Betrugsversuche wg. Identitätsklau per Telefon und Internet häufen sich

Die örtlichen Banken berichten, dass sich in letzter Zeit die Betrugsversuche von Kriminellen häufen. Mit erlangten Daten der Bankkunden wird zunehmend versucht, auf Bankguthaben zuzugreifen.

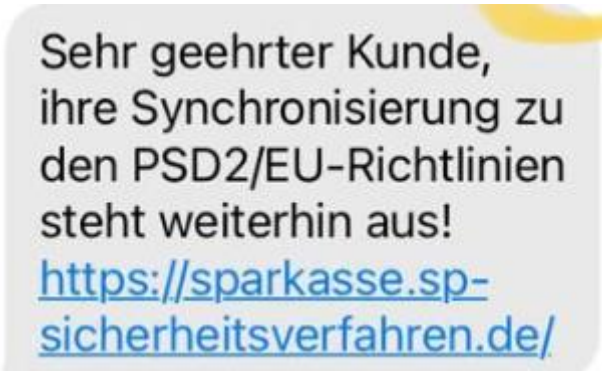
Jüngst hat sich ein Fall zugetragen, der nur durch die Umsicht einer Sparkassenmitarbeiterin ein gutes Ende genommen hat:

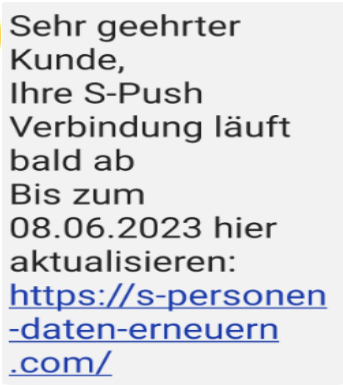
Die angebliche Kundin wollte eine telefonische Überweisung veranlassen. Auf Nachfrage der Sparkassenmitarbeiterin konnten persönliche Daten detailliert genannt werden, so dass eigentlich kein Zweifel an der Identität bestand. Aufgeflogen ist der Betrugsversuch nur an einem Kriterium, das wir aus Gründen von möglichen Nachahmern nicht ausführen wollen.

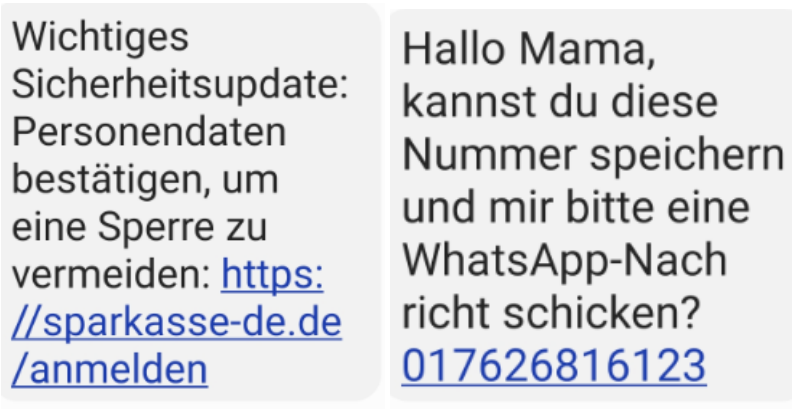
Nach dem Telefonat wurde umgehend mit der echten Kundin Kontakt aufgenommen. Diese sagte, sie hatte 10 Minuten vorher einen Anruf durch eine Dame von einer Datensicherungsfirma erhalten. Ihr wurde versprochen, dass nach Abgleich bestimmter Daten alle Aktivitäten der Kundin zukünftig verschlüsselt erscheinen. Die Kundin hat daraufhin viele persönliche Daten preisgegeben. Ein Fehler, der sehr viel Geld hätte kosten können...Gott sei Dank konnte die Sparkassenmitarbeiterin das Schlimmste verhindern.

Die Redaktion nimmt dies zum Anlass, Tipps und Sicherheitshinweise von Spezialisten zu erfragen, wie man sich schützen kann. Patricia Kaspar und Michael Segl, Mitarbeiter des Medialen Vertriebs der Sparkasse geben wertvolle Auskünfte:

Identitätsklau – wie kann man dies erkennen?
Michael Segl:
Zunächst ist wichtig, dass man die Betrugsmaschen kennt. Dabei kann man nicht zu viel aufklären, denn trotz vielfacher Berichte schaffen es die Kriminellen immer wieder, dass unschuldige und auch eigentliche aufgeklärte Personen auf sie hereinfallen. Ich habe Ihnen hier einige Beispiele mitgebracht:







Alle Versuche – ob am Telefon oder im Internet - zielen darauf ab, Daten direkt zu erhalten oder auf Internetseiten zu leiten, die dann Kontrolle über den Computer oder das Smartphone zu erhalten.

Wie kann ich einen Betrugsversuch von einer echten Nachricht unterscheiden?

Patricia Kaspar: Sehr, sehr schwer. Jeder Bankkunde sollte die Internet- und Mailadresse seiner Bank kennen und auch nur auf diese reagieren, wenn diese wirklich zu 100% stimmt. Bereits ein Bindestrich, ein Punkt oder eine andere Endung (z.B. .net statt .de) kann ein Betrugsversuch sein. Ich empfehle im Zweifelsfall, nicht auf die Nachricht zu reagieren und schon gar nicht auf den eingebetteten Link zu reagieren, sondern mich direkt durch den direkten Aufruf meiner Bank anmelden.

Wenn Sie einen Anruf am Telefon erhalten, werden Sie von echten Bankmitarbeitern nicht nach persönlichen Daten gefragt, da diese bereits vorliegen. Etwas anderes ist es, wenn Sie bei Ihrer Bank anrufen und damit eine Zahlung veranlassen wollen. Hier muss sich der Bankmitarbeiter über Ihre Identität vergewissern. Und die Fragen, die sie dann gestellt bekommen, sollten Sie auch nur beantworten, wenn Sie den Anruf tätigen, aber nicht erhalten.

Seien Sie besonders vorsichtig, wenn Ihnen jemand ungefragt Datensicherheit (Microsoftmitarbeiter oder Sicherheitsfirmen) oder größere Gelder verspricht, ohne dass Sie etwas veranlasst haben oder einen Anspruch haben. Lassen Sie sich nicht auf ein Gespräch ein und legen Sie sofort auf. Mittlerweile gibt es in Deutschland Fälle, wo mit künstlicher Identität Stimmen von vertrauten Personen nachgeahmt wurden und dadurch Zahlungen erschlichen wurden.

Besonders der sog. Enkeltrickbetrug oder wie in Ihrem Fall die letzte Nachricht ist besonders perfide.

Michael Segl: Ja, vor allem, da bei diesen Fällen Emotionen im Spiel sind und Angerufene geschockt werden. Zunächst erschleichen sich die Betrüger das Vertrauen, ein naher Familienangehöriger zu sein, dann wird mit einem schlimmen Ereignis gearbeitet. Meist soll ein Unfall, eine Verhaftung, ein Diebstahl passiert sein und bei aller Betroffenheit soll man schnell reagieren, um dem Familienangehörigen zu helfen. Dabei wird der Angerufene unter Zeitdruck genötigt, Geld zu überweisen. Ich empfehle allen, innerhalb der Familie abhörsicher (also ohne Sprachassistenten) ein Gespräch zu führen und zu vereinbaren, dass man nie auf telefonische dringende Geldforderungen eingehen werde und schon gar nicht auf eine Bitte per Email.

Wie kann ich mich schützen?
Michael Segl und Patricia Kaspar: Wir verbessern ständig unsere Systeme, z.B. haben wir aktuell eine

starke Geräteauthentifizierung vorgeschaltet, wo man im Onlinebanking die zu nutzenden Geräte als sicher mit einer TAN bestimmen muss. Auch informieren wir stets unsere Mitarbeiter/innen, um bekannte Betrugsmaschen zu erkennen. Unsere Kunden können auch auf unserer Homepage stets aktuelle Sicherheitswarnungen und Empfehlungen einsehen (Sicherheit im Internet | Sparkasse Freyung-Grafenau (spk-frg.de)

Vor allem aber ist es wichtig, dass jeder diese Tipps beherzigt:

1. **Gehen Sie vorsichtig mit Ihren Online-Banking-Daten (Anmeldename, PIN und TAN) um- tätigen Sie keine „Testüberweisungen“ auf Anforderung**

2. **Sicherer Umgang mit Telefonaten, E-Mails und Anhängen-**Ihre Sparkasse wird Sie niemals per Telefon oder E-Mail auffordern, Ihre Daten wie IBAN, Anmeldenamen PIN, TAN oder Ihre Kreditkartendaten preiszugeben oder diese auf einer Internetseite einzutragen.
   Bitte beachten Sie: dies gilt auch für Bestätigungs-E-Mails Ihrer Sparkasse bei Änderungen, die Sie im Online-Banking durchführen (Adressänderungen oder pushTAN-Verbindungen).

3. **Aufmerksam bleiben und Tageslimit festlegen** – kontrollieren Sie regelmäßig Ihre Umsätze und legen Sie ein Tageslimit fest, das Ihren regelmäßigen Umsätzen entspricht. Dieses kann schnell und unkompliziert bei einem besonderen Kauf (z.B. Auto) angepasst werden, aber wird natürlich nur selten benötigt

4. **Halten Sie PC und Smartphone stets aktuell -** Auf jedem Computer ist der Einsatz einer aktuellen Anti-viren-Software und einer Personal Firewall unverzichtbar. Gängige Betriebssysteme enthalten eine Firewall, die ein- und ausgehende Verbindungen prüft – achten Sie darauf, dass Sie stets ein aktuelles Betriebssystem und einen aktuellen Internet-Browser verwenden. Für einen optimalen Schutz aktualisieren Sie bitte regelmäßig Ihre Antiviren-Software.

5. **Nutzen Sie einen sicheren Internet-Zugang und Browser -** Vorsicht bei der Datenübertragung über ein kabelloses lokales Funknetzwerk (WLAN). Aktivieren Sie WLAN am besten nur, wenn Sie es gerade brauchen. Wenn Sie ein solches Netz betreiben, ist die Internet-Sicherheit nur dann gewährleistet, wenn Sie die Verschlüsselung aktivieren. Nutzen Sie für Ihr WLAN-Funknetz die Verschlüs-selungsmethode, die den größtmöglichen Schutz bietet. Nähere Informationen zu den verschiedenen Methoden entnehmen Sie bitte der Beschreibung Ihres WLAN-Routers. Wichtig: Verzichten Sie in öffentlich zugänglichen oder nicht abgesicherten Funknetzwerken ("Hotspots") auf Online-Banking. Ihre Daten könnten ausspioniert werden. Weitere hilfreiche Informationen zum sicheren Surfen im WLAN finden Sie beispielsweise beim Bundesamt für Sicherheit in der Informationstechnik.

6. **Sperren Sie im Zweifel Ihren Online-Banking-Zugang oder Ihre Karte über den deutschlandweit kostenfreien Sperr-Notruf 116 116.**

7. **Seien Sie mit Ihren Daten äußerst sorgsam -** Ihre Geburtsdaten, Ihre Kontoverbindung, oder sonstigen Bankdaten benötigen in der Regel nur Sie im direkten Austausch mit Ihrer Bank (Die Initiative geht dabei immer von Ihnen aus- kommen Sie keiner Aufforderung am Telefon oder per Mail nach!) Und fallen Sie nicht auf Fragen herein, in denen Sie etwas preisgeben (z.B. Anrufer meldet sich:“Hallo Oma ich bins“ – und Sie sagen, dann „Beate bist du es?“ – somit haben Sie den Namen ihrer Enkelin verraten. Oder „Ihr Geburtsort ist wie Ihr Wohnort Freyung?“ und Sie entgegnen: „Nein, nein , das ist Grafenau“ und schon hat ein Anrufer eine gewünschte Information)

8. **Wenden Sie sich an Ihre Bank, wenn Sie das Gefühl haben, ungewollt Daten preis gegeben zu haben. Vielleicht kann dann noch was verhindert werden.**

Wir hoffen, mit dieser Aufklärung unsere Kunden und die Leser der PNP zu schützen.