Cybercrime-News

2/2018

Scheckbetrug (Opfer ist Verkäufer)

Auf eine Verkaufsanzeige meldet sich ein Interessent, der – meist auf Englisch oder in schlechtem Deutsch – erklärt, die Ware kaufen zu wollen. Bezahlen möchte er mit einem **Bankscheck**, der **Versand** soll in ein Land **außerhalb der EU** erfolgen. Als der Scheck ankommt, bemerkt der Verkäufer, dass der angegebene Betrag den vereinbarten Kaufpreis deutlich übersteigt. Die Erklärungen dafür sind unterschiedlich. Mal behauptet der Käufer, dass dies der „Mindestbetrag" für einen Scheck gewesen sei, dass er sich verschrieben habe oder der Differenzbetrag für den Transport gedacht ist, den ein Freund übernehmen wird. Die **Differenz** soll in der Regel per **Western Union bzw. Auslandsüberweisung** an den Käufer selbst oder eben den vermeintlichen Transporteur rücküberwiesen werden. Wenn der Scheck auf der Bank hinterlegt wird, wird der Betrag zwar sofort gebucht, aber die Deckungsüberprüfung dauert einige Tage. Stellt sich der Scheck als **nicht gedeckt** oder gar **gefälscht** heraus, wird das Geld wieder vom Konto abgebucht. Dem Betroffenen bleibt weder das Geld des Schecks, noch der überwiesene Differenzbetrag (den er dem Käufer zurückbezahlt hat). Schlimmstenfalls wurde in der Zwischenzeit auch noch die Ware versandt und ist nicht mehr rückholbar.

Vorkassa-Trick (Opfer ist Käufer)

Der/die vermeintliche Verkäufer/in befindet sich meist **im Ausland** und bittet um **Vorabüberweisung** per Western Union, internationaler Überweisung bzw. auch Paysafecard oder Postanweisung. Oft handelt es sich bei den Angeboten um auffallend günstige Elektronikartikel oder Gebrauchtwagen. Trotz der Überweisung des Geldes wird die **Ware nicht zugestellt**. Auf Nachfrage reagiert der/die vermeintliche Verkäufer/in mit unterschiedlichen Argumenten, um das Ausbleiben zu rechtfertigen (der Artikel konnte nicht zugestellt werden, die Adressangabe war falsch, es gibt Verzögerungen beim

Transportunternehmen etc.). Nach einigen Tagen oder Wochen wird **nicht mehr auf E-Mails bzw. Rückfragen reagiert**, da der/die vermeintliche Verkäufer/in weiß, dass Sie bei diesen Zahlungsmethoden **keine Möglichkeit einer Rückbuchung** haben.

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**.