Dijital kanallarda
güvenli işlemler için bilgiler

Kamuoyu Duyurusu

11 Ekim 2024

Son dönemde, internet ve mobil kanallarda yaşanan dolandırıcılık vakalarının artması nedeniyle kamuoyunu bilgilendirme ihtiyacı doğmuştur.

Aşağıda, sıkça karşılaşılan dolandırıcılık yöntemlerine ve bu yöntemlerden korunma yollarına dair bilgilere yer verilmiştir:

Sıklıkla karşılaşılan dolandırıcılık türleri şunlardır:

- İnternetten Alışveriş Dolandırıcılığı: Sahte internet siteleri ve güvensiz alışveriş platformları üzerinden yapılan dolandırıcılık.
- Sosyal Mühendislik Yöntemleriyle Dolandırıcılık: Kişisel bilgilerin manipülasyon yoluyla ele geçirilmesi.
- Sosyal Medya Dolandırıcılığı: Sosyal medya platformlarında sahte hesaplar aracılığıyla yapılan dolandırıcılık.
- e-Posta Dolandırıcılığı: Sahte e-posta adreslerinden gelen mesajlar ile kişisel bilgilerin ele geçirilmesi.
- Oltalama Saldırıları: Sahte sms ve e-postalar yoluyla kişisel bilgilerin çalınması.
- Uzaktan Erişim Dolandırıcılığı: Cihazlara uzaktan erişim sağlayarak bilgi ve para çalma girişimleri.
- Zararlı Yazılım Dolandırıcılığı: Bilgisayarlara veya mobil cihazlara zararlı yazılımlar yükleyerek veri hırsızlığı yapılması.

Bu dolandırıcılık yöntemlerinden korunmak ve finansal güvenliğinizi artırmak için şu hususlara dikkat etmelisiniz:

1. SMS, e-posta veya sosyal medya yoluyla gelen bildirimlerdeki bağlantılara/linklere kaynağından emin değilseniz tıklamayın. Hizmet aldığınız kuruluşun resmi iletişim kanallarını kullanarak doğrulama yapın. Tek tık, sizi sahte sitelere veya virüslere yönlendirebilir.
2. Banka hesaplarınızı hiç kimseye kullandırmayın. Hesaplarınızın yasa dışı faaliyetlerde kullanılması halinde ağır hapis cezalarıyla karşılaşabilirsiniz.
3. Şifrelerinizi kimseyle paylaşmayın. Kendini savcı, polis, asker, banka çalışanı, avukat olarak tanıtan veya bir ödül, prim iadesi, kart aidatı iadesi için sizden şifrenizi, kart bilgilerinizi ve kişisel verilerinizi talep eden kişilere itibar etmeyin, bu amaçla gelen linklere tıklamayın.
4. Güvenliğinizden emin olmadığınız mobil uygulamaları cihazlarınıza yüklemeyin. Güvenlik açığı bulunan veya korsan uygulamalar, kişisel bilgilerinizi ele geçirebilir, cihazınıza zarar verebilir ve hatta kimlik hırsızlığına yol açabilir.

5. Bankalarca yapılan güvenlik duyurularını takip edin. Bilgilerinizin güncel kalması için bu duyurularda iletilen uyarıları dikkate alın.
6. Telefonunuza, bilgisayarınıza, tabletinize yüklediğiniz uygulamanın istenen izinlerini dikkatlice kontrol edin. Bankacılık uygulamalarınızı resmi uygulama mağazalarından indirin. Bilinmeyen veya güvenilir olmayan kaynaklardan uygulama indirmeyin.
7. Bankacılık uygulamalarında kullandığınız şifrelerinizi, başka uygulamalarda ve alışveriş sitelerinde kullanmayın. Daha az güvenlikli sitelerde şifreleriniz ele geçirilebilir, bankacılık uygulamalarınıza bu şifreler denenerek giriş yapılabilir.
8. Güvenliğinden emin olmadığınız internet sitelerinden alışveriş yapmayın. Dolandırıcılık amaçlı açılmış sahte bir site üzerinden dolandırılabilirsiniz.
9. Banka hesap özetlerinizi ve işlemlerinizi düzenli olarak kontrol edin, şüpheli bir durumda vakit kaybetmeden bankanızla iletişime geçin.

Bu kapsamda; dolandırıcılık vakalarına ilişkin olarak resmi kurumlar ve hizmet alınan kuruluşlar tarafından yapılan tüm uyarılar ve bilgilendirmeler dikkate alınmalıdır.

Kamuoyunun bilgisine sunulur.

Saygılarımızla,

Türkiye Bankalar Birliği