1) Her temsilci ve çalışanı Pratik İşlem para transfer sistemini kullanmaya başlamadan önce suç gelirinin aklanması, terörün finansmanı ve dolandırıcılığın önlenmesi eğitimini tamamlamak zorundadır.

2) Temsilci, "Müşterini Tanı" prensipleri çerçevesinde müşteri davranışlarını, işlemlerini ve müşteriden aldığı yanıtları değerlendirir, müşterinin dolandırıcılık kurbanı olduğuna dair şüphe duyarsa, işlemi reddeder.

3) Tüm temsilciler, aşağıda yer alan müşteri davranışlarını analiz etmelidir. Kullanıcılar, aşağıda yer alan müşteri davranışlarına karşı dikkatli olmalı, potansiyel bir dolandırıcılık girişiminin önüne geçmek adına müşteriye ilave sorular sormalıdır.
   3.1) Endişeli veya şaşkın görünen müşteriler, özellikle yaşlılar ve bağımlı yetişkinler,
   3.2) Para transfer hizmetini kullanan birine göre aşırı heyecanlı müşteriler,
   3.3) Acil durum sebebiyle para gönderen fakat duruma ilişkin çekinceleri olan müşteriler,
   3.4) Tanımadığı birine ilk defa para gönderen müşteriler,
   3.5) Telefon pazarlaması ile ürün satın alacağı yanılgısına düşen müşteriler.
   3.6) Hayatında ilk defa bu kadar büyük bir meblağ transfer eden, bu sebeple gergin, heyecanlı müşteriler,

   NOT: Tüm yaşlı ve yardıma muhtaç kişilere, para transfer etmek istedikleri kişiyi tanıyıp tanımadıkları sorulmalıdır. Çünkü bu kişiler, dolandırıcıların kolayca hedefi olabilmektedir.

4) Temsilciler ve hizmet noktaları da doğrudan dolandırıcıların hedefi olabilir. Dolandırıcılar, temsilciyi arayarak bilgisayar sistemine erişim sağlamak için çalışanları ikna etmeye çalışırlar. Bir kez erişim sağladıklarında ise temsilciyi maddî kayba uğratabilecek para transferleri gerçekleştirirler. Aşağıda bu girişimlere yönelik yaygın metotlardan bahsedilmiştir.

   4.1) Uzaktan erişim kandırmacası: Dolandırıcı, temsilciyi arayarak kendisini Pratik İşlem teknik çalışanı olarak tanıtır. Bir güncelleme çalışması kapsamında bilgisayara uzaktan bağlanması gerektiğini söyler. Uzaktan erişime izin verilir ise tüm kontrol dolandırıcının eline geçmiş olur.

   4.2) Bilgisayara sızma: Dolandırıcı, temsilciyi arayarak/e-posta atarak kendisini Pratik İşlem yetkilisi olarak tanıtır. Bu durum, tuzak linklere tıklanması, e-postaların açılması sonucunda kullanıcı ID ve şifresinin yetkisiz kişilerle paylaşılmasına sebep olabilir.

   4.3) Test işlem kandırmacası: Dolandırıcı, temsilciyi arayarak kendisini Pratik İşlem yetkilisi olarak tanıtır. Sistemin doğru çalıştığını kontrol etmek amacıyla bir veya birkaç adet test mahiyetinde giden para işlemi yapması yönünde kullanıcıyı yönlendirir. Kullanıcı talimatları izler ve işlemleri gerçekleştirir ise dolandırılmış demektir. Bunlar, işlem bedeli tahsil edilmeden gerçekleşen, maddi zarara sebep olan dolandırıcılık işlemleridir.

   4.4) Kod girişi: Dolandırıcı, temsilciyi arayarak kendisini Pratik İşlem yetkilisi olarak tanıtır. Dolandırıcı, sözde göndereceği formun doldurulmasını talep eder. Formda, hassas ödeme verileri ve müşteri kişisel bilgileri gibi işlem güvenliği ve gizliliğini sağlayan bilgiler istenir ve bu bilgiler ile tutarlar tahsil edilmeye çalışılır. ödeme verileri ve müşteri kişisel bilgileri gibi işlem güvenliği ve gizliliğini sağlayan bilgiler istenir ve bu bilgiler ile tutarlar tahsil edilmeye çalışılır.

Saygılarımızla,
Pratik İşlem Ödeme Kuruluşu A.Ş.