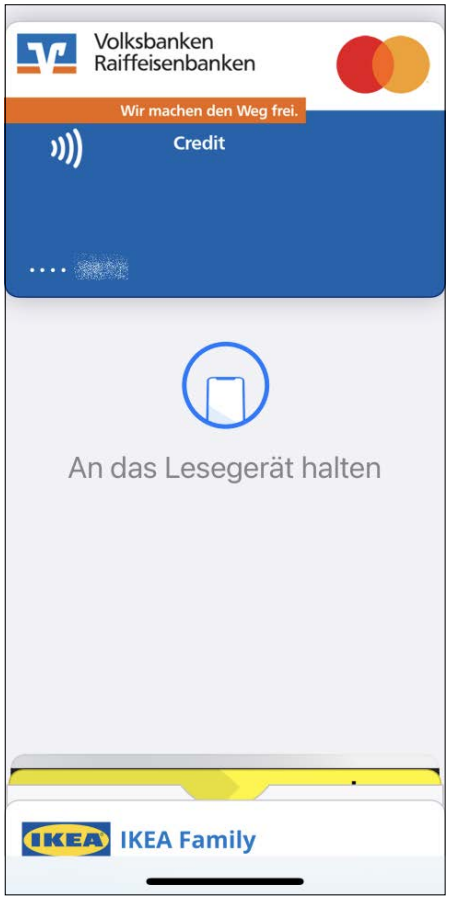
Neue Masche beim Kartenbetrug

Mit einem neuen Trick gelingt es Kriminellen, die Kredit- oder Debitkarte ihres Opfers in Apple Pay oder Google Pay zu missbrauchen – mithilfe eines digitalen Abbilds.

Das Landeskriminalamt (LKA) Niedersachsen warnt vor einer aktuellen Betrugsmasche, mit der Kriminelle Kredit- und Debitkartenbesitzer übers Ohr hauen. Das Schema funktioniert mit Visa, Mastercard und American Express ebenso wie mit der Girocard. Die Täter verleiten das Opfer dazu, ihnen Daten zu übermitteln und die Karte für ihre Smartphones freizuschalten. Mit Apple Pay oder Google Pay können die Täter dann die Karte oder das Konto des Betroffenen leerräumen.

Ausgangspunkt ist in aller Regel eine Phishing-Mail, die vermeintlich von der eigenen Bank oder Sparkasse stammt. Die Mail fordert das Opfer dazu auf, die Kartendaten auf der Homepage des Kreditinstituts aus einem vorgeschobenen Grund zu bestätigen, zu verifizieren oder zu aktualisieren – beispielsweise wegen eines Missbrauchs der Karte, technischen Schwierigkeiten oder einer neuen Rechtslage. Mitunter zeigen auch Suchmaschinen oder andere Webseiten solche Aufforderungen. Ein Link führt das Opfer direkt auf eine präparierte, scheinbar offizielle Internetseite Ihres Finanzinstituts. Dort soll es die Kartendaten einschließlich Ablaufdatum sowie seine Telefonnummer eingeben.



Bei dem neuen Betrugsschema erbeuten die Täter Kartendaten über Phishing und verleiten das Opfer anschließend dazu, ihnen die Karte dauerhaft für Apple Pay oder Google Pay freizugeben.

Kommt das Opfer dem nach, ruft innerhalb kurzer Zeit einer der Täter an und gibt sich als Bankmitarbeiter aus. Während des Gesprächs fordert er dazu auf, eine Push-Nachricht der Bank auf dem Smartphone zu bestätigen, eine TAN einzugeben oder ihm eine TAN zu nennen. Damit gibt das Opfer den digitalen Platzhalter der Karte auf dem Smartphone der Täter frei. Diese können damit nun ohne die PIN der echten Karte nach Belieben einkaufen oder Geld abheben.

Der Rat von LKA und c't: Weder Banken und Sparkassen noch andere Stellen wie Polizei oder Behörden verschicken Mails, in denen sie Kunden respektive Bürger dazu auffordern, Kartendaten zu bestätigen. Daher sollte man niemals darauf eingehen und auf keinen Fall auf Links in solchen Mails klicken. Bei einem tatsächlichen Missbrauchsverdacht sperren die Geldhäuser die Karte. Nach einer Sperre setzen sie sich mit den Betroffenen in Verbindung, meist per Brief, manchmal auch telefonisch. Ähnliches gilt bei technischen oder rechtlichen Problemen.

Echte Bankmitarbeiter werden dabei aber nie Passwörter oder PINs abfragen oder eine Push-Bestätigung oder TAN anfordern – auch nicht über SMS, WhatsApp oder Mail. Generell sollte man sorgfältig den Verwendungszweck prüfen, bevor man eine Zahlung oder Aktion mit seiner Karte per Push-Nachricht oder TAN freigibt. Ruft jemand an und das Telefon zeigt die Nummer der Bank an, ist das außerdem keine Echtheitsgarantie, denn Telefonnummern kann man leicht fälschen.

Da die Opfer die Karte selbst freigeschaltet haben, können sie nicht auf Kulanz des Kreditinstituts hoffen. Bemerken sie unberechtigte Abbuchungen, zum Beispiel auf der Kartenabrechnung oder im Onlinebanking, müssen sie die Karte so schnell wie möglich sperren und sollten Anzeige bei der Polizei erstatten. *(mon@ct.de)*

© Copyright by Heise Medien.
Persönliches PDF für alle Leser der c't aus 30625 Hannover