Hintergrundinformation zum Fallbeispiel: Falle beim Online-Verkauf

Eine Frau wollte über eine bekannte Internetplattform gebrauchte Kleidung verkaufen. Schon kurze Zeit später meldete sich ein vermeintlicher Interessent. Dieser bat darum, das Gespräch über einen Messengerdienst (wie WhatsApp) fortzusetzen.

Im Laufe des Gesprächs schickte der angebliche Käufer einen Link mit der Bitte, dort ein Video der Kleidung hochzuladen. Über diesen manipulierten Link wurden im Hintergrund vertrauliche Zugangsdaten der Verkäuferin ausgespäht (**Data-Harvesting**: das gezielte Abgreifen persönlicher Daten).

Kurz darauf nutzten die Täter die gestohlenen Daten, um Geld vom Bankkonto der Frau zu überweisen. Als die Verkäuferin mehrere Benachrichtigungen ihrer Banking-App zur Freigabe dieser Transaktionen erhielt, schöpfte sie keinen Verdacht. Sie nahm an, es handle sich um einen technischen Fehler ihrer Bank, und bestätigte die Anfragen. Dadurch autorisierte sie die Überweisungen unfreiwillig selbst – am Ende verlor sie einen fünfstelligen Geldbetrag.

(Frei nach einem Bericht von ORF.at)

Dieser Betrugsfall basiert auf einer Kombination aus **technischem Cyber-Angriff (Phishing & Data-Harvesting)** und **psychologischer Täuschung (Social Engineering)**. Die Täter nutzen dabei gezielt Sicherheitslücken im Verhalten des Opfers aus, da die technischen Sicherheitssysteme modernster Banken kaum direkt geknackt werden können.

Die drei Phasen des Betrugsablaufs

Phase 1: Der Plattformwechsel (Sicherheitsfilter umgehen)

- **Vorgehen:** Der angebliche Käufer nimmt Kontakt auf der Verkaufsplattform auf, drängt jedoch sofort darauf, das Gespräch über einen Messengerdienst (z. B. WhatsApp) fortzuführen.
- **Ziel der Täter:** Seriöse Verkaufsplattformen verfügen über automatische Sicherheitsfilter, die verdächtige Links oder Nachrichten mit Schlüsselwörtern blockieren oder Warnhinweise anzeigen. Durch den Wechsel auf WhatsApp werden diese Schutzsysteme wirkungslos gemacht.

Phase 2: Phishing & Data-Harvesting (Sammeln der Zugangsdaten)

- **Vorgehen:** Täter schicken unter einem Vorwand (z. B. *„Ich benötige ein Video der Ware“* oder *„Bestätige den Erhalt des Geldes über diesen Link“*) einen präparierten Link.
- **Technischer Hintergrund:** Der Link führt auf eine gefälschte Nachbildung einer Plattform oder Login-Seite. Wenn das Opfer dort Daten eingibt (oder der Link schädlichen Code ausführt), spionieren die Täter vertrauliche Online-Banking-Zugangsdaten (Verfügernummer, Passwörter, persönliche Daten) im Hintergrund aus. Dieser Vorgang wird als **Data-Harvesting** (Daten-Ernte) bezeichnet.

Phase 3: Aushebelung der 2-Faktor-Authentifizierung (2FA / Social Engineering)

- **Vorgehen:** Mit den gestohlenen Logins melden sich die Täter im Online-Banking des Opfers an und veranlassen Überweisungen. Da moderne Banken für jede Transaktion eine Freigabe verlangen (**2-Faktor-Authentifizierung**, z. B. per Banking-App oder Push-TAN), reicht das Passwort allein nicht aus.
- **Psychologischer Trick:** Die Täter nutzen die Verwirrung des Opfers aus oder täuschen vor, dass es sich um eine Validierung oder einen Fehler des Geldinstituts handelt. Das Opfer liest die Details der Freigabeanfrage in der Banking-App nicht aufmerksam durch und autorisiert die Überweisungen im Glauben, das Problem zu beheben. Damit schließt das Opfer die Transaktionskette für die Täter unwissentlich selbst ab.

Zusammenfassung

1. **Kommunikation auf der Plattform belassen** und keine Zahlungs-Links akzeptieren: Wenn die Zahlungsabwicklung nicht direkt über die Plattform läuft, sollte die Absprache (z. B. zur Banküberweisung oder Barzahlung) trotzdem ausschließlich im Chat der Verkaufsplattform stattfinden. Auf zugeschickte Links zu angeblichen „Zahlungsdienstleistern“ oder „Uploads“ sollte niemals geklickt werden.
2. **Keine fremden Links öffnen:** Links zum „Geldeingang“, „Video-Upload“ oder „Identitätsnachweis“ von Unbekannten sind zu 99 % Betrugsversuche.
3. **2FA-Freigaben immer prüfen:** Push-Nachrichten der Banking-App dürfen **niemals ungeprüft bestätigt** werden. Vor dem Klick auf „Freigeben“ müssen Betrag und Empfänger in der App kontrolliert werden.