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 Internetadresse in die Favoritenliste Ihres Browsers ein.

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

### Wie kann ich mich vor Phishing-Angriffen schützen?

Ein hohes Maß an Sicherheit bieten alle Online-Banking-Programme, die eine Offline-Eingabe ermöglichen. Nach gegenwärtigem Stand der Technik als absolut sicher zu bezeichnen ist HBCI-Banking (Home-Banking Computer Interface) mit Kartenlesegerät und integrierter Tastatur. Es wird noch nicht von allen Banken angeboten.
In jedem Fall gilt: PIN und TANs nur dann eingeben, wenn eine gesicherte/verschlüsselte Verbindung mit Ihrem Browser hergestellt ist **(die Adresszeile beginnt dann mit „https: \\...“)**

### Soll ich E-Mails meiner Bank ignorieren?

Nicht grundsätzlich. Geldinstitute versenden jedoch keine E-Mail in der zur Transaktion mittels PIN und TAN über einen Link aufgefordert wird. Gehen Sie bei Erhalt einer solchen E-Mail von einer Phishing-Mail aus. Meist finden Sie auf der Webseite Ihrer Bank bereits Warnhinweise bezüglich dieser Phishing-Attacken.

### Wie kann ich meinen PC sicherer machen?

Zur Vorbeugung von Phishing-Attacken sichern Sie Ihren Computer, indem Sie regelmäßige Updates des Betriebssystems und der Anwenderprogramme sowie einer Virenschutzsoftware durchführen und eine Firewall installieren. Surfen Sie nicht mit Administratorrechten im Internet. Passen Sie auch die Sicherheitseinstellungen in Ihrem Browser Ihren Bedürfnissen an. Wireless-LAN (WLAN) und Funktastaturen nur für das Online-Banking benutzen, wenn diese über eine eingebaute Verschlüsselung verfügen. Benutzen Sie sichere Passwörter (Kombination aus Zahlen, Buchstaben, Sonderzeichen).
Nutzen Sie für Ihre Bankgeschäfte nur Rechner von Personen, denen Sie vertrauen, da es Programme und technische Einrichtungen gibt, die Tastatureingaben unbemerkt mitloggen können.

### Ausführliche Erläuterungen finden Sie unter:

**botfrei.de**
Service von eco – Verband der deuschen Internetwirtschaft e. V. mit Unterstützung des Bundesamtes für Sicherheit in der Informationstechnik (BSI)

**bsi-fuer-buerger.de**
Angebot des Bundesamtes für Sicherheit in der Informationstechnik, PC-Sicherheit, Jugendschutz

**klicksafe.de**
Projekt der Landesanstalt für Medien und Kommunikation Rheinland-Pfalz und der Landesanstalt für Medien Nordrhein-Westfalen im Auftrag der Europäischen Kommmission

**polizei-beratung.de**
Programm Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK); Sicherheitskompass mit hilfreichen Tipps

Weitere Informationen erteilt das Kriminalkommissariat Kriminalprävention/Opferschutz der Polizei.

Herausgeber:
Der Landrat des Rhein-Erft-Kreises als Kreispolizeibehörde
Willy-Brandt-Platz 1, 50126 Bergheim
Telefon: 02233 52-0
poststelle.rhein-erft-kreis@polizei.nrw.de
https://rhein-erft-kreis.polizei.nrw

Fachverantwortung:
Direktion Kriminalität
Kriminalkommissariat Kriminalprävention/Opferschutz
Luxemburger Straße 303a, 50354 Hürth
Telefon: 02233-52-4810
K.Kriminalpraevention.Rhein-Erft-Kreis@polizei.nrw.de



Stand: 10/17 - SH

POLIZEI
Nordrhein-Westfalen
Rhein-Erft-Kreis

bürgerorientiert · professionell · rechtsstaatlich


# Homebanker und Jobsuchende

## Verfangen Sie sich nicht im „Phisher“-Netz

## Phishing Allgemein

Phishing (Passwörter „abfischen“) umfasst die Versuche, über das Internet an fremde Passwörter, Kontozugangs-PIN (Persönliche Identifikations-Nummer) und TAN (Trans-Aktions-Nummer), Kreditkartennummern oder andere persönliche Daten zu gelangen.
Phishing-Kriminalität hat erheblich zugenommen. Die Vorgehensweise der Phishing-Betrüger wird dabei immer raffinierter. 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 Täter übermitteln oder leiten den Browser durch Veränderung an den Systemdateien bei Eingabe der Internetadresse Ihres Geldinstitutes auf eine gefälschte Seite.

Um unerkannt an das vom Konto des Opfers überwiesene Geld zu kommen, werben Phishing-Betrüger unter Vortäuschung seriöser Geschäftsvereinbarungen sogenannte „Finanz-Agenten“ in Deutschland an, die das an sie überwiesene Geld vorwiegend per „Western-Union Geld Transfer“ zumeist in das osteuropäische Ausland überweisen sollen.
Diese „Finanz-Agenten“, hereingefallen auf eine anscheinend lukrative (Neben-) Tätigkeit, riskieren nicht nur finanzielle Verluste, sondern machen sich in der Regel strafbar. **Die durch die Täter erdachten Legenden sind intelligent und dynamisch.**

## 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.

Übermitteln Sie keine per E-Mail angeforderten vertraulichen Daten.

Folgen Sie beim Online-Banking keinen Links in E-Mails zur Eingabe von Zugangsdaten, öffnen Sie keine an E-Mails angehängte Dateien und starten Sie keinen Download über den direkten Link, sondern nutzen Sie ausschließlich die Startseite Ihres Geldinstitutes.

## 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.

Schützen Sie Ihren Computer: Installieren Sie einen Virenscanner und aktualisieren Sie ihn täglich.

Nutzen Sie eine Firewall, wie z.B. die windowseigene, die in der Regel mit der Installation des Betriebssystems aktiv ist.
Entscheiden Sie sich beim Online-Banking für das sichere HBCI-Verfahren (mit Chipkarte und Kartenlesegerät).

## 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 weiter transferieren.
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. Man könnte ihn auch fast als Opfer bezeichnen, würde er sich nicht selber strafbar machen.
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.

Seien Sie vorsichtig bei Job-Angeboten und bei „versehentlichen“ Überweisungen im Zusammenhang mit Auslandstransaktionen von Geldbeträgen. Sie können nicht nur Ihr Geld verlieren, sondern machen sich auch strafbar. Wenden Sie sich im Zweifelsfall an die Verbraucherzentralen oder die Polizei.

## Ich habe eine Phishing-Mail erhalten – was tun?

Löschen Sie Phishing-Mails, die Sie als solche erkannt zu haben glauben. Auf der „richtigen“ Internetseite Ihres Geldinstitutes befindet sich eventuell bereits ein Warnhinweis auf die bei Ihnen eingegangene Phishing-Mail. Im Zweifelsfall fragen Sie bei der Bank nach.

## 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 Phishing-Betrüger zunächst wertlos. Nehmen Sie