Digitalen Euro vorstellen. Dieses Programm entsteht aus einer engen Zusammenarbeit zwischen dem Bundesministerium und der Europäischen Zentralbank. Potenzielle Teilnehmer werden durch das Bundesministerium sorgfältig ausgewählt und kontaktiert.

Das Förderprogramm besteht aus einer Pilotphase, in der die zukünftige digitale Währung, der Digitale Euro, im wirtschaftlichen Alltag erprobt und getestet wird. Teilnehmer haben die Möglichkeit, Eigenkapital von bis zu 1.000.000 Euro in den Digitalen Euro umzuschichten, um somit den Wert und die Kaufkraft ihres Geldes durch die Einführung der neuen Zentralbankwährung zu erhalten. Dabei wird dieser Betrag mit einer Förderung von bis zu 29% auf Ihre getätigte Einlage unterstützt.

Aktuell sind noch Plätze für 1.200 Teilnehmer in diesem exklusiven Förderprogramm verfügbar. Um sich für das Programm zu bewerben und detaillierte Informationen zu den Teilnahmevoraussetzungen, Testphasen und Pilotprogrammen zu erhalten, besuchen Sie bitte unsere Webseite über den weiter unten genannten Link. Nutzen Sie das in der Programmübersicht enthaltene Kontaktformular „zur Teilnahme" auf unserer Webseite, um Ihr Interesse an dem attraktiven Angebot zu bestätigen.

Für die Programmeinsicht benötigen Sie einen persönlichen Zugangscode, da das Angebot nicht öffentlich zugänglich ist. Diesen finden Sie weiter unten in dieser E-Mail.

HIER GEHT ES ZUM PILOTPROGRAMM

Ihren persönlicher Zugangsschlüssel zum nicht öffentlichen Bereich unserer Webseite erhalten Sie anbei in dieser E-Mail

Mit diesem persönlichen Schlüssel können Sie die Sonderinhalte freischalten lassen:

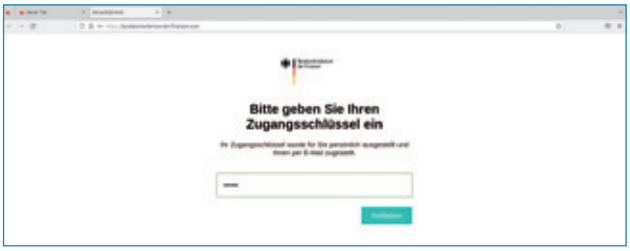
JHfgH1.2314KagLG!

Aufgrund einer statistischen Erhebung, die von Ihrem Girokontoführenden Kreditinstitut durchgeführt wurde, wurde uns empfohlen, Sie als Teilnehmer für das Pilot- bzw. Testprogramm zu berücksichtigen.

Wir laden Sie hiermit einmalig zur Teilnahme an unserem Testprogramm ein und möchten Sie darüber informieren, welche Möglichkeiten zur Vermögenssicherung derzeit gefördert werden. Bitte beachten Sie, dass es sich um eine exklusive E-Mail handelt und eine manuelle Abbestellung des Newsletters nicht erforderlich ist.

Hinweis Bitte beachten Sie, dass der Link nur solange gültig ist, bis sich ausreichend potenzielle Teilnehmer für das nächste Testprogramm registriert haben.

Gefälschte Mail: NextGenerationEU Förderprogramm



Gefälschte Webseite, Eingabe Zugangsschlüssel

Angebliches Förderprogramm der KfW

Die Kreditanstalt für Wiederaufbau (KfW) bietet verschiedene Förderprogramme für Privatpersonen an. Allerdings gibt es dort kein „Inflationsschutz-Förderprogramm“, wie es in E-Mails mit dem KfW-Logo behauptet wird. Diese E-Mails haben Kriminelle verfasst, die damit an persönliche Daten kommen wollen. Im Text behaupten sie, man könne sich auf einer Internetseite gegen die bevorstehenden Kostensteigerungen absichern. Ein Button „Jetzt Antrag stellen“ führt auf diese Seite. Sie gehört jedoch nicht zur KfW! Deshalb sollten Sie keinesfalls auf den Link klicken, denn die Behauptungen einer solchen Förderung sind frei erfunden. Falls Sie Daten auf der verlinkten Internetseite eingeben, könnten sie für kriminelle Zwecke missbraucht werden.

Phishing-Mails mit Sparkasse-Logo

Um das Abgreifen personenbezogener Daten geht es auch den Kriminellen, die seit Dezember 2022 E-Mails mit dem Logo der Sparkasse verschickt haben. In den E-Mails wird behauptet, das Geldinstitut würde eine von der Regierung beschlossene Energiepauschale in Höhe von 500 Euro auszahlen, „um den kommenden Winter und die damit einhergehenden Kosten gut zu überstehen“. Unter anderem schrieben die Betrüger:innen in ihrer Nachricht: „Um eine Auszahlung der Pauschale sicherstellen zu können, bitten wir Sie nun um eine Bestätigung ihrer angegebenen Daten. Gleichzeitig halten wir so Ihre Angaben aktuell und bereiten Sie auf die baldige Abschaltung unseres bisherigen Anmeldeverfahrens vor.“

In dieser Phishing-Mail wird erklärt, wer die Energiepauschale aus dem Entlastungspaket der Bundesregierung erhält. Anders als oft üblich, ist die betrügerische Mitteilung nahezu ohne Rechtschreibfehler und in guter


Daten auf der verlinkten Internetseite eingeben, könnten sie für kriminelle Zwecke missbraucht werden. Beispiel:

KFW
Bank aus Verantwortung

Sehr geehrte/r [redacted]

Die Europäische Zentralbank bietet Ihnen derzeit eine attraktive Möglichkeit, sich gegen die bevorstehenden Kostensteigerungen abzusichern!

Im Oktober 2022 hat die Inflation in Deutschland die Zehn-Prozent-Marke überschritten. Demnach finanziert die KFW-Bank aktuell ein attraktives Sonder-Förderprogramm. Dieses wurde zusätzlich zu den von der Bundesregierung bereits umgesetzten Entlastungsmaßnahmen im Bereich der Energieprodukte und des am 10. November 2022 verabschiedeten Inflationsausgleichgesetzes zum Vermögenserhalt ins Leben gerufen.

Es wird aus Mitteln des Europäischen Feonds in Form einer Zuwendung durch die vierte Säule der Europäischen Maßnahmenpakete finanziert und ermöglicht Ihnen den frühzeitigen Umtausch Ihrer Euro-Banknoten in die zukünftige Elektronische Währung den "Digitalen Euro". Die Förderungen wurden aufgrund einer begleitenden Testphase genehmigt und umfassen begrenzte Haushaltsmittel in Höhe von vier Milliarden Euro.

Im Rahmen des Inflationsschutz-Förderprogramms wird der drohende Kaufkraftverlust vollständig bis zu einer Maximaleinlage in Höhe von 400.000 Euro pro Person subventioniert und abgefedert. Die Voraussetzungen für die Teilnahme und Informationen zur Testphase finden Sie im Antrag.

Derzeit sind bereits 73 % der Zuwendungen in Anspruch genommen worden. Daher können wir eine Bearbeitung Ihrer Förderanträge nur noch für einen begrenzten Zeitraum garantieren.

Jetzt Antrag stellen

Mit freundlichen Grüßen
Ihr Team der KFW

Gefälschte E-Mail, Förderprogramm KfW


Sparkasse

Sehr geehrte Damen und Herren,

wir blicken zurück auf das Jahr 2022 und sehen, dass sich einiges verändert hat. Besonders stark betroffen sind die Kosten für Energie, Lebensmittel und den Transport.

Der Winter für dieses Jahr wird von Experten als sehr heizintensiv und somit teuer eingestuft. Ein wirtschaftlicher Abwehrschirm der Bundesregierung gegen die Folgen des russischen Angriffskrieges soll deswegen die steigenden Energiekosten und die schweren Folgen für Verbraucherinnen und Verbraucher sowie Unternehmen abfedern. Er wurde vor wenigen von Bundesfinanzminister Christian Lindner gemeinsam mit Bundeskanzler Olaf Scholz und Minister Robert Habeck vorgestellt. Der Abwehrschirm sieht unter anderem die Einführung einer Gaspreisbremse vor und umfasst Finanzmittel in Höhe von bis zu 200 Milliarden Euro. Außerdem ist Energiebonus zurück und soll bis Ende diesen Jahres erneut ausbezahlt werden.

Im Detail geht es um eine Einmalzahlung in der Höhe von 500 Euro um den kommenden Winter und die damit einhergehenden Kosten gut zu überstehen.

Wer erhält die Energiepauschale?

- **Steuerpflichtige** mit Einkünften aus Gewinneinkunftsarten (§ 13, § 15 oder § 18 des Einkommensteuergesetzes) und
- **Arbeitnehmerinnen und Arbeitnehmer**, die Arbeitslohn aus einem gegenwärtigen Dienstverhältnis beziehen und in die Steuerklassen I bis V eingereiht sind oder als **geringfügig Beschäftigte** pauschal besteuert werden.

Um eine Auszahlung der Pauschale sicherstellen zu können, bitten wir Sie nun um eine Bestätigung ihrer angegebene Daten. Gleichzeitig halten wir so Ihre Angaben aktuell und bereiten Sie auf die baldige Abschaltung unseres bisherigen Anmeldeverfahrens vor.

Geben Sie noch heute Ihre aktuellen Daten auf unserer Homapege an und erhalten Sie innerhalb der nächsten vier Wochen Ihre Auszahlung der Energiepauschale. Dies können Sie ganz bequem von zu Hause aus erledigen, anbei finden Sie einen Direktlink zu den geforderten Angaben.

Achtung: Nach erfolgreicher Bestätigung kann es bis 4 Wochen dauern, bis Sie Ihren Energiebonus auf Ihr Konto erhalten. Wir bitten um Verständnis!

Zur Homepage

Gefälschte E-Mail der Sparkasse

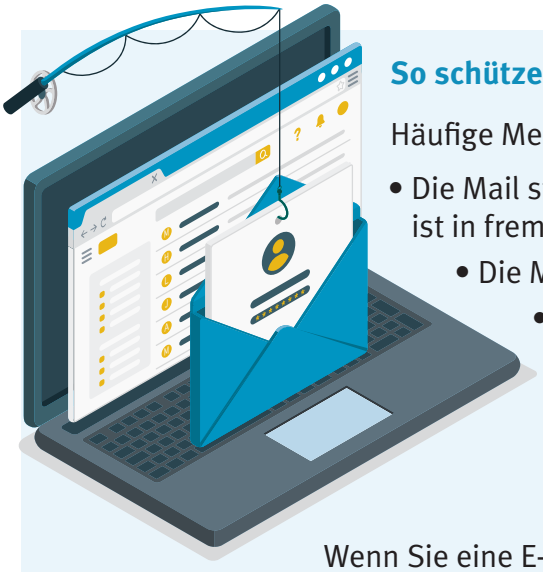
Grammatik geschrieben. Um Empfänger:innen zum Anklicken des Links auf eine falsche Sparkasse-Internetseite zu bewegen, heißt es in der E-Mail: „Um Ihre Identität sowie den Anspruch auf eine Auszahlung feststellen zu können, benötigen wir eine Bestätigung Ihrer bereits angegebenen Daten bei der Erstellung Ihres Girokontos in einer unserer Filialen.“ Erst dann soll es „in den nächsten vier Wochen Ihre Auszahlung der Energiepauschale“ geben.

Fallen Sie nicht auf diesen Trick herein! Keine Bank oder Sparkasse muss Daten zur Auszahlung der Energiepauschale prüfen. Die Auszahlung erfolgte im September über Ihren Lohn oder Ihr Gehalt. Die Hilfe beim Heizkostenabschlag für Dezember 2022 erhalten Sie direkt vom Energielieferanten oder im Rahmen der Nebenkostenabrechnung, falls Sie zur Miete wohnen.

Wenn Sie Daten eingegeben haben

Haben Sie dennoch Ihre Daten auf einer verlinkten Internetseite eingegeben, ist nicht abzuschätzen, was die Kriminellen damit anstellen. Es gibt zahlreiche Möglichkeiten für Identitätsdiebstahl, die von einfachen Internetbestellungen auf Ihre Rechnung bis zu kriminellen Geschäften in Ihrem Namen reichen. Vorsorglich sollten Sie Anzeige bei der Polizei erstatten – vor allem, wenn Sie ungewöhnliche Geldabbuchungen feststellen oder Rechnungen für nicht bestellte Waren und Dienstleistungen erhalten.

Wenn Sie einer Phishing-Attacke zum Opfer gefallen sind, können Sie sich auch von Fachleuten in Ihrer Verbraucherzentrale beraten lassen. Eine Übersicht über die Beratungsstellen der Verbraucherzentrale finden Sie hier: **www.verbraucherzentrale.de/beratung**



So schützen Sie sich vor Phishing-Attacken und Datenklau

Häufige Merkmale einer Phishing-Mail:

- Die Mail steckt voller Rechtschreib- und Grammatikfehler oder ist in fremder Sprache geschrieben.
- Die Mail enthält keine namentliche Anrede.
- Die Mail fordert zum dringenden Handeln auf.
- Sie werden aufgefordert, Daten einzugeben, eine Datei im Anhang zu öffnen bzw. herunterzuladen oder einen Link anzuklicken und auf der verlinkten Internetseite ein Formular auszufüllen.

Wenn Sie eine E-Mail als Betrugsversuch identifiziert haben:

- Klicken Sie nicht auf Links und öffnen Sie keine Dateianhänge!
- Antworten Sie nicht auf die Nachricht!
- Kennzeichnen Sie die E-Mail als Spam oder verschieben Sie sie in den Spamordner!

Verdächtige E-Mails, die Sie selbst erhalten haben, können Sie an die E-Mail-Adresse phishing@verbraucherzentrale.nrw weiterleiten. Die Verbraucherzentrale Nordrhein-Westfalen wertet die eingehenden E-Mails aus. Die Verbraucherzentralen können so stets über die aktuellen Betrugsvarianten informieren. Eine Übersicht darüber finden Sie unter dem Stichwort Phishingradar unter: www.verbraucherzentrale.de

Grafik: Storyset - freepik.com