Volksbank Lübbecker Land eG

Schutz vor Phishing und Trojanern

So erkennen Sie die Tricks!

Jeder hat das Wort schon einmal gehört: Phishing. Dahinter steckt der Versuch von Internetbetrügern, Bankkunden zu Überweisungen auf ein falsches Konto zu verleiten und so ihre Konten zu plündern. Die Aufforderung kann z.B. per E-Mail erfolgen oder durch die Nutzung von Schadsoftware, so genannte Trojaner. Allen Varianten gemeinsam ist, dass Sie mit einer scheinbar guten Begründung und unter gewissem Zeitdruck eine Aktion durchführen sollen. Dazu finden Sie in diesem Dokument einige Beispiele
Außerdem können Sie Ihren Zugang zum Online-Banking auch online sperren (innerhalb des Internet-Bankings auf „Service & Verwaltung“, dort den Bereich „Online-Sperren“).
Der beste Schutz –neben einem aktuellen Virenscanner – ist das Kennen der Methoden. Lesen Sie hier, wie aktuell versucht wird, Ihren PC und damit Ihr Online-Banking anzugreifen:

Überblick

Mit Genauigkeit und Sorgfalt vorgehen

Eine der wichtigsten Regeln beim Online-Banking lautet:

Gehen Sie mit Genauigkeit und Sorgfalt vor.

Mit den von uns angebotenen TAN-Verfahren sehen Sie ***VOR*** der Ausführung, welche Auftragsdaten (z.B. einer Überweisung) bei uns in der Bank angekommen sind. Überprüfen Sie also die Angaben der mobilenTAN oder die auf Ihrem TAN-Generator genau. Wollen Sie wirklich den angezeigten Auftrag ausführen?
Wenn nicht, beenden Sie Ihr Internet-Banking und setzen Sie sich mit uns telefonisch in Verbindung (0 57 41 / 3 28 – 2 52).

Und: Wir als Volksbank Lübbecker Land eG werden Sie niemals dazu auffordern, einen bestimmten Auftrag – warum auch immer – auszuführen. Es ist immer so, dass **Sie** eine Transaktion (z.B. Überweisung) erfassen und beauftragen, dann erfolgt unsere Frage nach einer TAN.

Häufige Vorgehensweisen

Die Internetbetrüger arbeiten häufig mit Schadsoftware, so genannten "Trojanern". Diese Schadsoftware "überblendet" das eigentliche Internet-Banking mit einer

Anwendung, deren Oberfläche dem tatsächlichen Design unseres Internet-Bankings entspricht. Oder die Betrüger veranlassen den Bankkunden per E-Mail unter falschem Vorwand zu einer Überweisung oder zur Angabe seiner Zugangsdaten zum Internet-Banking. So gelangen die Betrüger an wichtige Informationen, die Geld wert sind.

Beispiele

Täuschungsversuch: "Kontoüberprüfung wegen SEPA-Freischaltung" / „SEPA allgemein“

Aktuell nutzen Betrüger die Unsicherheit in Sachen SEPA dazu, Phishing Mails in Umlauf zu bringen. Die Phishing Mails werden versendet, um auf betrügerische Weise an personenbezogene Daten von Kunden zu gelangen. Die gefälschten E-Mails haben Betreffs wie beispielsweise "Ihr SEPA-Mandat" oder "SEPA-Umstellung". In den E-Mails werden Sie dazu aufgefordert, Ihre Kontodaten zu prüfen oder zu bestätigen.

So funktioniert der Betrug

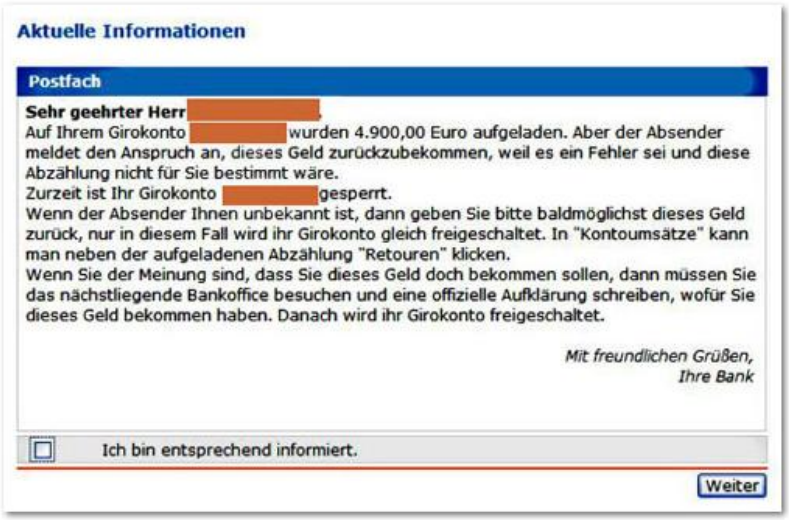
In vielen Fällen enthalten diese E-Mails Links, die für die Eingabe oder Kontrolle Ihrer Kontodaten angeklickt werden sollen. Der Link führt aber in der Regel auf eine gefälschte Seite. Dort wird Ihr Rechner dann mit Viren und Trojanern infiziert, mit denen Ihre Zugangsdaten ausgespäht werden können. In anderen Fällen erfolgt die Infizierung des Rechners mit Dateien, die der Phishing-E-Mail angehängt sind.

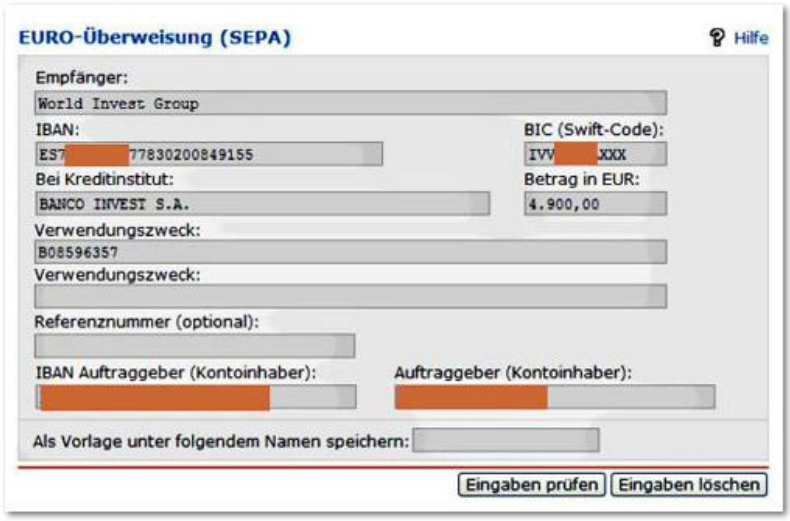
Abwehr der Phishing-Attacke

Wichtig:
Banken versenden grundsätzliche keine E-Mails, in denen Kunden dazu aufgefordert werden, ihre Kontodaten einzugeben.

Der beste Schutz vor Angriffen ist deshalb, derartige Mails ungeöffnet zu löschen. Grundsätzlich sollten Sie niemals einen in der E-Mail enthaltenen Link anklicken oder die beigefügten Dateianhänge öffnen. Wenn Sie vermuten, Opfer eines Phishing-Angriffs geworden zu sein, sollten Sie Ihr Internet-Banking umgehend sperren lassen und Kontakt mit Ihrer Volksbank Lübbecker Land eG aufnehmen.

Beispiele





Täuschung: "Fehlerhafter Geldeingang"

Der Nutzer erhält im Internet-Banking einen Hinweis auf einen falsch gebuchten Geldeingang. Aus diesem Grund sei nun sein Konto gesperrt. Um das Konto zu entsperren, soll der Anwender das vermeintlich falsch eingegangene Geld zurücküberweisen. Eine Variante „sperrt" nicht gleich das Konto, bittet aber um Eingabe einer TAN um „schnell und unbürokratisch" die falsche Gutschrift zu korrigieren.

So funktioniert der Betrug

Derlei Hinweise sind gefälscht, um Sie zu einer Überweisung zugunsten der Betrüger zu verleiten.

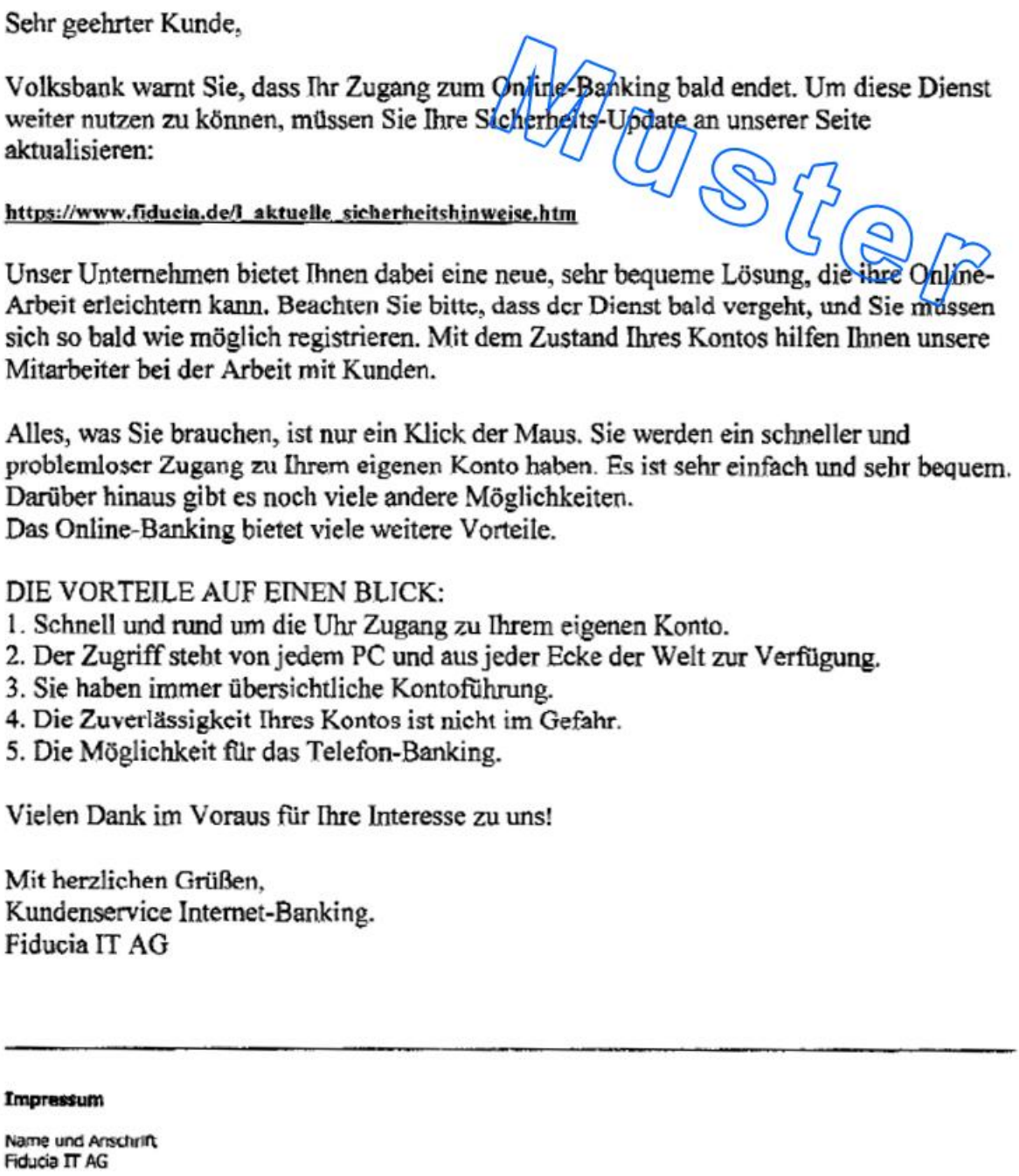
Manipulation der Umsatzanzeige

Auch die Kontrolle Ihrer Kontobewegungen kann durch diesen Trojaner um die „falsche Gutschrift" ergänzt sein. Angeblich zur Erleichterung der Rücküberweisung ist auf der manipulierten Umsatzanzeigeseite oft ein gefälschter Retour-Link programmiert. Durch Klicken des Retour-Links wird das gefälschte Überweisungsformular automatisch aufgerufen. Der Nutzer gibt im guten Glauben die TAN ein und versendet den Auftrag.

Abwehr der Phishing-Attacke

Auch hier gilt: Derlei Transaktionen entsprechen keinesfalls der Vorgehensweise Ihrer Volksbank Lübbecker Land eG. Seien Sie auch hier misstrauisch und wenden Sie sich bei Fragen an uns. Nehmen Sie keinesfalls Test- oder Rücküberweisungen vor.

Beispiele



Sehr geehrter Kunde,

Volksbank warnt Sie, dass Ihr Zugang zum Online-Banking bald endet. Um diese Dienst weiter nutzen zu können, müssen Sie Ihre Sicherheits-Update an unserer Seite aktualisieren:

https://www.fiducia.de/l_aktuelle_sicherheitshinweise.htm

Unser Unternehmen bietet Ihnen dabei eine neue, sehr bequeme Lösung, die ihre Online-Arbeit erleichtern kann. Beachten Sie bitte, dass der Dienst bald vergeht, und Sie müssen sich so bald wie möglich registrieren. Mit dem Zustand Ihres Kontos hilfen Ihnen unsere Mitarbeiter bei der Arbeit mit Kunden.

Alles, was Sie brauchen, ist nur ein Klick der Maus. Sie werden ein schneller und problemloser Zugang zu Ihrem eigenen Konto haben. Es ist sehr einfach und sehr bequem. Darüber hinaus gibt es noch viele andere Möglichkeiten.
Das Online-Banking bietet viele weitere Vorteile.

DIE VORTEILE AUF EINEN BLICK:
1. Schnell und rund um die Uhr Zugang zu Ihrem eigenen Konto.
2. Der Zugriff steht von jedem PC und aus jeder Ecke der Welt zur Verfügung.
3. Sie haben immer übersichtliche Kontoführung.
4. Die Zuverlässigkeit Ihres Kontos ist nicht im Gefahr.
5. Die Möglichkeit für das Telefon-Banking.

Vielen Dank im Voraus für Ihre Interesse zu uns!

Mit herzlichen Grüßen,
Kundenservice Internet-Banking.
Fiducia IT AG

Impressum

Name und Anschrift
Fiducia IT AG

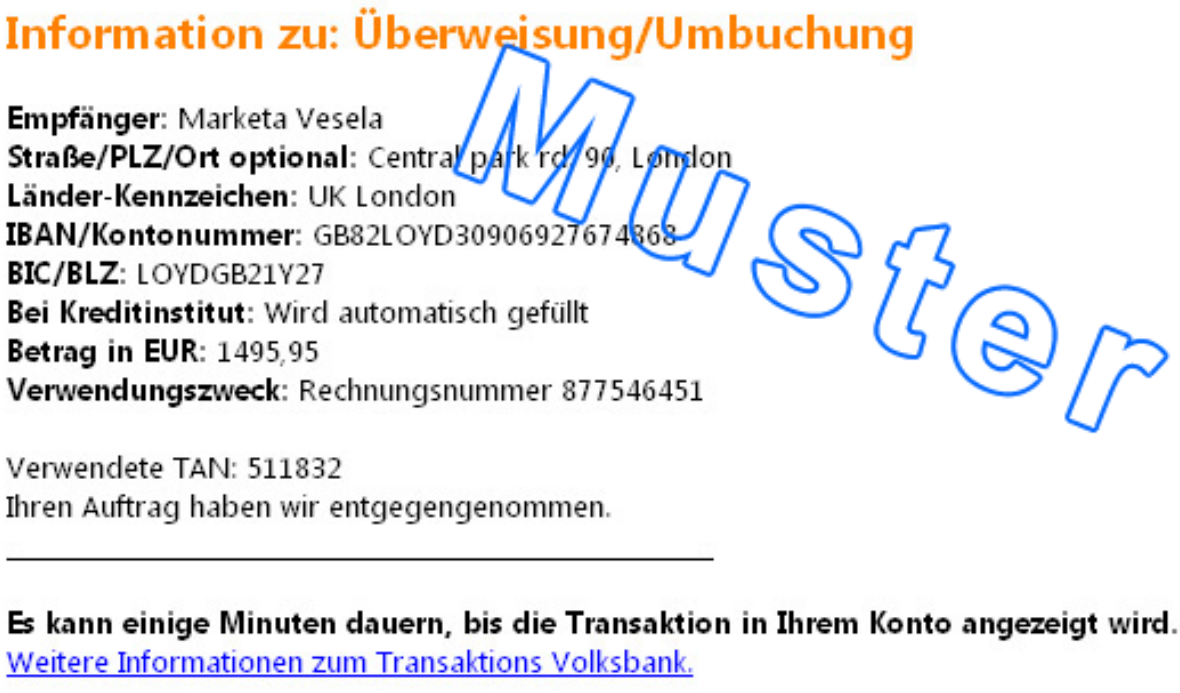
Täuschung: "Neue Sicherheitseinstellungen"

Der Kunde erhält scheinbar von seiner Bank einen Hinweis, dass eine Systemüberprüfung ansteht, die ein paar Sekunden in Anspruch nimmt. Stimmt der Nutzer dieser Sicherheitsüberprüfung zu, leitet der Trojaner den Kunden automatisch in den Dialog zur "Testüberweisung" weiter.

So funktioniert der Betrug
Der Trojaner gaukelt dem Anwender nun eine Testüberweisung oder eine Sicherheitsüberprüfung vor. Der Nutzer soll eine bereits vor-ausgefüllte Überweisung zu Test- bzw. Sicherheitszwecken mit einer korrekten TAN durchführen. Gibt der Nutzer die TAN ein, führt er eine normale Überweisung aus in dem Glauben, es würde sich um eine simulierte Überweisung zu Testzwecken handeln.

Abwehr der Phishing-Attacke
Ihre Volksbank Lübbecker Land eG wird niemals zu Test- oder Sicherheitszwecken eine solche Anfrage an Sie stellen. Öffnen sie keinesfalls Links in solchen E-Mails und löschen Sie sie sofort.

Beispiele



Täuschung: "ausgeführte Überweisung von Ihrem Konto"

Sie erhalten eine E-Mail, in der Ihnen eine Buchung von Ihrem Konto bestätigt wird. Für Details enthält die Mail einen Link.

So funktioniert der Betrug

Da Ihnen die Überweisungsdaten (Betrag, Empfänger, …) nicht bekannt vorkommen und Sie sich die „falsche" Überweisung genauer ansehen bzw. stoppen wollen, klicken Sie auf den Link „Details". Der Link führt aber in der Regel auf eine gefälschte Seite. Dort wird Ihr Rechner dann mit Viren und Trojanern infiziert, mit denen Ihre Zugangsdaten ausgespäht werden können.

Abwehr der Phishing-Attacke

Ihre Volksbank Lübbecker Land eG sendet Ihnen niemals unaufgefordert Mails mit Überweisungsbestätigungen. Öffnen sie keinesfalls die Links/Anlagen in solchen E-Mails und löschen Sie sie sofort.

Wenn Sie Fragen zum Thema Online-Banking, Sicherheit oder Phishing haben, rufen Sie uns an:
05741 / 328-0
05741 / 328-252

Wir kümmern uns um Ihr Anliegen!