POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

bürgerorientiert • professionell • rechtsstaatlich

Vermeintliche Anrufe von Europol oder Interpol
Präventionshinweise für Bürgerinnen und Bürger

Allgemeine Informationen

Es ist leider keine Seltenheit, dass sich Täterinnen und Täter am Telefon häufig als andere Personen ausgeben, um kriminelle Handlungen zu begehen. So kommt es auch vor, dass der Name der Polizei missbräuchlich eingesetzt wird. Im Hinblick auf das Phänomen „Falscher Polizeibeamter“ haben präventive Maßnahmen dazu beigetragen, dass Bürgerinnen und Bürger nicht mehr so häufig auf diese Masche hereinfallen. Aber: Die Kriminellen passen in solchen Momenten ihre jeweiligen Strategien an.

Die Täterinnen und Täter rufen wie bisher bei Ihren potenziellen Opfern an. Mittels des sogenannten „Call-ID-Spoofing“ wird die Rufnummernübermittlung beim Angerufenen so manipuliert, dass auf dem Display z. B. die Rufnummer der örtlichen Polizei, Staatsanwaltschaft usw. oder sogar die Notrufnummer 110 (in der Regel in Verbindung mit der örtlichen Vorwahl (z. B. 0211 110) oder anderen Zahlenfolgen vorweg) erscheint.

Anrufer: „Europol oder Interpol“

Kriminelle geben sich am Telefon als Mitarbeitende der europäischen Polizeibehörde Europol aus und setzen die Angerufenen mit erfundenen Geschichten, in deren Mittelpunkt sie stehen, unter Druck. Im einzelnen können dies Straftaten sein, in die man angeblich selber verwickelt sei oder aber auch Ereignisse zum Nachteil naher Angehörige oder Freunde.
Die Anruferin oder der Anrufer fordert die potenziellen Geschädigten auf, an ein extra eingerichtetes Konto für Kryptowährung sowie an ein Konto in Übersee hohe Geldmengen zu transferieren. Die Kriminellen kommunizieren teilweise über mehrere Stunden mit den Geschädigten und setzen sie dadurch noch mehr unter Druck.
In einzelnen Fällen bezeichnen sich die Kriminellen als Police Officer oder als Mitarbeitende des Federal Police Department, Interpol oder Europol. Angeblich sei auch das Bankkonto betroffen oder es gäbe ein großes Ermittlungsverfahren. Würde man eine Auskunft verweigern, so wurde auch bereits mit fünf Jahren Haft gedroht.

In bekannten Fällen wurde dazu aufgefordert, das Geld vom eigenen Bankkonto auf ein ausländisches Konto zu überweisen, um einer Gefängnisstrafe zu entgehen.

Kontakt:
Landeskriminalamt Nordrhein-Westfalen
Völklinger Straße 49
40221 Düsseldorf

Stand: März 2022

Wenn Sie angerufen werden:

LASSEN SIE SICH NIE UNTER DRUCK SETZEN

- Gibt sich die Anruferin/der Anrufer als Polizeibeamtin/Polizeibeamter aus, rufen Sie Ihre örtliche Polizeibehörde selbst an.
- Geben Sie unbekannten Personen keine Auskünfte über Ihre Vermögensverhältnisse oder andere sensible Daten.
- Transferieren Sie auf Grund solcher Anrufe keine Gelder, ohne sich vorher zu informieren und abzusichern.

Wenn Sie Opfer eines solchen Anrufes geworden sind, wenden Sie sich in jedem Fall an die Polizei und erstatten Sie eine Anzeige und setzen sich mit Ihrem kontoführenden Institut auseinander.

Weiterführende Informationen und Links

Als Opfer einer Straftat sind Sie nicht auf sich alleine gestellt. Sie werden durch zahlreiche Hilfs- und Beratungsangebote unterstützt. Weitere Informationen erhalten Sie unter: www.polizeiberatung.de/opferinformationen

Bei weiteren Fragen wenden Sie sich an die Kriminalkommissariate Kriminalprävention und Opferschutz beziehungsweise an die für Kriminalprävention und Opferschutz zuständigen Organisationseinheiten in Ihrer Nähe. Den Kontakt finden Sie über https://polizei.nrw/

Ihr Ansprechpartner:

Kontakt:
Landeskriminalamt Nordrhein-Westfalen
Völklinger Straße 49
40221 Düsseldorf

Stand: März 2022

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

bürgerorientiert • professionell • rechtsstaatlich

Phishing Attacken
Präventionshinweise für Bürgerinnen und Bürger

Allgemeine Informationen

Phishing (Passwörter „abfischen“) umfasst die Versuche, unberechtigt über das Internet an fremde Passwörter, Kontozugangs - PINs(Persönliche Identifikations-Nummer), TAN (Trans-Aktions-Nummer), Kreditkartennummern oder andere persönliche Daten zu gelangen.
Die Phishing-Betrüger versenden E-Mails oder setzen Schadprogramme wie „Trojanische Pferde“ ein. Die E-Mails wirken authentisch und sind vielfach in deutscher Sprache stilistisch einwandfrei und fehlerlos abgefasst. Die „Trojanischen Pferde“ können Ihre Tastatureingaben beim Online-Banking protokollieren und an Täterinnen/ Täter übermitteln oder leiten den Browser durch Veränderung an den Systemdateien bei Eingabe der Internetadresse Ihres Geldinstitutes auf eine gefälschte Seite.

Phishing-Schadprogramme

„Trojanische Pferde“, die z. B. in Dateianhängen versteckt sind, installieren sich beim Öffnen des Anhanges oftmals auch unbemerkt von Antivirensoftware auf Ihrem Computer und arbeiten weiterhin unbemerkt im Hintergrund. Sie leiten entweder Aufrufe Ihrer Online-Banking-Seiten auf Phishing-Seiten um oder protokollieren die bei den Transaktionen eingegebenen Tastatureingaben und senden diese Informationen an den Phishing-Betrüger. Hier schützt nur ein aktueller Virenscanner und eine Firewall, die nur den von Ihnen ausgewählten Programmen die Kommunikation ins Internet gestatten. Dabei ist Achtsamkeit geboten, denn „Trojanische Pferde“ benutzen häufig Programmnamen, die denen der Standardprogramme sehr ähnlich sind.

Phishing-Mails

Phishing-Mails weisen als Absender eine scheinbar vertrauenswürdige Organisation (z.B. Bank, Sparkasse) aus und fordern Sie unter Vorwänden auf, Ihre persönlichen Zugangsdaten über einen Link in der E-Mail im Internet einzugeben.
Der Link führt jedoch nicht zu der Webseite Ihres Geldinstitutes, sondern zu einer täuschend echt wirkenden Kopie des Phishing-Betrügers. Nach Eingabe der Daten wird häufig eine Fehlermeldung über eine wegen technischer Probleme missglückte Transaktion ausgegeben. Der Phishing-Betrüger ist nun im Besitz Ihrer persönlichen Zugangsdaten und kann diese nutzen.

Ich habe eine Phishing-Mail erhalten – was tun?

Löschen Sie sofort Phishing-Mails, die Sie als solche erkannt zu haben glauben. Auf der „richtigen“ Internetseite Ihres Geldinstitutes befindet sich eventuell bereits ein Warn-hinweis auf die bei Ihnen eingegangene Phishing-Mail. Im Zweifelsfall fragen Sie bei Ihrem Geldinstitut nach. Nehmen Sie umgehend Kontakt mit Ihrem Geldinstitut auf. Achten Sie stets darauf, mit der richtigen Webseite Ihres Geldinstitutes verbunden zu sein, indem Sie die Adressleiste in Ihrem Browser genau überprüfen oder tragen Sie diese Internet-adresse in die Favoritenliste Ihres Browsers ein. Die meisten Geldinstitute

lehnen eine Haftung/ Erstattung des verlorenen Betrages bei grober Fahrlässigkeit des Online-Banking-Nutzers ab.

Jobangebote für Finanz-Transaktionen

Phishing-Betrüger überweisen die betrügerisch erlangten Geldbeträge nicht auf eigene Konten. Sie werben per Mailing in Jobbörsen oder in Zeitungsannoncen „Finanz-Agenten“ an, denen eine äußerst lukrative Nebentätigkeit mit hohen Einkünften versprochen wird. Bei der Anwerbung treten sie unter Vortäuschen falscher Tatsachen, z.B. als Heiratsvermittlung, Finanzdienstleister oder Im- und Exportunternehmen, auf. Tatsächlich stammen die eingegangenen Geldbeträge von den Opfern eines Phishing-Betruges. Die Finanz-Agenten sollen die auf ihren Konten eingehenden hohen Geldbeträge gegen eine Provision ins Ausland weitertransferieren. Im Gegensatz zu den Überweisungen der Finanz-Agenten können per Western-Union abgewickelte Transfers nicht rückgängig gemacht werden. Der Finanz-Agent geht demnach ein hohes finanzielles Risiko ein. Eine Variante ist die unvorhergesehene Überweisung eines Geldbetrages auf Ihr Konto, der ebenfalls aus einem Phishing-Betrug stammt. Als Kontoinhaber werden Sie anschließend per E-Mail gebeten, den angeblich „versehentlich“ überwiesenen Betrag abzüglich einer Provision, ebenfalls meistens per Western-Union, ins Ausland zu überweisen.

Ich habe den Verdacht, Opfer eines Phishing-Angriffs geworden zu sein. Was kann ich tun?

Kontrollieren Sie sofort die Kontobewegungen und veranlassen Sie ggf. die Sperrung Ihrer TAN-Liste und des Kontozugangs. Die Sperrung erfolgt automatisch, wenn Sie mehrfach hintereinander (ca. 3-9 Mal) eine falsche Kontozugangs-PIN eingeben. Dann sind „abgephischte“ PIN und TAN für Betrüger zunächst wertlos.

Weiterführende Informationen und Links

Als Opfer einer Straftat sind Sie nicht auf sich alleine gestellt. Sie werden durch zahlreiche Hilfs- und Beratungsangebote unterstützt. Weitere Informationen erhalten Sie unter www.polizeiberatung.de/opferinformationen

www.mach-dein-passwort-stark.de

www.bsi-für-bürger.de

Bei weiteren Fragen wenden Sie sich an die Kriminalkommissariate Kriminalprävention und Opferschutz beziehungsweise an die für Kriminalprävention und Opferschutz zuständigen Organisationseinheiten in Ihrer Nähe. Den Kontakt finden Sie über https://polizei.nrw/

Ihr Ansprechpartner:

Herausgeber

Landeskriminalamt Nordrhein-Westfalen

Völklinger Str. 49

40221 Düsseldorf

Stand

März 2022

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

bürgerorientiert · professionell · rechtsstaatlich

Präventionshinweis für Bürgerinnen und Bürger

Neue Variante des Enkeltricks unter Nutzung eines Messenger-Dienstes, z. B. WhatsApp

Informationen

Die Polizei warnt vor einer neuen Variante des Enkeltricks:

Der klassische Enkeltrick

Täterinnen und Täter rufen ältere Menschen unter dem Vorwand an, Verwandte oder gute Bekannte zu sein: „Rate mal, wer am Telefon ist?“. Dann täuschen sie einen finanziellen Engpass vor und bitten um hohe Bargeldbeträge, weil sie das Geld aufgrund einer Notlage sofort benötigten (zum Beispiel nach einem Autounfall).

Durch mehrere Telefonanrufe innerhalb kurzer Zeit erhöht die Anruferin oder der Anrufer den psychischen Druck auf das Opfer, verbunden mit Appellen wie: „Hilf mir bitte!“.

Die Täterinnen und die Täter fordern absolute Verschwiegenheit gegenüber Dritten (zum Beispiel anderen Verwandten). Weil sie angeblich nicht selbst kommen können, vereinbaren sie mit den älteren Menschen ein Kennwort, das eine andere Person nennen wird, wenn das Geld abgeholt wird.

In zahlreichen Fällen haben die älteren Opfer nach solchen Gesprächen hohe Geldbeträge von ihrem Konto abgehoben, um der oder dem vermeintlichen Angehörigen zu helfen.

Neue Variante unter Nutzung eines Messenger-Dienstes, hier: WhatsApp

Die falschen Verwandten oder Bekannten nehmen über WhatsApp mit einer dem Opfer unbekannten Rufnummer Kontakt auf.

In der Regel wird das Opfer mit „Hallo Mama! Ich habe eine neue Telefonnummer.“ oder ähnlichem kontaktiert. Die Kontaktaufnahme wird damit begründet, dass z. B. das Handy verloren wurde.

Als nächstes wird das Opfer aufgefordert, die neue Nummer zu speichern. Kurze Zeit danach geht die nächste WhatsApp-Nachricht ein, dass z. B. eine offene Rechnung von mehreren Tausend Euro bezahlt werden müsse. Die oder der vermeintliche Angehörige habe aber aufgrund der Umstände keine Möglichkeit, auf Online-Banking zuzugreifen, um eine Überweisung durchzuführen.

Es ergeht nun die Bitte an das Opfer, diese Überweisung auf ein von der oder dem vermeintlichen Angehörigen genanntes Konto vorzunehmen, um die behauptete offene Rechnung zu begleichen. Das Geld würde angeblich in wenigen Tagen an das Opfer zurückgezahlt werden, was jedoch nicht geschieht.

Kontakt:
Landeskriminalamt Nordrhein-Westfalen
Völklinger Straße 49
40221 Düsseldorf

Juni 2021

Die Polizei gibt hierzu folgende Hinweise:

> Gehen Sie auf keinen Fall auf Geldzahlungsforderungen über Messenger-Dienste ein.

> Wenn Sie auf diese Weise von einer oder einem angeblich Bekannten oder Verwandten unter einer fremden Nummer kontaktiert werden, fragen Sie unter den Ihnen zuvor bekannten Erreichbarkeiten persönlich nach, ob tatsächlich die Nummer gewechselt wurde.

> Nehmen Sie eine fremde Nummer nicht sofort als Kontakt auf.

Wenn Sie bereits Opfer geworden sind:

> Erstatten Sie immer eine Strafanzeige. Nur so erhält die Polizei Kenntnis von der Straftat und kann die Täterinnen oder Täter verfolgen. Außerdem erhält sie dadurch Informationen zum Ausmaß des Deliktsfelds und kann Zusammenhänge herstellen und ggf. Tatserien erkennen. Eine Anzeige können Sie persönlich auf der nächstgelegenen Polizeidienststelle oder online unter https://polizei.nrw/ erstatten.

> Leisten Sie auf keinen Fall weitere Geldzahlungen.

> Informieren Sie Ihr kontoführendes Geldinstitut, um eventuell getätigte Geldflüsse anzuhalten oder rückgängig zu machen.

Weiterführende Hinweise und Links:

Als Opfer einer Straftat sind Sie nicht auf sich alleine gestellt. Sie werden durch zahlreiche Hilfs- und Beratungsangebote unterstützt. Sie erhalten dort Hilfe in Form von Gesprächen oder beim Umgang mit den Behörden. Ggf. begleiten Sie die Mitarbeitenden zu Gerichten, Polizei, Rechtsanwälten und anderen Institutionen.

www.polizei-beratung.de

www.weisser-ring.de

Bei weiteren Fragen wenden Sie sich an die Kriminalkommissariate Kriminalprävention und Opferschutz beziehungsweise an die für Kriminalprävention und Opferschutz zuständigen Organisationseinheiten in Ihrer Nähe. Den Kontakt finden Sie über:

https://polizei.nrw/

Ihr Ansprechpartner:

Kontakt:
Landeskriminalamt Nordrhein-Westfalen
Völklinger Straße 49
40221 Düsseldorf

Juni 2021