Technische Universität Berlin
Institut für Psychologie und Arbeitswissenschaft
Fachgebiet Mensch-Maschine-Systeme

Prof. Dr.-Ing. Matthias Rötting
Dr.-Ing. Ulrike Schmuntzsch
Dipl.-Psych. Christine Paulisch

Betrugsschutz beim Online-Banking
Nutzeraspekte und Mensch-Maschine-Interaktion

Zusammenfassung der Ergebnisse

Phishing-Angriffe & Trojaner

- Mehrheit der Probanden misstraut dem Phishing-Angriff per E-Mail und zeigt Skepsis gegenüber der Mobilnummer-/TAN-Abfrage beim Login
- 28% verwenden TAN ohne Überprüfung des Betrages oder der IBAN
- 40% achten auf https-Verschlüsselung
- 76% würden die Sicherheitsausnahmeregel für das Zertifikat bestätigen

mTAN vs. chipTAN

- hohe Rate fehlgeschlagener Übermittlungen beim chipTAN-Verfahren
- mTAN-Verfahren wird hinsichtlich der Gebrauchstauglichkeit und Nutzerfreundlichkeit besser bewertet als das chipTAN-Verfahren

Verschiedene Betrugsszenarien

<u>Aufforderung zur Rücküberweisung</u>

- 44% erkennen den Angriff nicht, aber nur 12% überweisen den Betrag zurück (Druck durch Kontosperrung bewegt zur Rücküberweisung)

<u>Aufforderung zur Eingabe der Mobilfunknummer</u>

- 68% geben Mobilfunknummer ein; 44% haben keinen Zweifel an der Legitimität der Abfrage; eher sicheres Gefühl „Wer sollte sonst etwas mit der Nummer machen können?"
- nur TAN-Abfrage vorab wird als gefährlich eingestuft

<u>Änderung der Transaktionsdaten im Hintergrund</u>

- 65% gleichen die IBAN in der SMS, bzw. im TAN-Generator nicht mit den einzugebenden Daten ab
- 70% überprüfen nicht den zu überweisenden Betrag
- 71% erkennen den Betrug nicht oder erst nach der Transaktion

<u>über alle drei Betrugsszenarien</u>

- im Durchschnitt gleichen 56% die IBAN in der SMS, bzw. im TAN-Generator nicht mit den einzugebenden Daten ab; weitere 44% überprüfen den Betrag in beiden Anzeigen nicht

Sichere digitale Identitäten – Elektronischer Personalausweis

- mittelmäßige Bewertung der Gebrauchstauglichkeit
- Einwände wegen Sicherheitsbedenken, höherem Aufwand und unklarem Nutzen
- Skepsis gegenüber zusätzlichem Gerät (Anschaffungskosten, Mobilitätseinschränkung)

Nutzerfreundlichkeit von CAPTCHAs und Alertsystemen

- gemittelt über zwei Nutzerstudien würden 67% der Probanden CAPTCHAs nutzen, wenn diese die Sicherheit erhöhen
- Wunsch nach einfacheren CAPTCHAs ohne Heraussuchen/Zusammenrechnen von Zahlen
- als Alternativen wurden Bilder-CAPTCHAs genannt

Fokusgruppendiskussion zu Alertsystemen: Ampelsystem, Balkensystem, Infosystem

- grundsätzlich positive Haltung gegenüber Alertsystemen (erzeugen Risikobewusstsein und stellen Information über Gefahren bereit)
- Wunsch nach einem Alertsystem direkt auf der Startseite der Bank

Ampel- und Balkensystem:

- erzeugen ggf. eine „falsche" Sicherheit beim Status „grün"
- werfen Fragen bzgl. des erforderlichen sicheren Nutzerverhaltens auf („Was soll ich als Nutzer jetzt bei „rot" oder „gelb" machen, bzw. kann ich überhaupt etwas machen?")

Eindeutige Präferenz für das Infosystem:

- hervorgehobener Informationscharakter, insbesondere durch Screenshots
- Detailbeschreibungen zu Gefahren
- Wunsch nach genauen Handlungsanweisungen in der Detailbeschreibung

Welche Erwartungen und Wünsche zum Thema Sicherheit beim Online-Banking werden an die Bank gestellt?

- Publikation aktueller Betrugsfälle und Schutzmaßnahmen
- genaue Anleitung, wie bei vermeintlichem Betrug vorzugehen ist

Welche Aspekte beim Online-Banking werden als besonders kritisch betrachtet? Was ist der Grund dafür?

- die Länge der IBAN wird als kritisch gesehen - hier wäre eine übersichtlichere Darstellung hilfreich, z.B. durch die Hervorhebung der Einzelkomponenten
- bei Aufforderungen zur Eingabe ist oft unklar, ob diese echt oder gefälscht sind
- gewünscht werden konkrete Handlungsanweisungen
- Zeitdruck führt zu Vernachlässigung der Überprüfung

Welche Hilfestellungen werden von den Probanden genannt, die bei der Identifizierung von Betrugsfällen unterstützen könnten?

- Alertsysteme, welche über aktuelle Angriffe informieren
- anschaulich gestaltete Lernplattform mit Betrugsbeispielen
- Pop-Up nach Übermittlung der Transaktionsdaten als Erinnerung zur Überprüfung der Bankdaten