MÜŞTERİ GÜVENLİK BİLGİLENDİRMELERİ

Güvenliğiniz İçin

Şirketimiz müşterilerinin güvenliğini her zaman ön planda tutmakta olup bu kapsamda çalışmalarını sürdürmektedir.

Şirketimiz kanalları aracılığıyla gerçekleştirilen tüm işlemlerinizin kaydı sistemlerimizde tutulmakta olup bu kayıtlar müşteri bilgilerinin gizliliği kapsamında güvenli ortamlarda saklanmaktadır.

Bilgi güvenliğiniz açısından Şirketimiz adı ve logosu kullanılarak Şirketimiz tarafından gönderilmiş gibi gösterilen dolandırıcılık amaçlı SMS, e-postalarda ve Şirketimiz adına açılan sahte sosyal medya hesaplarında yer alan linkleri tıklamayınız.

Zaman Kontrolü Uygulaması

Uygulamaya girdikten sonra 10 dakika içinde işlem yapmaz iseniz sizin güvenliğiniz için otomatik olarak parola giriş ekranına çıkartılırsınız. Böylece bilgisayarınızın başından ayrılsanız bile bir başkasının işlem yapmasını engellemiş olursunuz.

Bilgilerin Bütünlüğü ve Güvenliğini Sağlıyoruz

Web sitemiz ile sizin bilgisayarınız arasındaki verilerin gizliliği ve bütünlüğü TLS (Transport Layer Security) 1.2. 256 bit şifreleme ile korunmaktadır. Giriş sayfasında adres alanında sertifika bilgilerinin yeşil renkte olduğunu kontrol ediniz.

Güvenli Çıkış

İşlemlerinizi tamamladıktan sonra çıkmak istediğinizde sağ tarafta yer alan “Güvenli Çıkış” butonunu kullanmanızı öneriyoruz. Uygulamaya girdikten sonra 10 dakika içinde işlem yapmaz iseniz sizin güvenliğiniz için otomatik olarak şifre giriş ekranına çıkartılırsınız.

Dolandırıcılıkta Dikkat Edilecek Hususlar

Dolandırıcılık, günümüzde maalesef yaygın bir sorun haline gelmiştir. Güvenliğiniz açısından Şirketimiz adı ve logosu kullanılarak Şirketimiz tarafından gönderilmiş gibi gösterilen, dolandırıcılık amaçlı SMS, e-postalarda ve Şirketimiz adına açılan sahte sosyal medya hesaplarında yer alan linkleri tıklamayınız.

Kullanıcılarımızın, dolandırıcılık girişimlerine karşı dikkatli olması önemlidir. İşte dikkat etmeniz gereken bazı hususlar:

Kişisel ve Finansal Bilgilerinizi Paylaşmayın: Hesap bilgileri, kimlik numarası, şifreler gibi kişisel bilgilerinizi asla başkalarıyla paylaşmayın. Şirketimiz, sizden bu tür bilgileri asla talep etmez.

Şüpheli E-postalara Dikkat: Bilinmeyen veya şüpheli kaynaklardan gelen e-postalara dikkat edin. Bu e-postalar, sizden kişisel bilgilerinizi veya parolanızı isteyebilir. Bu tür e-postaları hemen silin ve açmayın.

Güncel Yazılım Kullanın: Uygulamayı kullanırken cihazınızda güncel bir antivirüs programı ve güvenlik yazılımı bulundurun. Bu, zararlı yazılımların ve virüslerin cihazınıza bulaşmasını engeller.

Hesap Güvenliğiyle İlgili Dikkat Edilmesi Gerekenler

Şirketimiz, kullanıcıların güvenliğini sağlamak için çeşitli önlemler almaktadır. Ancak sizin de güvenliğiniz için dikkat etmeniz gereken bazı noktalar vardır:

Güçlü Parola Kullanın: Uygulamaya giriş yaparken güçlü bir parola kullanmanız önemlidir. Parolanızı düzenli olarak değiştirin ve başkalarıyla paylaşmaktan kaçının.

Düzenli Güncellemeleri Kontrol Edin: Uygulamanın güncellemelerini düzenli olarak kontrol edin ve en son sürümü kullanmaya özen gösterin. Güncellemeler, yeni güvenlik önlemleri ve hata düzeltmeleri içerebilir.

Parolanızı güçlü ve benzersiz bir şekilde oluşturun. Başkalarının tahmin edemeyeceği karmaşık bir kombinasyon kullanın ve düzenli olarak değiştirin.

Parolanızı kimseyle paylaşmayın ve başkalarının erişimine izin vermeyin.

Oturumunuzu her zaman güvenli bir bağlantı üzerinden (HTTPS) gerçekleştirin.

Cihazınızı ve tarayıcınızı güncel tutun, güvenlik güncellemelerini zamanında yükleyin.

Fraud İşlemleri Hakkında Bilgilendirme

Şirketimiz, fraud işlemlerini tespit etmek ve önlemek için gelişmiş algoritmalar kullanmaktadır. Ancak sizin de fraud işlemlerine karşı dikkatli olmanız önemlidir. Bazı fraud işlemleri ve alınabilecek önlemlere aşağıda yer verilmiştir:

Oltalama Saldırıları (Phishing): Oltalama saldırısı, sahte web siteleri veya e-postalar aracılığıyla kişisel bilgilerinizi çalmayı amaçlayan bir dolandırıcılık yöntemidir. Sahtekarlığı gerçekleştirecek kişi/kişiler; bir banka, kart şirketi veya finansal işlemler gerçekleştiren bir finans şirketinden geliyormuş gibi hazırladığı sahte e-postayı, elde edebildiği tüm e-posta adreslerine gönderir. E-postanın konusu; müşterilerin bilgilerinin güncellenmesi veya şifrelerin değiştirilmesi amacı içeren ifadelerden ve ilgili kurumların sayfalarının birebir kopyası şeklinde görünen internet sayfalarına giden linklerden oluşmaktadır. Her zaman güvenilir kaynaklara erişim sağlayın ve şüpheli bağlantılara tıklamaktan kaçının.

Sahte Siteler: Dolandırıcılar, özellikle banka ve finans kurumlarının sitelerinin görsel olarak benzerlerini hazırlayıp bu sitelere girilen bilgilerin kendilerine gönderilmesini sağlayabilirler. İnternet dolandırıcıları, bu sahte sitelere arama motorlarındaki reklam/sponsor linkleriyle ziyaretçi çekebilecekleri gibi, gerçek sitenin adresinin çok benzeri bir adrese yerleştirerek kişilerin yanlışlıkla gelmelerini de bekleyebilirler.

Kimlik Avı: Kimlik avı, sahte kişilerin sizin yerinize işlem yapmasıdır. Bu tür durumlarda, hesap hareketlerinizi düzenli olarak kontrol edin ve şüpheli aktiviteleri hemen bildirin.

Kart Dolandırıcılığı: Kart dolandırıcılığı, kart bilgilerinizi çalmayı amaçlayan bir saldırıdır. Kart bilgilerinizi güvende tutmak için güvenilir alışveriş sitelerini tercih edin ve düzenli olarak hesap hareketlerinizi kontrol edin.

Keylogger: Bilgisayar kullanıcılarının internette dolaşırken klavye kullanarak girdikleri bilgileri kaydeden ve bu bilgileri kötü niyetli kişilere gönderen bir yazılım türüdür. Keylogger yazılımları, yeterince korunmayan bilgisayarlara korsanlar tarafından sistem açıklarından yararlanılarak uzaktan yüklenebileceği gibi kullanıcı tarafından oyunlar, e-postalar, vb. aracılığıyla farkında olmadan da yüklenebilir. Keylogger yüklenmiş bir bilgisayardan web sitesine giriş yapıldığında kullanılan tüm bilgiler korsanlar tarafından ele geçirilebilir.

Screenlogger: Keylogger ile aynı prensipte çalışan ve klavye tuşları yerine ekran görüntülerini kaydeden bir yazılım türüdür. Bilgisayarınızda tıkladığınız her anın resmini çekerek kaydeden bu programlar sayesinde sanal klavye kullanılarak girilen bilgiler de ele geçirilebilmektedir.

Güvenli Kullanım Kılavuzu

- Şirketimiz e-posta aracılığıyla kişisel bilgilerinizi ya da şifrelerinizi kesinlikle talep etmemektedir. Aldığınız e-posta sizi kişisel bilgilerinizi veya parolanızı girmeniz için bir siteye yönlendiriyorsa, derhal 0850 522 56 23'ü arayarak Destek Hattı'mıza bilgi veriniz ve lütfen hiçbir bilgi girişi yapmadan tarayıcı programınızın penceresini kapatınız.
- Kurumsal giriş sayfasındayken tarayıcınızın adres çubuğunda kilit olup olmadığını kontrol ediniz. Kilit üzerine çift tıklanınca açılan sertifikada görüntülenen adres bilgisinin (issued to) parao.com.tr olduğundan emin olunuz.
- İnternet kafe gibi internetin ve bilgisayarın ortak kullanıldığı alanlarda uygulamamıza girmemeye dikkat ediniz.
- Uygulamamızda işlemlerinizi sona erdirdikten sonra mutlaka "Güvenli Çıkış" butonunu kullanınız.
- Uygulamamıza erişim yaptığınız bilgisayarlarda "Desktop Firewall" (kişisel güvenlik duvarı) veya "windows firewall" (windows güvenlik duvarı) uygulamaları kullanınız. Bu uygulamalarla kullanılmayan port ve servisleri kapatınız.
- Devamlı güncellenen bir Antivirüs ürünü kullanınız.
- Uygulamamıza girerken kullanılan parola girişlerinde sanal klavyeyi tercih ediniz.
- Kullandığınız parolaların, basit ve tahmin edilebilir olmamasına özen gösteriniz.
- Uygulamamıza girdiğinizde son hesap hareketlerinizi kontrol ediniz, olağandışı durumlarda Destek Hattı'mızı arayınız.
- Şirket personeli dahil hiç kimseye parolanızı hiçbir zaman söylemeyiniz ve kişisel bilgilerinizi üçüncü şahıslarla paylaşmayınız.
- Parolanızı herhangi bir yere yazmayınız ya da kaydetmeyiniz.