Phishing – Digitale Girokarte
Schützen Sie Ihr Bankkonto!

Die digitale Girokarte ermöglicht das kontaktlose Bezahlen mit einem Smartphone - ein Service, der von einigen Banken, zum Beispiel Sparkassen, Volks- und Raiffeisenbanken, PSD-Banken und Sparda-Banken, angeboten wird. Zur Einrichtung wird lediglich ein Smartphone mit Nahfeldkommunikations-Funktionalität (NFC) benötigt. Das heißt: Über NFC kann ein kompatibles Smartphone Daten mit anderen NFC-fähigen Geräten in der Nähe drahtlos austauschen, so dass beispielsweise ein kontaktloses Bezahlen möglich ist. Das ist praktisch, aber…

„Phishing“ droht

„Phishing“ besteht übersetzt aus zwei Wortinhalten: „Passwörter ernten“ und „fischen/angeln“. Umschrieben werden damit also Betrügereien, bei denen die Täterinnen und Täter versuchen, sich Ihnen gegenüber als vertrauenswürdig darzustellen. Sie sollen dazu verleitet werden, persönliche Daten preiszugeben oder eine Aktion zu tätigen, die Ihnen (finanziell) schadet - und das bequem und zeitnah im Rahmen einer elektronischen Kommunikation im Internet. Wenn also Ihre Daten in falsche Hände kommen, können Täterinnen und Täter uneingeschränkt über Ihr Guthaben verfügen.

Medien beschreiben das Vorgehen als digitalen Bankraub. Die Täterinnen oder Täter handeln zur Vorbereitung per E-Mail, SMS, über gefälschte Webseiten oder per Telefon, um Ihnen Daten zu entlocken. Gehen Sie drauf ein, haben die Kriminellen Sie an der Angel. Sie bedienen sich Ihrer Bankdaten, um sich selbst unabhängig von Ihrer physischen Girokarte, die Sie in Ihrem Portemonnaie oder Ihrer Brieftasche haben, heimlich ein digitales Abbild Ihrer Girokarte auszustellen und bald darauf Ihr Konto leerzuräumen.

Zwei praktische Beispiele

Variante 1: Als angeblicher Bankmitarbeiter ruft Täter A Sie an und teilt Ihnen mit, dass es verdächtige Geldbewegungen auf Ihrem Bankkonto gegeben habe. Unter anderem sei eine unberechtigte Abbuchung von Ihrem Konto erfolgt. Zwecks Rückbuchung des Betrages benötige er rasch Ihre PIN, also Ihre persönliche Identifikationsnummer, und eine TAN, also Transaktionsnummer, um das Geld noch zurückholen zu können…

Variante 2: Täterin B sendet Ihnen eine E-Mail, die täuschend echt wie sonstige Mails von Ihrer Hausbank aussieht. Möglicher Inhalt: Sie werden aufgefordert das Zugangsverfahren für Ihr Online-Banking zu aktualisieren. Oder die Person gaukelt Ihnen vor, eine plötzliche Sperrung, eine erforderliche Verifizierung oder eine Änderung rechtlicher Bestimmungen bedinge ein sofortiges Handeln. Ziel ist, an Ihre persönlichen Daten heranzukommen - möglichst umfassend.

Weiterer Tatablauf

Sie werden angeleitet, einen in der E-Mail befindlichen Link anzuklicken. Dieser führt Sie auf eine gefälschte Internetseite, die dem Original Ihrer Hausbank bis aufs i-Tüpfelchen gleicht. Bei professionellen Taten ist die Seite eins zu eins gespiegelt und ohne Auffälligkeit in Sprache oder Orthografie. Sie können eigentlich nur an der Absenderangabe (im Header) der E-Mail oder an einer auffälligen URL-Adresse erkennen, dass etwas nicht stimmt. Also etwa bei einem Schreibfehler wie: http://b0nn.polizei.nrw/ [b0nn.polizei.nrw] statt richtig: https://bonn.polizei.nrw/ [bonn.polizei.nrw] oder bei einer falschen Domainerweiterung, also etwa „.org“ statt „.de“.

Das heißt im Klartext: Lassen Sie sich vom äußeren Schein nicht täuschen. Prüfen Sie alles genau. Denn auf einer gefälschten Seite werden Sie aufgefordert, Ihre persönlichen Daten (Adresse, Telefonnummer, Kontonummer, PIN, Passwort des Online-Bankings) einzugeben. Wenn Sie das tun, brauchen die Kriminellen jetzt nur noch eine TAN-Transaktionsnummer, die Sie entweder für angeblich weitere Schritte in der Verfahrensabfolge selbst generieren und eingeben sollen oder die etwas zeitversetzt telefonisch abgefragt wird.

Und dann werden Konten leergeräumt

Häufig erhalten die Phishing-Opfer nämlich am Folgetag einen Anruf, bei dem angebliche Bankmitarbeitende Sie auffordern, eine Push-TAN in der Push-TAN-App zu bestätigen, die diese während des Gespräches erhalten. Statt der angeblichen Rückbuchung, Aktualisierung, Freischaltung oder Verifizierung genehmigen Sie dann mit der Auftragsbestätigung in der Push-TAN-App, dass eine digitale Girokarten zu Ihrem Konto sofort auf dem Smartphone der Täterinnen und Täter erstellt und aktiviert wird.

Die können nun ihr eigenes Smartphone mit der fremden digitalen Karte einsetzen, ohne selbst die physische Debitkarte mit PIN zu besitzen. Sie können an zahlreichen Geldautomaten oder im Einzelhandel bei jeweils vorhandener NFC-Funktion kontaktlos Bargeld abheben oder einkaufen. Und wer dann seine Kontobewegungen nicht zeitnah kontrolliert, bemerkt Abbuchungen oder Auszahlungen oft erst, wenn das Konto leergeräumt ist.

Schützen Sie sich:

- Seien Sie vorsichtig und beachten Sie bei der Nutzung des Online-Banking und der digitalen Debitkarte die Vorgaben Ihrer Bank! Informieren Sie sich hier umfassend.
- Achten Sie darauf, die Webseite für das Onlinebanking nur über die Ihnen bekannte offizielle Webadresse aufzurufen. Geben Sie die Internetbanking-Adresse Ihrer Bank immer selbständig in den Webbrowser ein und nutzen Sie nicht den Umweg über Suchmaschinen!
- Geben Sie Ihre Zugangsdaten zum Online-Banking nur auf der Online-Banking-Seite Ihrer Bank ein.
- Seien Sie vorsichtig bei eingehenden E-Mails. Betrügerische E-Mails sehen oft täuschend echt aus. Achten Sie auf die Absenderdaten.
- Banken werden Kundinnen und Kunden niemals per E-Mail, SMS oder Telefon nach persönlichen Informationen wie PIN oder Kontonummer fragen, in E-Mails oder SMS einen Link zum Online-Banking einfügen oder zu Rücküberweisungen auffordern.
- Identifizieren Sie eine E-Mail als Betrugsversuch, klicken Sie nicht auf Links und öffnen Sie keine Dateianhänge.
- Lassen Sie sich bei Anrufen angeblicher Bankmitarbeitenden unter keinen Umständen verleiten, sensible persönliche oder kontenbezogene Daten preiszugeben.
- PIN oder (Push-)TAN geben Sie bitte niemals an Dritte heraus - auch nicht an angebliche Bankmitarbeitende oder angebliche Polizeibeamte. Wenn Sie das tun, sind Kriminelle in der Lage, sich selbst eine elektronische Debitkarte zu Ihrem Konto auszustellen und Abbuchungen von Ihrem Konto vorzunehmen.
- Klären Sie im Zweifel solche Aufforderungen mittels unmittelbarer Kontaktaufnahme zum echten Kundensupport. Entnehmen Sie die Erreichbarkeit aus Ihren Bankunterlagen.
- Stellen Sie bei Prüfung Ihres Kontostandes unberechtigte Abbuchungen fest, handeln sie sofort. Prüfen Sie die im Onlinebanking hinterlegten Geräte oder Karten.
- Wenden Sie sich unverzüglich an Ihre Bank, sollten Sie das Phishing oder den Anruf eines falschen Mitarbeitenden erkennen, und erstatten Sie Anzeige bei der Polizei.
- Überprüfen Sie die Höhe Ihrer eingestellten Limits. Reduzieren Sie alles auf das üblicherweise Notwendige. - Sie können die Limits bei Bedarf jederzeit wieder erhöhen.

Bleiben Sie auf dem Laufenden über aktuelle Phishing-Warnungen und Empfehlungen bei Ihrer Polizei und Ihrer Hausbank.

Weiterführende Hinweise finden Sie auch unter: www.polizei-beratung.de

Für Rückfragen stehen wir zur Verfügung:

Polizeipräsidium Bonn - Direktion Kriminalität - KK Kriminalprävention und Opferschutz
Königswinterer Str. 500
53227 Bonn
Telefon: 0228-15-7676
E-Mail: KKKPO.Bonn@polizei.nrw.de