Cybercrime-News

1/2018

Vorschussbetrug

Der angebliche Verkäufer behauptet zumeist im Ausland aufhältig zu sein und ersucht Sie um Überweisung einer Vorauszahlung per Finanzdienstleister wie etwa Western Union. Der angebotene Artikel wird entweder zu einem auffallend günstigen Preis oder weit unter dem Handelswert inseriert. Trotz Bezahlung wird keine Ware geliefert. Auf Ihre Nachfrage reagiert der Verkäufer mit verschiedensten Argumenten wie etwa Zustellprobleme, bis nach einiger Zeit keine Reaktion mehr erfolgt.

Eine unbekannte Person oder Institution macht per E-Mail Hoffnung auf einen **Lotteriegewinn**, eine **Millionen-Erbschaft**, eine tolle **Wohnung zum Schnäppchenpreis** oder verspricht eine **hohe Provision**, wenn man bei der Überweisung von Geldbeträgen „mithilft". Oftmals gibt der Absender zu verstehen, dass es sich um eine höchst „vertrauliche" oder „dringende" Sache handelt und man speziell „ausgewählt" wurde. Auch wenn alles sehr verlockend klingt – es handelt sich dabei mit ziemlicher Sicherheit um einen so genannten **Vorschussbetrug** oder engl. **Scamming**.

Der Trick ist immer der gleiche: Bevor die versprochenen Geldbeträge überwiesen werden, werden die Opfer dazu gedrängt (oft über dutzende E-Mails oder Chatnachrichten), eine **Vorauszahlung** zu leisten (für entstandene Spesen, Steuern, Flugtickets etc.). Von den versprochenen Geldbeträgen sieht man natürlich nichts und die Vorauszahlung ist ebenfalls weg. Hinzu kommt, dass die Opfer auch manchmal zur **Bekanntgabe von geheimen Bank- oder Zugangsdaten** sowie der **Unterzeichnung von Dokumenten** aufgefordert werden.

Als wichtigste Regel gilt: **Werden Ihnen per E-Mail Angebote gemacht, die zu schön sind, um wahr zu sein, sollten die Alarmglocken schrillen! → arg. „Gesunder Menschenverstand, Bauchgefühl!"**

Schutzmöglichkeiten:

- **Auch im Internet hat niemand etwas zu verschenken.** Antworten Sie nicht auf dubiose E-Mail-Versprechungen mit ungewöhnlich hohen Profiten – auch nicht, um das „Geschäft“ abzusagen – und **löschen Sie die E-Mails sofort**.
- **Senden Sie Unbekannten weder Geld noch persönliche Dokumente** und erledigen Sie auch keine „Gefälligkeiten“ (wie z.B. Geldtransfers, Scheck einlösen, Briefe/Pakete weiterleiten).
- **Antworten Sie nicht** auf E-Mails, die mit Gewinnspielen in Zusammenhang stehen, an denen Sie nicht teilgenommen haben. Reagieren Sie auch nicht auf Mitteilungen oder Mahnungen zu Waren, die Sie nicht bestellt haben.
- Lassen Sie sich **nicht** durch Aussagen **unter Druck setzen**, dass es angeblich um sehr hohe Geldbeträge geht, die Sache „dringend“ ist oder prominente Personen involviert sind.
- Wählen Sie keine in der Nachricht angegebene Telefonnummer. Oft sind es **gebührenpflichtige Mehrwertnummern**.
- Geben Sie Teile der dubiosen E-Mail (z.B. den Betreff) oder den Namen Ihrer neuen Internet-Bekanntschaft mit dem Zusatz „Scam“ **in eine Suchmaschine** ein. Die Suchergebnisse können in vielen Fällen einen Betrug entlarven.
- **Lassen Sie sich keine überhöhten Schecks für Privatverkäufe oder schnelle „Nebenjobs“ andrehen** und überweisen Sie niemals geforderte Differenzbeträge. Die Schecks werden ein paar Wochen später platzen und das überwiesene Geld ist auch weg (Scheckbetrug).
- Sollten Sie bereits Geld überwiesen haben, wenden Sie sich an die **Polizei**. Es ist meistens jedoch sehr schwierig, die Täter/innen von Vorschussbetrug zu ermitteln und zu verurteilen.