POLIZEI
Nordrhein-Westfalen
Köln

bürgerorientiert · professionell · rechtsstaatlich

Betrug mit digitalen Zahlungskarten
Präventionshinweise für den Einzelhandel

„Können Sie mir noch 200 Euro auszahlen?“ – Diesen Satz hört man häufig an den Kassen der Supermärkte. Doch Vorsicht – es könnte sich hierbei um einen Betrug mit einer digitalen Zahlungskarte handeln.

Was sind digitale Kredit- und Debitkarten?

Digitale Debit- oder Zahlungskarten sind digitale Abbilder einer physischen Karte auf dem Smartphone oder der Smartwatch. Die digitale Debitkarte wird in den meisten Fällen über die eine sogenannte Wallet der betriebssystem-eigenen Dienste, wie Apple Pay oder Google Pay oder die Apps der Banken im Smartphone hinterlegt. Der Bezahlvorgang an der Kasse im Einzelhandel wird dann mittels Near Field Communication – oder kurz NFC – übertragen.

Wie funktioniert die Betrugsmasche?

Über eine Phishing-Seite geraten die Betrüger an die sensiblen Bankdaten der Betroffenen.
Dies erfolgt beispielsweise über fingierte E-Mails, über Messenger oder soziale Netzwerke im Namen einer Bank oder eines Bezahldienstes wie PayPal. Man wird aufgefordert, seine Bankdaten über die hinterlegte Verlinkung zu aktualisieren oder zu bestätigen. Potenzielle Opfer werden auf täuschend echte Bank- oder PayPal-Seiten weitergeleitet.
Damit die Betrüger die digitale Kreditkarte nutzen können, muss diese noch freigeschaltet werden. Dazu kontaktieren sie ihre Opfer, geben sich zum Beispiel am Telefon als Bankmitarbeitende aus und fordern die angerufene Person unter einem Vorwand auf, eine Push-TAN zu bestätigen, die diese während des Gespräches erhält. Mit der mitgeteilten TAN werden die jeweiligen digitalen Karten dann sofort auf dem Täterhandy freigeschaltet. Der Bezahlvorgang kann ohne den Besitz der physischen Karte oder der PIN abgeschlossen werden.

Wie agieren die Täter und Täterinnen?

- Ist die die digitale Karte auf dem Täterhandy eingerichtet, wird versucht, in kurzer Zeit einen möglichst hohen Bargeldbetrag zu generieren. Die z. Zt. gängige Masche ist der Erwerb von Gutscheinkarten (5 - 50 Euro) oder geringwertiger Waren beispielsweise Zigaretten.
- Beim Kauf wird eine Cashback-Auszahlung in Höhe von 200 Euro verlangt. Die Zahlung erfolgt mittels Apple Pay oder Google Pay. Es kann zu mehreren Cashback-Auszahlungen nacheinander kommen.

Profil und Erscheinungsbild der Täter und Täterinnen

- Bei den Tätern und Täterinnen handelt es sich häufig um eher jüngere Personen (15-25 Jahre).
- Sie versuchen oftmals ihr äußeres Erscheinungsbild zu verschleiern. Dies geschieht beispielsweise durch das Tragen von Mund- und Nasenschutz, Sonnenbrillen, Basecaps oder Kapuzen, die tief ins Gesicht gezogen werden.

Die Polizei bittet um Ihre Mithilfe

- Die Polizei möchte insbesondere das Verkaufspersonal für diese Betrugsmaschen sensibilisieren und um Unterstützung bitten:
- Seien Sie misstrauisch, wenn größere Bargeldsummen als Cashback-Auszahlung verlangt oder mehrere Auszahlungen nacheinander gefordert werden.
- Lassen Sie sich im Verdachtsfall den Personalausweis zeigen und fotografieren Sie diesen.
- Lassen Sie sich durch Ihr Sicherheitspersonal / Ladendetektiv unterstützen.
- Verständigen Sie die Polizei unter der 110 und melden den möglichen Betrug.
- Sichern Sie evtl. vorhandenes Videomaterial.
- Achten Sie auf Begleitpersonen und mögliche genutzte Fahrzeuge. Notieren Sie das
- Kennzeichen, wenn möglich.

Helfen Sie mit!

Die Bedeutung des stationären Einzelhandels ist nicht zu unterschätzen! Die Mitarbeitenden an den Kassen - als „letztes Glied“ in dieser Betrugsmasche - können einem möglichen Betrug noch vorbeugen!

Weitere Informationen erhalten Sie auf den

Internet Seiten der Polizei Köln
Polizeiberatung
LKA Niedersachsen – Betrug mit digitalen Debitkarten

Polizeipräsidium Köln - Kriminalkommissariat Kriminalprävention/Opferschutz
Walter-Pauli-Ring 2-6, 51103 Köln, Tel.: 0221 229-8655, E-Mail:
kriminalpraevention.koeln@polizei.nrw.de
Stand: 12/2024 - MV