Chroń swoje karty

Data publikacji: 4.03.2021 17:35

Przestępstwo polegające na nielegalnym skopiowaniu zawartości paska magnetycznego karty płatniczej bez wiedzy jej posiadacza w celu wytworzenia kopii i wykonywania nieuprawnionych płatności za towary i usługi lub wypłat z bankomatów nazywa się Skimming. Przestępstwo to nie omija także kart chipowych.

Fot: Policja

Jak informuje policja, istnieją dwa rodzaje skimmingu: skimming w placówce handlowej oraz skimming bankomatowy.

Skimming w placówce handlowej polega na wykonaniu kopii karty przez sprzedawcę lub inną osobę, która weszła w jej chwilowe posiadanie. Ponieważ w takiej sytuacji przestępcy nie zawsze mają możliwość poznać kod PIN sklonowanej karty, kopie mogą wykorzystać tylko w przypadku kart, które nie wymagają autoryzacji przy pomocy PIN-u, i tylko w płatnościach za towary i usługi. Nie mogą wykorzystać skopiowanej karty do pobierania pieniędzy z bankomatów.

Znacznie bardziej niebezpieczny jest **skimming bankomatowy**, polegający na tym, że przestępcy instalują na bankomatach lub w ich wnętrzu (czytniku) specjalne urządzenia, które służą do pozyskiwania danych z paska magnetycznego lub chipa (czytnik) oraz PIN-u: kamera, fałszywa klawiatura lub płaska płytka obwodu umieszczona w czytniku na kartę dzięki której można podsłuchać i zmanipulować komunikację między terminalem a chipem i uzyskać numer PIN. Zarejestrowane w ten sposób informacje są najczęściej transmitowane drogą radiową i służą do produkcji fałszywych kart, za pomocą których możliwe jest pobieranie gotówki z kont klientów banków za pośrednictwem bankomatów.

Jeżeli mamy możliwość, to lepiej korzystać z bankomatów wewnątrz banków (istnieje mniejsze prawdopodobieństwo, że przestępcy odważą się zamontować tam urządzenia skimmujące). Mundurowi apelują także, by zwracać uwagę na wygląd bankomatów, szczególnie na wystające, niepasujące do całości jego elementy jak klawiatury, nakładki na miejsce wsuwania karty, elementy znajdujące się nad klawiaturą bankomatu, gdzie mogą zamontowane być miniaturowe kamery.

Wpisując natomiast kod PIN, należy zasłaniać ręką klawiaturę tak, aby kod nie został zauważony przez inne osoby lub zarejestrowany przez kamerę jeżeli przestępcy zdołali ją w pobliżu zainstalować. Jeśli bankomat wzbudza podejrzenia, lepiej jest skorzystać z innego lub poprosić o sprawdzenie pracownika banku.

Karty bankomatowe, szczególnie te z możliwością transakcji zbliżeniowych chronimy przed możliwością odczytania danych przez skimmerów w specjalnym etui, które eliminuje takie działanie na odległość, na przykład w środkach komunikacji miejskiej lub centrach handlowych

red./policja