

BİLGİ GÜVENLİĞİ VE GÜVENLİ KULLANIM REHBERİ

Değerli Kullanıcılarımız ve Ziyaretçilerimiz,

Hangipara Elektronik Para ve Ödeme Hizmetleri A.Ş. olarak, bilgi güvenliğinizi ve kişisel verilerinizin korunmasını en üst düzeyde önemsiyoruz. Türkiye Cumhuriyet Merkez Bankası (TCMB) düzenlemeleri ve küresel bilgi güvenliği standartları uyarınca, dijital platformlarda güvenliğinizi sağlamak amacıyla dikkat etmeniz gereken asgari hususları aşağıda bilgilerinize sunarız.

1. Kimlik Doğrulama Bilgilerinin ve Şifrelerin Güvenliği

- **Kişiyi Özel Bilgiler:** Uygulamamız üzerinde kullanacağınız şifre, PIN kodu, tek kullanımlık SMS onay kodları (OTP) ve kişisel bilgilerinizi **hiç kimseyle (şirket personelimiz dahil)** kesinlikle paylaşmayınız.
- **Güçlü Şifre Kullanımı:** Şifrelerinizin kolay tahmin edilemeyecek (ardışık sayılar, doğum tarihi vb. içermeyen) karmaşık yapılarda olmasına özen gösteriniz ve şifrelerinizi belirli periyotlarla güncelleyiniz.
- **Bilgilerin Saklanması:** Şifre ve PIN kodlarınızı dijital veya fiziksel ortamlarda başkalarının erişebileceği şekilde yazılı olarak saklamayınız.

2. Oltalama (Phishing) ve Sosyal Mühendislik Saldırıları

- **Resmi Kanallarımızı Kontrol Edin:** Şirketimiz adına gönderilmiş gibi görünen ancak şüpheli ibareler barındıran e-posta, SMS veya sosyal medya mesajlarına karşı dikkatli olunuz. Şirketimizin resmi internet adresi yalnızca **www.hangipara.com.tr** dir.
- **Adres Çubuğu Kontrolü:** Sitemize giriş yaparken tarayıcınızın adres çubuğunda güvenli bağlantıyı simgeleyen kilit işareti (HTTPS protokolü) bulunduğundan emin olunuz.
- **Ödül/Hediye Vaatlerine İtibar Etmeyiniz:** Sosyal medyada veya arama motorlarında şirketimizin adını ve logosunu taklit ederek "ödül kazanma", "hediye çeki" veya "masraf iadesi" vaatleriyle sizden şifre ya da kart bilgisi talep eden sahte internet sitelerine kesinlikle itibar etmeyiniz.

3. Cihaz ve Ağ Güvenliği

- **Güncel Yazılımlar:** Dijital servislerimize erişmek için kullandığınız bilgisayar, akıllı telefon ve tablet gibi cihazların işletim sistemlerinin ve tarayıcılarının güncel olmasına dikkat ediniz.
- **Güvenilir Ağlar:** Finansal işlemlerinizi veya kullanıcı girişlerinizi, halka açık ve şifresiz Wi-Fi (kablosuz internet) ağları üzerinden gerçekleştirmemeye özen gösteriniz.

- **Lisanslı Programlar:** Cihazlarınızda lisanssız/korsan yazılımlar kullanmayınız ve güvenilir bir antivirüs/anti-malware programı bulundurmayı tercih ediniz.

4. Şüpheli Durumların Bildirilmesi

- Sistemlerimize erişim sağladığınız cihazınızın kaybolması/çalınması, şifrelerinizin yetkisiz kişilerce ele geçirildiğinden şüphelenmeniz veya şirketimiz adına yapılan şüpheli bir iletişimle karşılaşmanız durumunda, vakit kaybetmeksizin resmi iletişim kanallarımız üzerinden bizimle irtibata geçmeniz kritik önem arz etmektedir.