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