PHISHING – SCHUTZ VOR DATENDIEBSTAHL

Allgemeines:

Phishing bezeichnet den Versuch Ihre persönlichen Daten über das Internet zu erlangen. Via Emails oder betrügerische Webseiten wird versucht, persönliche Daten oder Informationen wie Kreditkartennummern, Kontodaten sowie Zugangsdaten zu Ihren Email- und weiteren Accounts (Amazon, Ebay, Facebook, Twitter usw.) abzufragen.

Zur Vorgehensweise der Täter:

Phishing gibt es in unterschiedlichsten Varianten. Fingierte Emails etwa sollen beim Nutzer den Eindruck erwecken, sie kämen von einer Bank oder einem Online-Auktionshaus. Die Empfängerin oder der Empfänger wird aufgefordert, einen Link anzuklicken vom dem er zu einer meist täuschend echt aussehenden Betrugs-Webseite geleitet wird. Dort wird das Opfer unter einem Vorwand gebeten seine persönlichen Daten – darunter auch Passwörter, Pins und Tans – einzutragen.

Im Schadensfall nehmen Sie bitte sofort mit dem betroffenen Dienstleister (Bankinstitut, PayPal, Ebay, Amazon usw.) Kontakt auf, informieren diesen von dem Vorfall und veranlassen nötigenfalls die sofortige Sperre. Danach erstatten Sie bitte umgehend Anzeige auf einer Polizeiinspektion.

Tipps des Bundeskriminalamts:

- Kein seriöses Unternehmen oder Bankinstitut fordert per Email zur Eingabe von persönlichen Daten wie Passwörter usw. auf.

- Internetseiten, auf denen man sensible Nutzerdaten eingeben muss, erkennen Sie an den Buchstaben „https“ in der Adresszeile der Webseite und einem Schloss- oder Schlüssel-Symbol im Internet-Browser. Weiters sind sichere Webseiten auch an einer grün hinterlegten Adresszeile oder an einem grün hinterlegten Zertifikatszeichen erkennbar, wenn sich der Betreiber einer unabhängigen Prüfung unterzogen hat.

- Überprüfen Sie die Adresszeile des Webbrowsers. Oft reicht ein Blick, um zu erkennen, dass es sich gar nicht um die richtige Website handelt. Sind Sie sich nicht sicher, geben Sie die Ihnen bekannte und gewohnte Adresse per Hand ein.

- Richten Sie sich Ihre wichtigen Homepages, wie zum Beispiel Bankzugang etc. als Favoriten in Ihrem Browser ein und verwenden Sie nur diese. Stellen Sie so sicher, dass Sie nur die offiziellen Seiten verwenden.

- Wichtig ist der Schutz durch Passwörter: Soweit möglich, verwenden Sie nicht das gleiche Passwort für mehrere Dienste – etwa E-Mail-Konto, Online-Shops und Communitys. Je länger und komplexer ein Passwort ist, desto schwerer ist es zu knacken. Es sollte mindestens acht Zeichen lang sein und aus einer zufälligen Reihenfolge von Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen bestehen. Ein solches könnte leicht erstellt werden, indem sich der Benutzer einen Satz überlegt und von jedem Wort den ersten Buchstaben sowie alle Zahlen und

Sonderzeichen verwendet (zum Beispiel der Satz: „Ich bin am 1. Jänner 1970 geboren.“ ergäbe das Passwort: Iba1.J1970g.).

- Wer sich die zahlreichen Codes schwer merken kann, dem helfen so genannte Passwort-Safes. Das sind PC-Programme, mit denen sich Geheimzahlen sicher speichern lassen. Der Anwender braucht sich dann nur noch ein Haupt-Passwort zu merken, welches natürlich entsprechend schwer zu erraten sein sollte.

- Sind Sie sich unsicher, ob Sie ein Passwort bekannt gegeben haben, dann ändern Sie als erstes das Passwort und melden Sie diesen Vorgang an die Betreiber der Homepage bzw. dem Unternehmen.

- Den Anweisungen solcher Mails sollte man keinesfalls nachkommen, sondern sie unverzüglich aus dem Account löschen. Kreditkarten- und Bankinstitute sowie Online-Shops würden Sie niemals per E-Mail zur Bekanntgabe von Daten auffordern.

Weitere Information erhalten Sie in der nächsten Polizeiinspektion, auf der Homepage www.bmi.gv.at/praevention und auch per BMI-Sicherheitsapp.

Die Spezialisten der Kriminalprävention stehen Ihnen kostenlos und österreichweit unter der Telefonnummer 059133 zur Verfügung.