Banka kartı bilgilerinin korunması

V01 I Ocak 2019

CORPORATE STORE DEVICE TRAINING DEPARTMENT

INDITEX ITX MERKEN

Banka kartı bilgilerinin korunması

Kredi kartı ve banka kartı bilgileri (kart numarası, son kullanma tarihi, CVV ve PIN kodu) çok **hassas** bilgilerdir. Bu yüzden:

- Mağazalarımızda banka kartlarının **hileli kullanımı engellemeli**;
- Müşterilerimizin **bilgilerini korumalı**;
- Inditex grubunun bu bilgilerle ilgili dahili kurallarına hakim olmalı ve **bu kuralları uygulamalıyız**.

Müşteri ilişkilerinde…

… müşterinin kişisel bigilerine saygı göstermeli ve bu bilgilerle işlem yaparken güvenlik uygulamalarını kullanmalıyız.

Bununla ne demek istiyoruz?

- Kasa güvenlik kurallarına her zaman saygı gösterin
- Banka kartı bilgileri kişiye özel ve çok hassas bilgilerdir, bu yüzden bu bilgileri hiç bir zaman (ne kağıda ne de dijital bir uygulamaya) **not etmeyin** ve **üçüncü kişilerin bu bilgilere ulaşmasına asla izin vermeyin**.
- Banka kartı ile işlem yaparken **müşterinin gözü önünde olduğunuzdan** ve **müşterinin banka kartını her zaman görebildiğinden** emin olun.
- **PIN-kodunun** (banka kartının güvenlik numarası) gizli olduğunu unutmayın, müşteri PIN-kodunu **giriş yaparken cihaza bakmayın**.
- Ödeme ve iade işlemlerini yaparken **sadece yetki verilmiş cihazları** yani PINPAD'leri, datafonları vs. kullanın.

Kart numarasına özel dikkat gösterin

Kartların sahiplerini korumak için, **hiçbir belge veya cihazda kart numarasının tamamının gösterilmemesi** çok önemlidir.

Gösterilmesine izin verilen rakamlar yalnızca ilk 6 ve son 4 rakamdır.

1234567890121234 ✗

1234******561234 ✗

123456******1234 √

**********1234 √


Online Card EUR 7.99
SALE
Card Number: 542418******1765
Mastercard
Expired date.....: 0812
VERIFONE TEST 1

Bu konu çok önemlidir, bu nedenle izin verilenden daha çok rakamın gösterildiğini veya basıldığını tespit ederseniz derhal bildirin.

Kartla ödeme cihazlarının korunması

Kartla ödeme cihazlarının **hileyle değiştirilmesini ya da manipüle edilmesini** engellememizde şu şekilde yardımcı olabilirsiniz:

01.- Cihazların **teknisyen tarafından bakımı ya da değiştirilmesi** sırasında:

- Bakım ya da değiştirme işlemine **yetki verildiğinden** emin olun;
- Teknisyenin **kimliğini kontrol edin**

02.- Şu durumlarda **cihazları kullanmayın:**

- **Anormal durumlar** belirirse (normalde belirmeyen mesajlar, olağandışı işlem hataları vs.)
- Cihazın **manipüle edildiğine dair belirtiler** varsa (cihazın görünümünde farklılıklar, çatlaklar/kırıklar vs.)

03.- Sabah kasalari açmadan önce, olası usulsüzlükleri tespit etmek için kredi kartı ile **ödeme araçlarının hızlı bir şekilde kontrolünü yapın**. Herhangi bir durum tespit ederseniz **yöneticinize haber verin**.

Aşağıda böyle durumları tespit etmenize yardımcı olacak bazı örnekler görebilirsiniz.

Kartla ödeme cihazlarında manipülasyona dair belirtiler

Cihazda muhtemel değişiklikler

Cihazın kullanımında fark edeceğiniz en ufak bir fark bile cihazda değişiklik yapıldığına işaret olabilir veya yanlýþ bir cihazla deðiþtirilmiþ olan.

Resimdeki örnek:

Bu durumda cihaza sonradan eklenen bir parça sebebiyle kart cihaza tamamen sokulamıyor ve bu durumda kartın magnetik okuyucudan geçirilmesi zorunluluğu doğuyor. Magnetik okuyucuların güvenliği çok daha düşüktür ve bu okuyuculara dışarıdan müdahale etmek çok daha kolaydır.

Kartla ödeme cihazlarında manipülasyona dair belirtiler

Cihazda muhtemel değişiklikler

Cihazda yeni parçalar ve **harici değişiklikler** cihazda değişiklik yapıldığına dair belirtiler olabilir.

Resimdeki örnek:

Cihazın kablosu değiştirilmiş. Bu değişiklik hırsızların cihazdan bilgi çalmak için eklediği fazladan kabloları saklamada kullanılabilir

Kartla ödeme cihazlarında manipülasyona dair belirtiler

Cihazda muhtemel değişiklikler

Cihazın **estetik görüntüsündeki ufak değişiklikler bile** kredi kartı hırsızlığına dair belirtiler olabilir.

Resimdeki örnek:

Çıkartmanın altına kurulmuş mekanizma, müşterinin PIN-kodu girişini kaydetmede kullanılır.

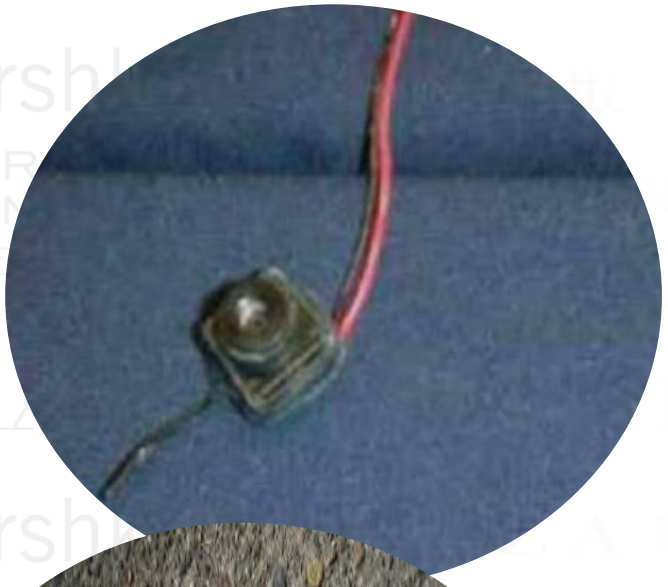
Kartla ödeme cihazlarında manipülasyona dair belirtiler

Garanti etiketleri

Tüm cihazlarda **güvenlik/garanti etiketleri** mevcuttur. Bu etiketler cihazın **kimi vidaları ya da kapakları üzerine** yerleştirilmiştir ve cihazın içinin açılıp açılmadığını anlamakta kullanılırlar.

Dolandırıcılar bu etiketleri çıkarıp, kendi etiketlerini yapıştırırlar.

İki resimdeki etiketleri inceleyin ve aralarındaki farklara dikkat edin.



Kartla ödeme cihazlarında manipülasyona dair belirtiler

Şüpheli ek cihazlar

Müşterilerin **PİN-kodlarını kaydetmede** sıkça kullanılan başka bir cihaz da **kamera**dır.

Bu kamera ve kamera pili genelde cihazın **vida kaplama parçaları altına**, sadece lensi dışarıda kalacak şekilde yerleştirilir.

Kartla ödeme cihazlarında manipülasyona dair belirtiler

Şüpheli ek cihazlar

Dolandırıcılıkta kullanılan kart okuyucuları, banka kartlarının takılabileceği yuvalardan herhangi birine yerleştirilmiş olabilir. Bu okuyucular kartın **yakınında** bulunduğundan **NFC (temassız bilgi aktarımı) teknolojisini** kullanabilirler.

NFC teknolojisi ile dolandırıcılık vakalarında dolandırıcılar kart okuyucusu yerine, cihazın yakınına **dışarıdan yerleştirdikleri bir sensörden** de faydalanabilir.

Bazı durumlarda **gizli ufak okuyucular** da kullanılıyor olabilir.

Banka kartı bilgilerinin korunması

Dikkatli olun ve hemen harekete geçin!

Cihazların manipüle edilmesi durumlarına karşı, müşterilerin kendileri dahil olmak üzere **sürekli dikkatli olun**. Mağaza çalışanları söz konusu olduğunda bile.

Şüpheli bir durumla karşılaşırsanız (manipülasyon belirtileri, hırsızlık, cihazlar üzerinde yeni parçalar ya da daha önceden olmayan uygulamalar, şüpheli ya da riskli hareketler vs.):

…**hemen mağaza sorumlusu ile, cihaz sorumluları ile, İnsan Kaynakları ile ve Kayıp Önleme ile ve Mağaza Güvenliği ile irtibata geçin.** Tüm şüpheli durumlar, bu departmanlar/kişiler tarafından Kart Bilgilerini Koruma Grubu'na (carddataprotection@inditex.com) ya da Dijital Veriler, Ödeme Cihazları ve Bilgi Güvenliği departmanlarına rapor edilmelidir.