SPARKASSE
CASSA DI RISPARMIO

SKIMMING
Wie Bankomat- und Kreditkarten geklont werden

Betrüger werden immer einfallsreicher, wenn es darum geht, an Kartendaten und Geheimnummern zu gelangen. So ist in letzter Zeit eine markante Zunahme von ‘Skimming‘-Fällen an Geldautomaten auf nationaler und auch internationaler Ebene zu verzeichnen.

Der Datenklau passiert dabei ganz unbemerkt bei der Behebung von Bargeld am Automaten. Die Betrüger bringen einen Vorbau am Kartenschlitz an, den sogenannten ‘Skimmer‘, der beim Einführen der Karte den Magnetstreifen und somit die darin enthaltenen Daten liest. Eine Miniaturkamera, die unauffällig am Bankomat-Gerät montiert ist, zeichnet die Eingabe der Geheimzahl auf und sendet die Aufnahme anschließend per Funk an den Täter. Der Betroffene bemerkt in der Regel davon nichts und hegt auch keinen Verdacht, da er die Abhebung problemlos zu Ende führen kann.

Ähnlich wird hin und wieder mit **Türöffner-Attrappen** versucht, an die Geheimnummern und Kontodaten zu gelangen. **Diese fragen die PIN ab, wo normalerweise das Einschieben der Kartegenügt um die Tür zu öffnen**.

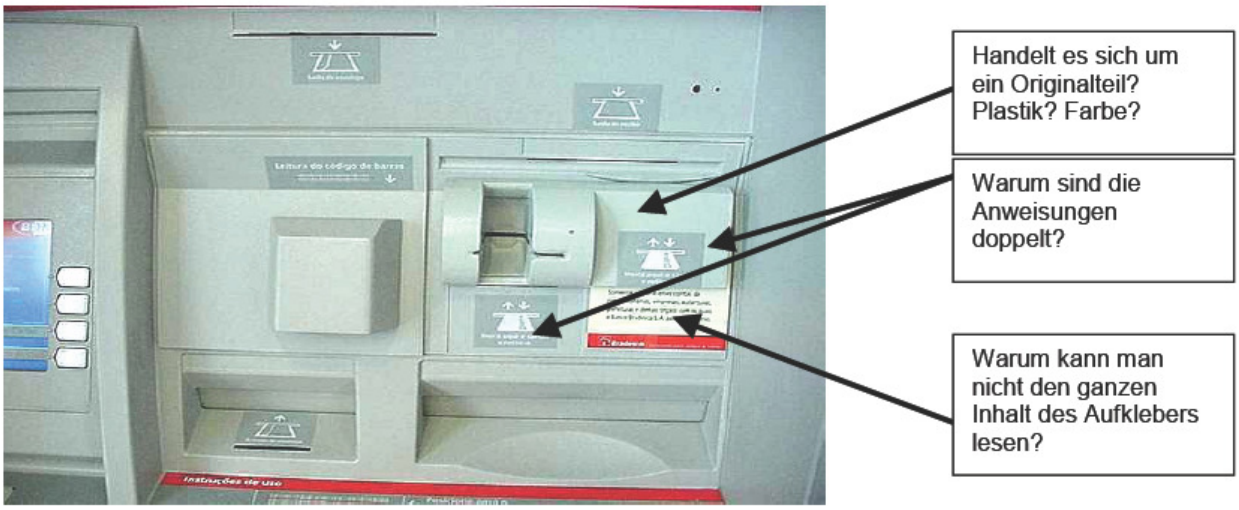
Vorsicht ist jedenfalls mehr als angebracht. Besonders an Wochenenden sollten Sie vermehrte Wachsamkeit walten lassen. Fallen Ihnen verdächtige Vorrichtungen, Zettel oder Spuren wie Klebstoffrückstände am Bankomat-Gerät oder den Kartenlesegeräten am Eingang zu den Self-Service Zonen auf, kontaktieren Sie unverzüglich die Behörden!

SPARKASSE
CASSA DI RISPARMIO

Wie kann man sich einen manipulierten Geldausgabeautomaten vorstellen?

Folgende Bilder sollen in Form eines Beispiels veranschaulichen, wie Betrüger Bancomat-Geräte manipulieren können, so dass Sie in den Besitz von Kartendaten sowie Geheimnummern gelangen.

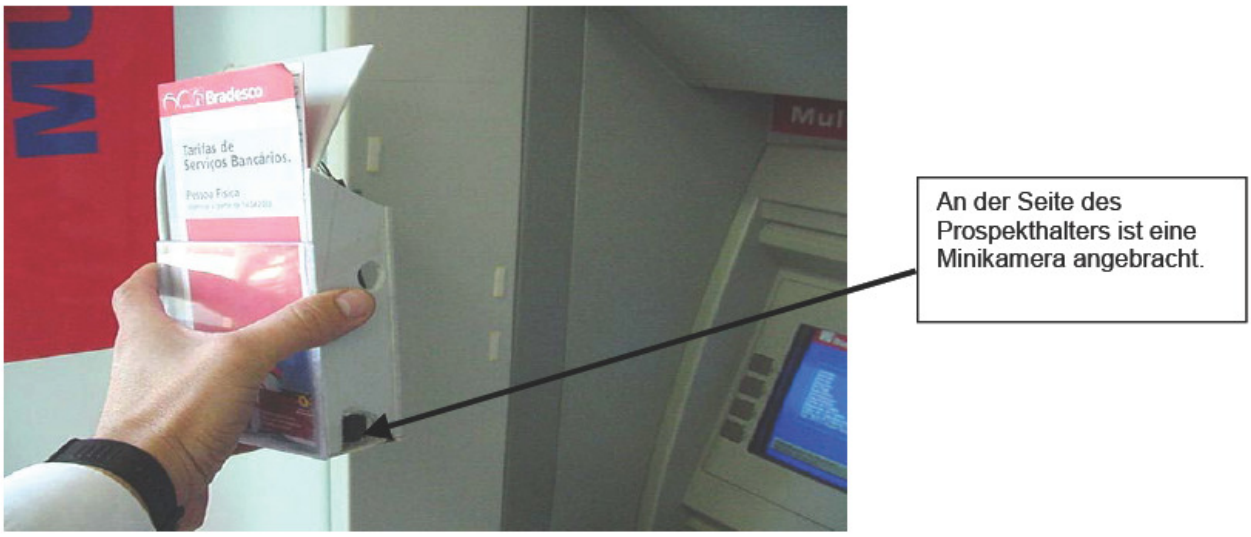
Ein auf den ersten Blick scheinbar gewöhnlicher Bankomat.



In Wahrheit wurde ein Vorbau am Kartenschlitz angebracht, „durch“ den die Karte in den eigentlichen Kartenschlitz eingeführt wird.

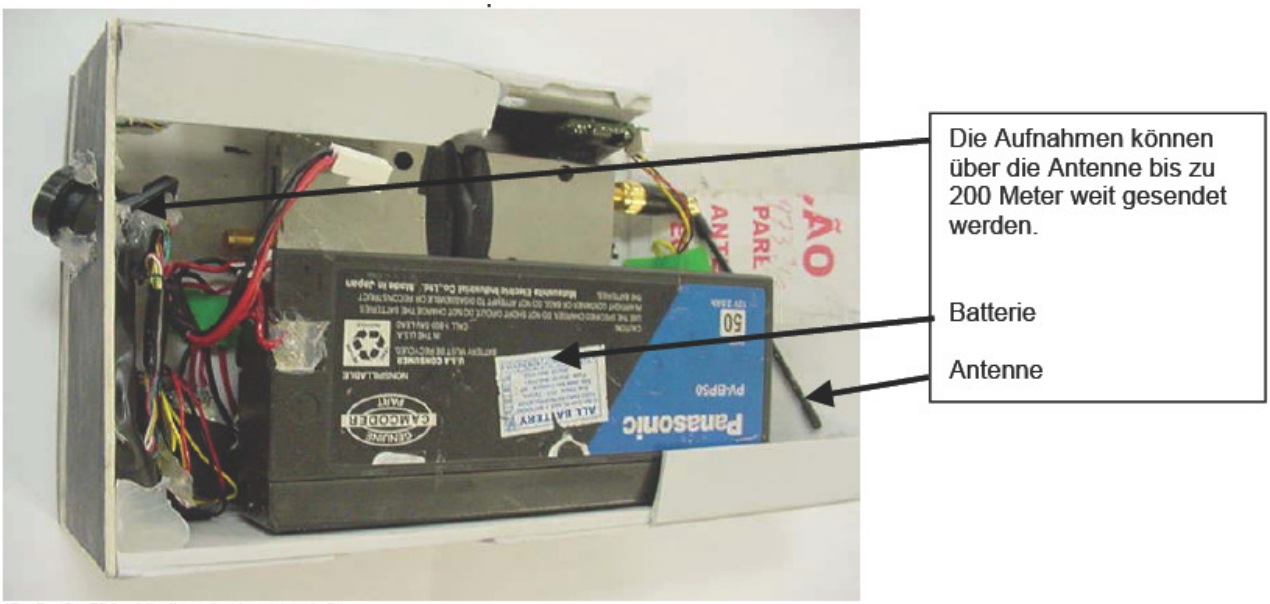
In der Nähe des Bildschirms bzw. der Tastatur ist ein unscheinbarer Prospekthalter angebracht.

Der sich jedoch bei genauer Betrachtung als High-Tech-Gerät entpuppt



Die Miniaturkamera hält zum einen fest, was am Bildschirm angezeigt wird und zum anderen, was der Kunde mittels Tastatur eingibt.

Das Innenleben des vermeintlichen Prospekthalters.



(Quelle aller Bilder: http://www.bradesco.com.br/)

Die Aufnahmen können über die Antenne bis zu 200 Meter weit gesendet werden.

SPARKASSE
CASSA DI RISPARMIO

Was versteht man unter Lebanese Loop?

Dabei handelt es sich um eine weitere Form des „Kartenklaus“. Ziel des weniger verbreiteten „Lebanese Loop“ ist es, an die Originalkarte zu kommen. Dazu wird ein Modul auf den Bankomaten aufgesetzt, das die Karte blockiert bzw. einbehält. Um an die PIN zu kommen wird entweder wie beim Skimming mit versteckten Kameras gearbeitet oder aber mit zusätzlichen Ablenkungsmanövern. Dabei gibt es auch besonders kaltschnäuzige Gauner, die dem Kunden bei diesem Scheindefekt auch noch beratend zur Seite stehen und so an die Geheimzahl gelangen. Sobald der Kunde gegangen ist, wird der Aufsatz abgebaut und die Karte entnommen.