Musterlösung

Arbeitsauftrag: Cyber-Security und Online-Betrug

Aufgabe 1:

a) Bring die drei Absätze in die richtige zeitliche Reihenfolge. Verschiebe den Text in Word so, wie der Betrug der Reihe nach abgelaufen ist.
b) Verwendet anschließend die Nummerierungsfunktion in Microsoft Word, damit die Fehler von 1 bis 3 klar ersichtlich werden.

1. **Plattformwechsel**: Die Verkäuferin verlegte die Kommunikation auf einen externen Messengerdienst (wie WhatsApp), wodurch die Schutz- und Warnsysteme der Verkaufsplattform umgangen wurden.
2. **Klick auf Phishing-Link:** Sie klickte auf einen fremden Link, den ihr der Betrüger geschickt hatte. Dort sollte sie ein Video hochladen. Auf dieser gefälschten Seite wurden aber heimlich ihre geheimen Passwörter für das Online-Banking gestohlen (**Phishing** und **Data Harvesting**).
3. **Unbedachte 2FA-Freigabe:** Die Verkäuferin bekam Push-Nachrichten von ihrer Banking-App auf das Handy. Weil sie an einen technischen Fehler ihrer Bank glaubte, klickte sie auf „Bestätigen“. Damit erlaubte sie den Dieben unabsichtlich, ihr Geld auf ein anderes Konto zu überweisen (Zwei-Faktor-Authentifizierung).

Aufgabe 2:

a) Bringe die folgenden **6 Schritte** der Betrugsmasche in die richtige zeitliche Reihenfolge (von 1 bis 6). Verschiebe die Absätze an die richtige Stelle.
b) Verwende anschließend die Nummerierungsfunktion in Microsoft Word, damit die Schritte von 1 bis 6 klar ersichtlich werden.

Richtige Reihenfolge 1–6:

1. Eine Frau bietet über eine Online-Plattform gebrauchte Kleidung zum Verkauf an.
2. Ein angeblicher Käufer meldet sich und überredet die Frau, für das weitere Gespräch auf einen Messengerdienst (z. B. WhatsApp) zu wechseln.
3. Der angebliche Käufer schickt der Frau einen Link mit der Bitte, dort ein Video der Ware hochzuladen.
4. Die Verkäuferin klickt auf den zugeschickten Link, woraufhin ihre vertraulichen Online-Banking-Daten unbemerkt ausgespäht werden.
5. Die Täter nutzen die gestohlenen Zugangsdaten, um im Online-Banking der Frau Überweisungen einzurichten.
6. Die Frau glaubt an einen Systemfehler ihrer Bank und bestätigt die Freigabeanfragen in ihrer Banking-App.

Aufgabe 3: Wichtige Begriffe zum Fallbeispiel

Kopiere die Erklärungen zu den Begriffen (zu finden unterhalb der Tabelle) in die in die rechte Spalte der Tabelle. ***Beachte***: Die Reihenfolge der Erklärungen ist zufällig! Überlege, was zu den Begriffen passt.

Begriff	Erklärung
Phishing	Das Versenden gefälschter Links oder Nachrichten, um Nutzer auf trügerische Webseiten zu locken und vertrauliche Zugangsdaten abzufangen.
Data-Harvesting	Das systematische und zielgerichtete Abgreifen („Abernten“) persönlicher Daten wie Passwörter, Bankdaten oder Kontoinformationen.
2-Faktor-Authentifizierung (2FA)	Ein zweistufiger Sicherheitsnachweis beim Online-Banking. Neben den Zugangsdaten (Faktor 1) ist eine zusätzliche Freigabe nötig (Faktor 2, z. B. per Banking-App).
Social Engineering	Das gezielte Manipulieren von Menschen (z. B. durch das Vortäuschen von Systemfehlern oder Kaufabsichten), um sie zu unbedachten Handlungen zu verleiten.
Messenger-Betrug	Eine Masche, bei der Täter die Opfer von geschützten Verkaufsplattformen auf private Messengerdienste (z. B. WhatsApp) locken, um Sicherheitsfilter zu umgehen.