

Voorlichting voor ondernemers over skimming van betaalpassen

Wat is skimming?

Skimming is een vorm van betaalpasfraude, waarbij criminelen de magneetstrip kopiëren van een betaalpas (bv pinpas of credit card) en de pincode bemachtigen op het moment dat er een rechtmatige transactie wordt verricht. Vervolgens maken ze een kopie van de pas. Hiermee kunnen ze geld opnemen en betalen in binnen- en buitenland. Het komt voor dat criminelen dat doen door bij ondernemers in te breken en de betaalautomaat te manipuleren.

Is elektronisch betalen veilig?

Betaalpasfraude is altijd erg vervelend. Het is het werk van georganiseerde criminelen die internationaal werken. In Nederland is het aantal fraudegevallen zeer laag in verhouding tot het aantal betalingen met betaalpas. De betaalpas is en blijft een veilig betaalmiddel. Bovendien verhoogt elektronisch betalen de veiligheid in uw onderneming. Als er minder geld in de kassa zit, is het niet meer zo aantrekkelijk om een overval te plegen.

Hoe weet u of een betaalautomaat veilig is?

Alle Nederlandse betaalautomaten zijn uitgebreid getest op veiligheid. De organisaties die het elektronische betalingsverkeer regelen, werken voortdurend aan het verbeteren van de veiligheid en signaleren verdachte transacties. Fraude is echter niet geheel uit te sluiten. Mocht u bij het elektronisch betalen door een klant iets vreemds opvallen, waarschuw dan de politie of het meldpunt onveilige betaalsituaties (030 – 283 65 55).

Wat heb ik als ondernemer te maken met skimming van betaalpassen?

Als ondernemer zult u niet snel direct financiële schade leiden door skimming van betaalpassen, mits u aan de acceptatievoorwaarden voldoet. Het is een pas van een consument die wordt misbruikt. Let wel; als ondernemer kunt u aansprakelijk zijn wanneer personeel passen kopieert of wanneer u bepaalde controleverplichtingen (met name met creditcards) niet nakomt. Als skimming bij uw onderneming heeft plaatsgevonden kan dit nadelige effecten hebben voor uw imago en leiden tot omzetsderving doordat klanten uw onderneming gaan mijden. Bovendien krijgt het vertrouwen in elektronisch betalen een deuk wanneer fraude op grote schaal zou toenemen. We zijn dus allemaal gebaat bij een veilig elektronisch betalingsverkeer.

Wat kunt u als ondernemer doen om fraude met betaalpassen te voorkomen?

De belangrijkste tips zijn:

1. Plaats betaalapparatuur na sluitingstijd achter slot en grendel. Kan dat niet; richt waar mogelijk een beveiligingscamera of bewegingsmelder op de kassa met de betaalapparatuur.
2. Laat betalingen door zo min mogelijk personeelsleden verrichten.
3. Is er ingebroken (zowel wanneer er spullen zijn verdwenen als wanneer dat niet het geval lijkt te zijn), controleer met name de betaalapparatuur en onderzoek ook of er ergens verborgen camera's zijn geplaatst.
4. Controleer dagelijks bij opening of er buiten uw medeweten iets is gebeurd met of veranderd aan de betaalapparatuur.
5. Controleer indien mogelijk de aangeboden betaalpassen op echtheid.

Hebt u nog vragen?

Over uw betaalautomaat: Neem contact op met uw betaalautomatenleverancier om preventieve maatregelen te bespreken.

Algemene informatie: Op de website www.allesoverbetalen.nl staat meer informatie over het betalen met een betaalpas en over betalingsverkeer in het algemeen. Via deze website zijn ook tips te vinden over een veilige opstelling van betaalapparatuur.