SCHUTZ VOR
NOTFALL- UND BETTEL EMAIL

Derartige E-Mails werden besonders zur Urlaubszeit verstärkt in Umlauf gebracht. Internetbetrüger versuchen so vermeintlichen Freunden und Bekannten Geld herauszulocken.

Zur Vorgangsweise der Täter:

Notfall-E-Mail
Der Täter verschaffen sich widerrechtlichen Zugang zum Email-Account des Opfers und versendet dann sog. Notfall-E-Mails an die Kontakte im Adressverzeichnis. In der Mail selbst wird vorgegeben, dass man sich in einer Notlage im Ausland befindet und dringend Geld für die vom Konsulant / der Botschaft genehmigten Rückreise und die Bezahlung des Hotels benötigt. Die Zahlung soll dann über Geld-Transfer-Dienste wie z.B. Western Union erfolgen. Hier ist eine Nachvollziehbarkeit schwierig bis unmöglich, die Behebung selbst geschieht zumeist unter Vorlage von gefälschten Ausweisdokumenten.

Hier ist es wichtig zu versuchen, seinen E-Mail Account wieder zu erlangen und Betroffene im Vorfeld von dem Vorfall in Kenntnis zu setzen, damit keine Zahlungen getätigt werden. Zu beachten ist, dass analog zum "übernommenen" Mail-Account zumeist ein gleichlautender Mail-Account bei einem anderen Mail-Anbieter erstellt wird, welcher zusätzlich zur Verschleierung beiträgt. Es erscheint sinnvoll, auch diesen Dienstanbieter von dem Vorfall sowie dem nur für Betrugszwecke erstellten Account zu informieren und um die Löschung oder Sperre desselben zu ersuchen.

Bettel-E-Mail
Ein plötzlich namensgleicher und fast identer Facebook-Account. Hierbei wird vom Täter versucht die tatsächliche Identität eines Unbeteiligten für seine Betrugszwecke auszunutzen. Es werden gleiche Namen verwendet, es werden die widerrechtlich kopierten Fotos verwendet, es gibt einen gleichlautenden Mail-Account bei einem anderen Anbieter und es werden die Kontakte des Unbeteiligten als mögliche Opfer verwendet.

"Ich muss dringend etwas kaufen, habe aber meinen Pin vergessen ..."; so oder so ähnlich beginnen die meisten der hier gemeldeten Betrugsversuche. Danach wird man ersucht via online-Banking oder bei Tankstellen und Trafiken elektronisches Geld z.B. in Form von Paysafekarten zu erwerben und anschließend die Nummern zu übermitteln. Die Rückzahlung wird für den nächsten Tag, natürlich inklusive eines kleinen verlockenden Aufschlags, versprochen. Die Höhe der geforderten Summe beträgt meist um die 500,- Euro.

Die Umstände und Varianten in beiden Betrugsfällen sind vielfach und ändern sich nach Täter(-gruppen) fast täglich. Die genannten Beispiele sind daher plakativ, sollen jedoch im Ansatz den Ablauf der Betrugsmasche darstellen und Sie sensibilisieren. "Freunde" und Bekannte fragen üblicherweise nicht per Mail oder Facebook nach Geld, auch nicht in der Not!

Das Bundeskriminalamt empfiehlt generell:

Verwenden Sie sichere Passwörter mit entsprechender Länge, Groß-, Klein-Schreibung und Sonderzeichen, damit die Täter weder Mail- noch "social media" Accounts hacken können!

Geben Sie keine Passwörter oder Zugangsdaten zu Ihren Accounts bekannt, ändern Sie die Zugangsdaten regelmäßig und vergeben dabei komplexe Passwörter.

Überweisen Sie niemals Geldbeträge ohne Gegencheck: Versuchen Sie die betroffene Person persönlich zu erreichen!

Überweisen Sie Geld mittels Transferdiensten nur nach eingehender Überprüfung und persönlichem Kontakt mit dem Empfänger!

Warnen Sie weitere, möglicherweise direkt betroffene Kontakte und sensibilisieren Sie diese!

Ist bereits ein Schaden eingetreten, erstatten Sie auf der nächsten Polizeiinspektion eine Anzeige!

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.