



Gemeinsames Präventionsprojekt von Polizei und VKP **Gefahr durch neue Medien – Wie sicher Sie leben, entscheiden Sie selbst!**

Serienbeitrag 3: Betrug durch eMails

Die Polizei WHV/FRI und der VKP-WHV berichten in dieser Ausgabe über die bereits als klassisch geltenden eMails, mit denen Sie hinteres Licht geführt werden sollen. Trotz zum Teil fantasievoller Geschichten blieb die Masche bei allen Fischzügen der letzten zehn Jahre immer gleich: Man erschleicht sich das Vertrauen der Opfer und erreicht unter irgendeinem Vorwand eine Geldzahlung im Voraus für eine Leistung.

Der Nigeria-Betrug : Dem Opfer wird eine großzügige Belohnung versprochen, wenn es jemandem hilft, eine größere Geldsumme außer Landes zu schaffen, z.B. eine Erbschaft oder Gewinne aus Öl – und Diamantenhandel. Die Herkunft liegt meist in Afrika, typischerweise Nigeria. Damit das funktioniert, muss das Opfer aber zunächst eine bestimmte Geldsumme überweisen, um angebliche Bankspesen zu decken. Natürlich hört man nie wieder etwas von den Betrügern, sobald man die Summe überwiesen hat.

Lotterie-Gewinn : Man bekommt per E-Mail eine Gewinnbenachrichtigung von einer Lotterie. Bevor man den Jackpot kassieren kann, soll man jedoch z.B. Anwaltskosten im Voraus bezahlen. Fällt man darauf herein, ist das überwiesene Geld verloren.

Jan Pauser, Sachbearbeiter im 3. Fachkommissariat, fragt sich dann immer : **Warum rechnen Sie mit einer Gewinnauszahlung, wenn Sie gar kein Lotterie-Los besitzen ?**

Der "Russisches Mädchen"-Trick : Ein bezaubernd schönes Mädchen aus Russland will angeblich das Opfer besuchen. Allerdings fehlt ihr aus irgendeinem Grund das Geld für den Flug. Wer den gewünschten Betrag überweist, bleibt nicht nur einsam, sondern kann sich auch noch von seinem Geld verabschieden.

Job-Angebote : Man bekommt einen Nebenjob angeboten, bei dem man von zu Hause arbeiten und mit wenig Zeitaufwand viel Geld verdienen kann. Das hört sich zunächst verlockend an. Nimmt man das Stellenangebot an, muss man zunächst seine Kontonummer angeben. Danach verwenden die kriminellen Arbeitgeber das Konto des Opfers für Geldwäscheaktionen. Wer mitspielt, macht sich zum Komplizen und muss selbst mit Strafen rechnen.

Social Network : Hacker stehlen die Zugangsdaten zu Diensten wie Facebook und ändern das Passwort, so dass sich das Opfer nicht mehr einloggen kann. Danach geben sie sich als das Opfer aus und versenden E-Mails an alle Kontakte, in denen sie um Geld bitten. Der Grund: Man sei im Urlaub ausgeraubt worden und benötige dringend eine Geldüberweisung, um die Hotelrechnung zu zahlen.

Die Entschädigungsmasche : Der Nachfolger des Nigeria-Betrugs - man bekommt eine E-Mail, in der von einem Fond die Rede ist, um Opfer des Nigeria-Betrugs zu entschädigen. Man selbst gehöre zu den "glücklichen" Opfern, die eine Ausgleichszahlung bekämen - natürlich erst, nachdem man selbst einen Betrag überwiesen hat.

Der Kniff mit dem "zu hohen Scheck": Die Betrüger kontaktieren ihr Opfer, die einen Gegenstand, z.B. ein Auto im Internet zum Kauf anbieten. Man einigt sich auf den Kaufpreis und will per Scheck im Voraus bezahlen. Anschließend wird ein Scheck mit einer viel höheren Summe geschickt als vereinbart wurde. Die Betrüger melden sich und bitten um Erstattung der Differenz - meist per Direktüberweisung etwa mit Western Union. Geht man darauf ein, stellt man fest, dass der Scheck eine Totalfälschung war und die angebliche "Differenz-Erstattung" verloren ist.

Grundsätzlich gilt :

Der Trick der Täter ist es, an **Gier und Gutgläubigkeit** der Mitmenschen zu appellieren, um auf diese Weise leicht und viel Geld verdienen zu können. **Misstrauen ist deshalb immer angebracht.** Neben finanziellen Verlusten erleiden die Opfer aber einen noch viel größeren Schaden, der ihr Leben und vor allem ihr Verhältnis zu anderen Menschen nachhaltig verändert, nämlich den Vertrauensverlust in ihre Mitmenschen.

Die **beste Verteidigung** ist daher :

die eigene **Leichtgläubigkeit** ablegen,
drohende Betrugsmanöver **rechtzeitig** erkennen
und dadurch finanzielle Schäden **vermeiden.**

Sie können helfen, die massenhafte Flut dieser eMails einzudämmen, in dem Sie diese eMails **nicht pauschal** an Ihren gesamten Freundeskreis **weiterleiten**. Löschen Sie gerade die nutzfreien und sinnlosen Kettenbriefe aus Ihrem Posteingang und aktivieren Sie immer den sog. Spam-Filter. So bewahren Sie zumindest Ihre Freunde, Familie und Bekannte vor dem drohenden Ärger mit Spam-Mails und finanziellem Schaden!

Siehe dazu auch : www.bsi-fuer-buerger.de

Die Beauftragte für Kriminalprävention der Polizei, Polizeioberkommissarin Katja Reents, bietet darüber hinaus Vorträge und persönliche Beratungen zu diesem Thema an. Sie ist dienstlich unter der Rufnummer 04421-942-108 zu erreichen.

Für Rückfragen stehen wir Ihnen gerne zur Verfügung:

Markus Wallenhorst
Presse- und Öffentlichkeitsarbeit
Polizeiinspektion Wilhelmshaven/Friesland
04421-942-404
markus.wallenhorst@polizei.niedersachsen.de

Andrea Papenroth, Pressesprecherin des
VKP,
Tel. 04421-942-437
andrea.papenroth@polizei.niedersachsen.de