

## Dijital Güvenlik Rehberi

### **Kişisel Bilgilerinizi ve PİN'lerinizi Bilgisayarınızda/Cep Telefonunuzda Saklamaktan Kaçın**

Kimlik kartınız çok önemli bir belgedir. Bu nedenle, kimlik kartınızın taranmış kopyasını bilgisayarınızda saklamayın. Kullandığınız ürünle ilgili kullanım ve güvenlik bilgilerini düzenli olarak takip ettiğinizden emin olun. Banka kartı şifrenizi ve internet bankacılığı şifrenizi kartınızda, cüzdanınızda veya çantanızda bulundurmaktan veya cep telefonunuza kaydetmekten kaçın.

### **Bilgilerinizi Paylaşmaktan Kaçın**

E-Bankacılık/mobil bankacılık şifresi, kart bilgileri, kart şifresi, SMS ile gönderilen mobil onay kodu ve tek kullanımlık şifreler kişisel bilgilerinizdir. Güvenlik açısından bu tür bilgileri Bankamız personeli de dahil olmak üzere üçüncü kişilerle paylaşmaktan kaçınmalısınız.

### **Bilgisayarınızın Güvende Olduğundan Emin Olun**

Lisanslı işletim sistemi ve programları kullandığınızdan emin olun ve işletim sisteminizi ve yazılımınızı düzenli olarak güncelleyin. Anti-virüs, anti-spyware ve kişisel güvenlik duvarı gibi güvenlik kalkanları kullandığınızdan emin olun. İnternet kafe gibi ortak kullanılan bilgisayarlarda bankacılık işlemleri yapmaktan kaçın.

### **Kişisel Bilgilerinizi Soran E-postalara/Aramalara Cevap Vermekten Kaçın**

Bankalar, e-posta yoluyla kişisel bilgilerinizi veya şifrelerinizi istemez. Parolalarınız sözlü, yazılı veya IVR üzerinden soruluyorsa, bu gibi durumlarda asla bilgi vermeyin ve +383 38 245 245 numaralı telefonda bizlerle iletişime geçin.

Size yardımcı olmak için size telefon numaralarını veren kişilerden yardım almayı kabul etmeyin.

### **PİN'inizin Güvenlik Seviyesinin Yüksek Olduğundan Emin Olun**

Tuttuğunuz takımın kuruluş yılı veya doğum günleri, özel gün ve tarihler veya telefon numaraları gibi kolay anlaşılır şifreler seçmeyin.

<https://www.isbankkosova.com/EN> sitemizi kullanmak için herhangi bir linke tıklamak yerine tarayıcınızın adres çubuğuna [www.isbankkosova.com](http://www.isbankkosova.com) yazmanız yeterlidir. İnternet Şubemiz "https" protokolü kullanmaktadır.

### **Güvenliği Bilinmeyen Kablosuz Ağları Kullanmaktan Kaçın**

Wi-Fi, Bluetooth ve Kızılötesi gibi kablosuz yöntemler, cep telefonlarına yetkisiz erişim riskine yol açabilir. Bu nedenle güvenli bulmadığınız kablosuz ağları kullanmaktan kaçın.

Kaynağını ve güvenliğini bilmediğiniz Bluetooth üzerinden aktarılan dosyaları kabul etmekten kaçın; ihtiyacınız olmadığında bu tür uygulamaları kapalı tutun.

### **Cep Telefonunuzu Güvenlik Kodu, Tuş Kilidi gibi uygulamalar ve Güncel Anti-Virüs Yazılımları ile Koruyun**

Kötü amaçlı yazılımlar cep telefonunuzdaki bilgileri çalabilir, kullanıcının bilgisi dışında bir şey arayabilir veya SMS gönderebilir. Bu tür yazılımlardan korunmak için;

- Mobil uygulamaları güvenli uygulama mağazalarından indirin
- Tanımadığınız kişilerden gelen e-posta ve ekleri açmayın
- Anti-virüs yazılımı kullanarak korumayı destekleyin