Christian Prantner und Jakob Kalina

ACHTUNG, BETRÜGERISCHES „DATEN-FISCHEN“ BEI BANKKUNDINNEN (PHISHING)!

April 2020

Die AK warnt, dass aktuell wieder Phishing-E-Mails im Umlauf sind, die Banken betreffen – Phishing (Kürzel hergeleitet aus dem Englischen: Password Fishing) bedeutet so viel wie Datenklau im Internet.

In dieser E-Mail ist von *„einem neuen Zahlungskontrollsystem“* die Rede, das der Empfänger unbedingt aktivieren müsse, *„um eine Deaktivierung zu vermeiden“* – so steht es in dem Text, den Bankkunde Martin Maier in den letzten Tagen mehrmals empfangen hat. In Summe gingen drei E-Mails – vermeintlich – von Raiffeisen in seinem elektronischen Posteingang ein.

Ein Blick auf die E-Mails, die innerhalb von drei Wochen – beginnend mit **22. März bis zuletzt am 17. April 2020** – bei Herrn Meier einlangten, zeigte, dass die vermeintlichen Nachrichten von **„ELBA Raiffeisen“** plumpe Fälschungen waren und Betrugsabsichten hegten – die Absenderadresse stammte nicht von Raiffeisen und der Text war in gebrochenem Deutsch verfasst. Wie in all diesen betrügerischen Nachrichten waren auch in den E-Mails, die Herr Maier bekam, Links auf die vermeintliche Bank-Website enthalten. Nur: diese Links führen direkt auf eine Website der Betrüger, die in der Folge die Kontakt- und Zugangsdaten zu einem Konto abfragen.

Sehr häufig wird der Betrug durch Telefonanrufe der Betrüger vollendet, die zum Schluss nach einer Transaktionsnummer (TAN) fragen, die – vom angerufenen Bankkunden bekanntgeben – die betrügerische Abbuchung vom Konto ermöglicht.

Wie sieht die aktuelle betrügerische E-Mail – vermeintlich von Raiffeisen ELBA – aus (eingelangt am 17.4.2020)?

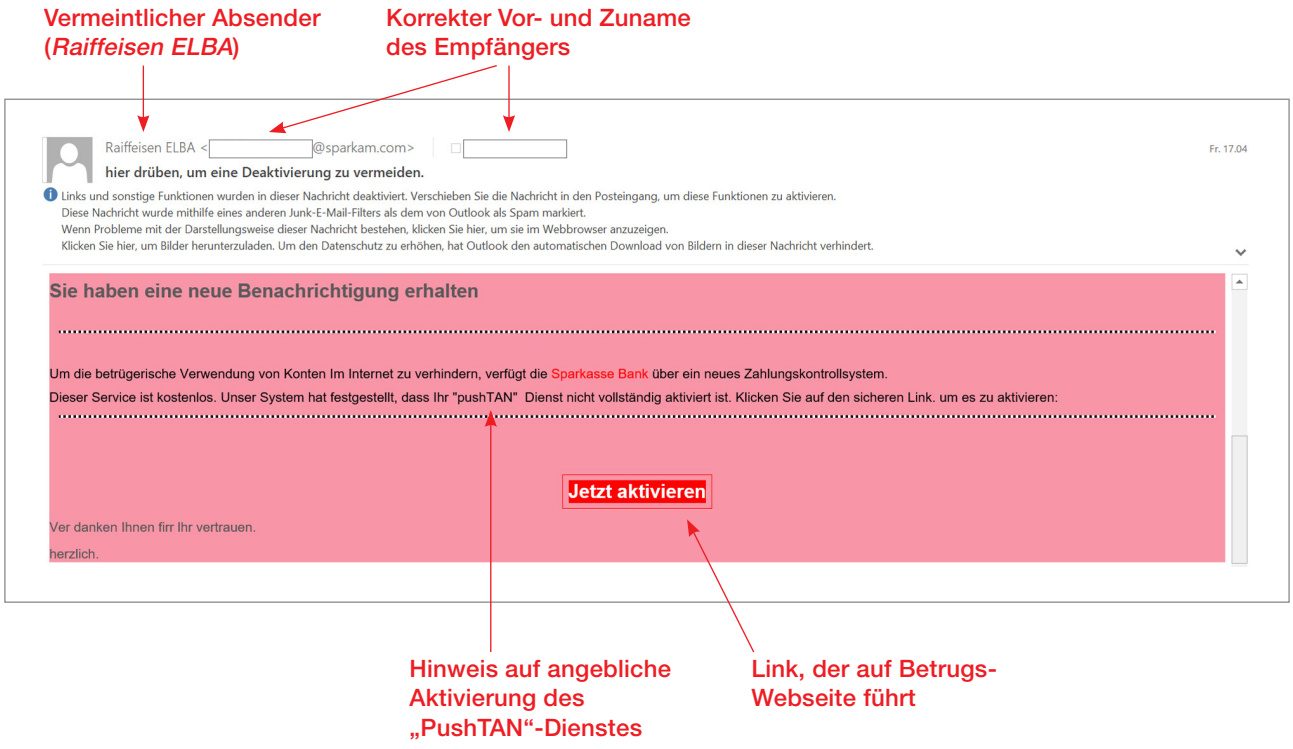

Abbildung 1: Screen von betrügersicher E-Mail vom 17.4.2020

Seit etlichen Jahren sind **gefälschte E-Mails** im Umlauf, die – vermeintlich im Namen einer Bank oder eines Kreditkartenanbieters – den Empfänger der E-Mail auffordern, sensible Zugangsdaten zu einem Girokonto oder zur Kreditkarte bekanntzugeben. Vermehrt geschieht vergleichbares mit gefälschten Banken-SMS. Beide Nachrichtenarten haben jedoch **betrügerischen Hintergrund**, denn sie beabsichtigen, Kriminellen den Zugriff auf ein fremdes OnlineBanking-Konto zu ermöglichen.

WIE KÖNNEN DIE PHASEN DES PHISHING-BETRUGES AUSSEHEN (BEISPIEL)?

Die AK hat die Phasen des Phishing-Betruges anhand eines Praxisbeispiels nachgestellt.
Die Abfolge in vier Schritten:

Schritt 1: Die SMS mit betrügerischen Hintergrund – mit Link zur Fake-Website

Das ist eine Phishing-SMS mit betrügerischem Hintergrund: Das Ziel ist es, dass der Nachrichten-Empfänger bzw. Kunde/Kundin der Bank – unten **exemplarisch** der Raiffeisen Bank – den angegebenen Link anklickt:

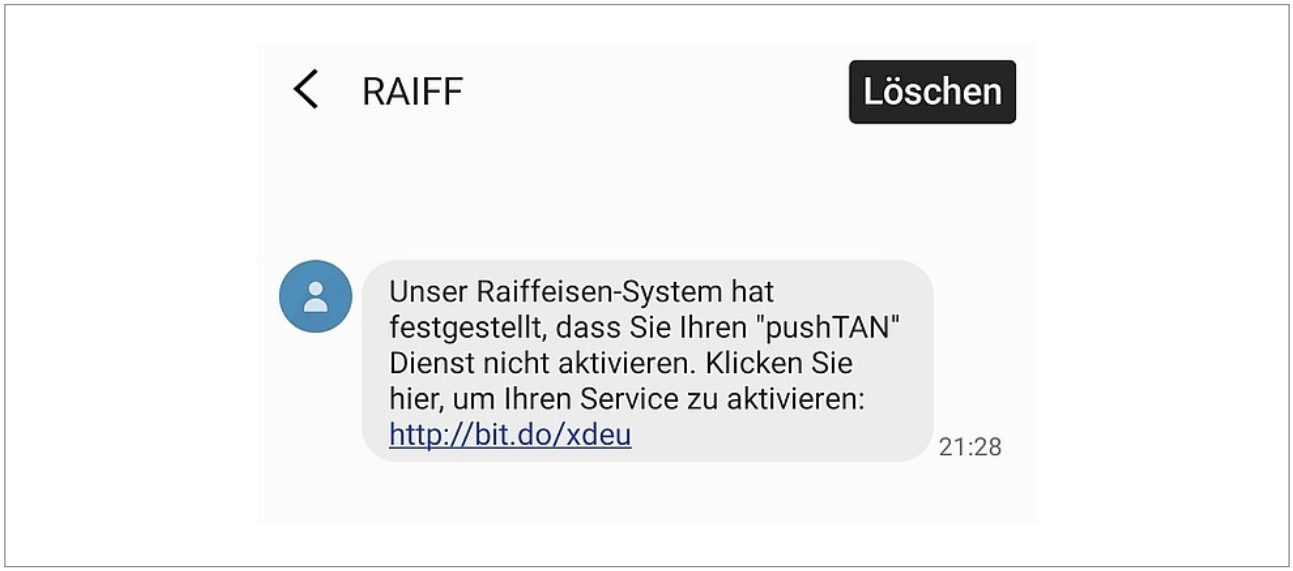

Abbildung 2: Phishing-SMS mit Link

Schritt 2: Nach „Klick“ auf den Link in der SMS – gefakte Anmeldemaske erscheint zur Eingabe der Zugangsdaten (Abfrage von: Verfügernummer und PIN)

Wenn der in der SMS angegebene Link angeklickt wird, erscheint die Maske, wo die Zugangsdaten (Verfügernummer und PIN – Persönliche Identifikations Nummer) eingegeben werden sollen – allerdings ist dies nicht die Anmeldemaske der Raiffeisen Bank, sondern eine Fake-Website der Kriminellen, die die Zugangsdaten sammeln soll:

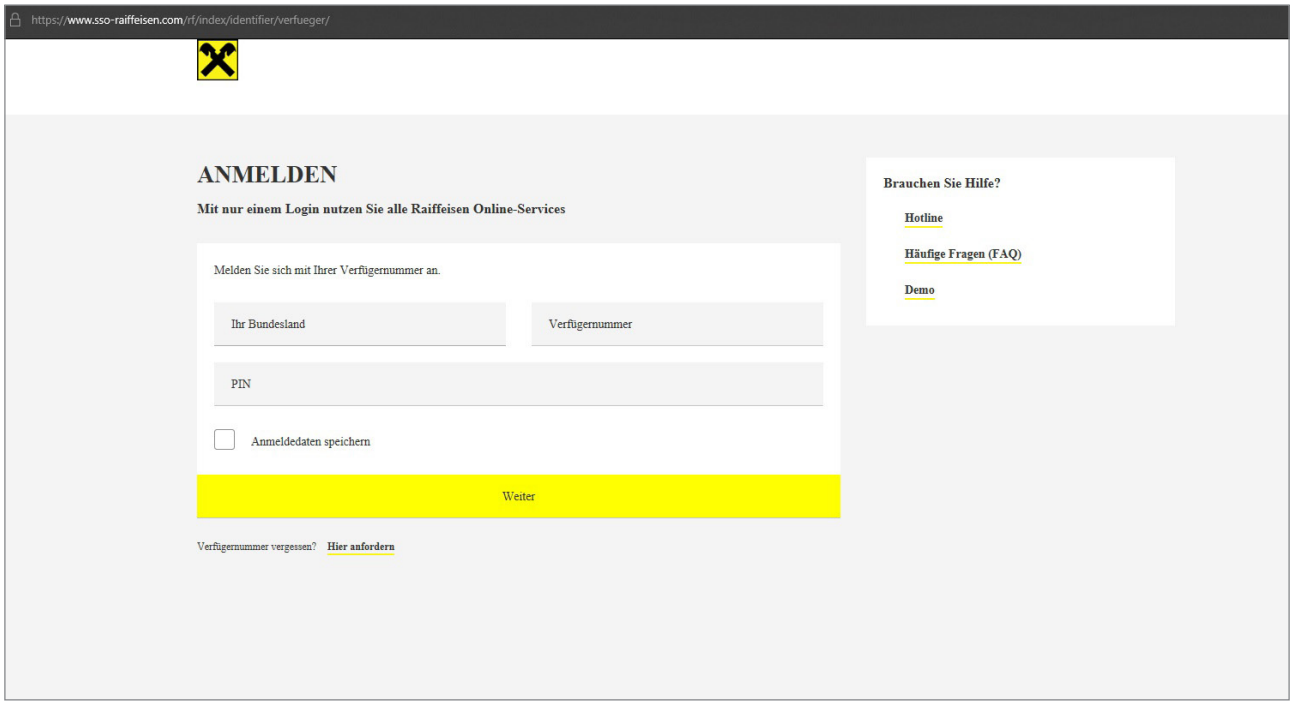

Abbildung 3: Fake-Login-Bereich durch Eingabe-Abfrage des Passwortes

Schritt 3: Abfrage des TAN-Codes (Transaktionsnummern) auf der Fake-Website, der auf das Handy des/der Kontoinhabers/-in gesendet wird.

Der nächste Schritt zum erfolgreichen Betrug: Die Kriminellen haben sich – in Kenntnis von Verfügernummer und PIN – mit den Zugangsdaten des Opfers in das Online-Banking-Konto angemeldet und eine Überweisung gestartet. Die/der Kontoinhaber/-in erhält deshalb einen TAN-Code auf sein/ihr Handy und soll diesen den Kriminellen in das Datenfeld der gefälschten Website eingeben. Wenn das passiert, dann wird die Überweisung freigeben - und das Geld ist vom Konto verschwunden.

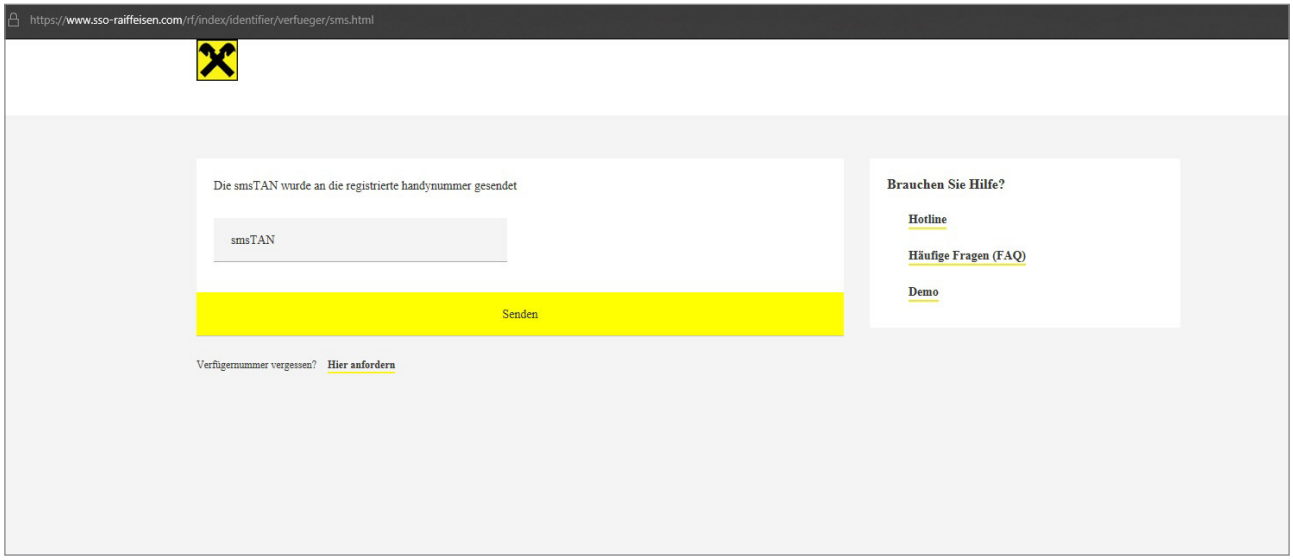

Abbildung 4: Vermeintliche Eingabemaske für den TAN (Transaktionsnummer). Auch diese Maske ist ein Fake (eine Fälschung).

Schritt 4: In einem letzten Schritt Abfrage der Kreditkartendaten auf der Fake-Website.

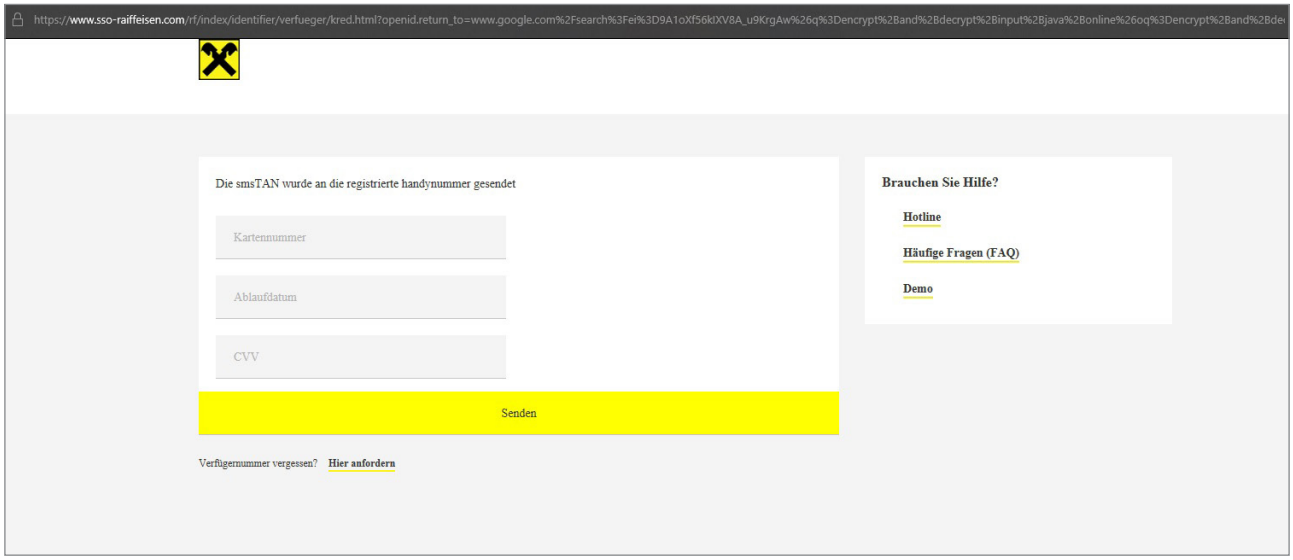

Abbildung 5: Vermeintliche Eingabemaske für die Kreditkartendaten. Auch diese Maske ist ein Fake.

Im letzten Schritt fragen die Kriminellen noch die Kreditkartendaten ihres Opfers ab, die sie für Einkäufe auf fremde Kosten benötigen. Damit ist der Datendiebstahl abgeschlossen.

WORAN ERKENNEN KONSUMENTINNEN PHISHINGMAILS?

KonsumentInnen können Phishing-Nachrichten unter anderem anhand der nachfolgenden Punkte erkennen:

- Banken senden keine E-Mails oder SMS an KundInnen, mit denen sie diese dazu auffordern, dass sie eine Website aufrufen und sich auf dieser mit ihren persönlichen Zugangsdaten anmelden (und gegebenenfalls aus einer unbekannten Quelle eine vermeintliche Sicherheits-App installieren).

- Die Inhalte der gefälschten Nachrichten nennen einen Grund, wie zum Beispiel aktuelle Gesetzesänderungen, der es angeblich notwendig machen, dass KonsumentInnen ihre persönlichen Daten samt Zugangsdaten auf einer Website überprüfen und/oder ein Programm installieren müssen.

- Die gefälschten Nachrichten verlinken auf eine Website, die nicht zur Bank gehört. Das sehen KonsumentInnen in der Adressleiste ihres Webbrowsers, die sie über die tatsächlich aufgerufene Website informiert.

- Die Anrede der Nachrichten ist mit „Sehr geehrter Kunde“ unpersönlich gehalten. Banken benennen ihre KundInnen direkt beim Namen.

- Als Absender scheint zumeist eine Bank auf. Die dazugehörige E-Mailadresse gehört zumeist jedoch einem Dritten.

Impressum

Medieninhaber: Kammer für Arbeiter und Angestellte für Wien,
Prinz-Eugen-Straße 20–22, 1040 Wien, Telefon: (01) 501 65 0
Offenlegung gem. § 25 MedienG: siehe wien.arbeiterkammer.at/impressum

Zulassungsnummer: AK Wien 02Z34648 M
AuftraggeberInnen: AK Wien, Konsumentenschutz
Autoren: Christian Prantner und Jakob Kalina
Grafik Umschlag und Druck: AK Wien
Verlags- und Herstellungsort: Wien

Stand April 2020
Im Auftrag der Kammer für Arbeiter und Angestellte für Wien

#FÜRIMMER

Gesellschaftskritische Wissenschaft: die Studien der AK Wien

Alle Studien zum Download:
wien.arbeiterkammer.at/service/studien

youtube.com/AKoesterreich
twitter.com/arbeiterkammer
facebook.com/arbeiterkammer
@ich.bin.die.gerechtigkeit

ARBEITERKAMMER.AT/100

AK 100 JAHRE GERECHTIGKEIT