

MÜŞTERİ BİLGİLENDİRME METNİ

İnternet, doğası gereği sınırları geniş bir yapı üzerinde kurulduğu için sahtekârlık, dolandırıcılık, virüs bulaşması, yetkisiz erişim, şifre ve kişisel bilgilerin çalınması gibi kötü niyetli saldırılara maruz kalma riski taşır. T.O.M KATILIM BANKASI A.Ş. ("TOM BANK") bu riskleri asgari seviyede tutmak için teknolojinin imkân sağladığı bütün önlemleri almıştır. Bilinçli bir internet kullanıcısı olarak aşağıda belirttiğimiz konularda bilgi sahibi olmanız, kendinize ait önlemleri almanız internet üzerinden size sunduğumuz hizmetlerden daha güvenli olarak yararlanmanızı sağlayacaktır.

- İnternet tarayıcısının adres çubuğunda çıkan yeşil kilit simgesi, sitemizin T.O.M KATILIM BANKASI A.Ş.'ye ait olduğu ve güvenli olarak kullanabileceğiniz anlamına gelir.
- Diğer internet sitelerinde ya da e-postalarda yer alan bağlantılara güvenmeyin. Bu bağlantıları erişim için kullanmayın.
- Kaynağından emin olmadığınız SMS ya da e-posta yoluyla gönderilen linklere tıklamayın. Bu linklere tıklamanız halinde ise bu sitelerde kişisel bilgilerinizi, şifrenizi kullanmayın.
- TOM BANK mobil uygulamasını indirerek hesabınıza erişmek istemeniz durumunda, tek kullanımlık SMS şifresi telefonunuza iletilmektedir. SMS şifrenizin cep telefonunuza SMS mesajı olarak iletilmesinde aksaklık yaşamanız halinde derhal 0 850 762 42 34 numaralı çağrı merkezimizi ve abonesi olduğunuz GSM operatörünüzü arayınız.
- Hassas verileriniz olan kart numaranızı ve şifrenizi korumanız ve gizli tutmanız; üçüncü kişilerle paylaşmamanız gerekir. Şifrenizin üçüncü kişiler tarafından kullanılmasıyla doğabilecek zarar ve kayıplardan T.O.M KATILIM BANKASI A.Ş. sorumlu değildir. Kullanıcı olarak sizlerin hak ve sorumluluklarınız şirketimizle imzalamış olduğunuz bankacılık hizmetleri sözleşmesi içerisinde yer almaktadır.
- Şifrelerinizi kolayca tahmin edilebilir kişisel bilgilerinizden ya da bunların kombinasyonundan oluşacak şekilde belirlemeyin.
- Kartınız kuryeden teslim aldıktan sonra hiçbir nedenle tekrar kurye görevlisine vermeyin. Zarfın açık olmadığından emin olun.
- Kartınızı kaybederseniz zaman kaybetmeden 0 850 762 42 34 numaralı çağrı merkezimizi arayarak kartınızı iptal ettirin.
- Dolandırıcılık girişimlerine maruz kalmamak için kart şifrenizi şirket personeli dahil olmak üzere hiç kimse ile paylaşmayın. Dolandırıcılık şüphesi durumunda zaman kaybetmeden 0 850 762 42 34 numaralı çağrı merkezimizi arayarak durum bildiriminde bulunmanız gerekmektedir.
- Hesap hareketlerinizi belirli aralıklarla kontrol edin. Gerçekleştirmedeğinizi düşündüğünüz ya da şüphelendiğiniz herhangi bir işlem olduğunu fark ederseniz hemen 0 850 762 42 34 numaralı çağrı merkezimizi arayın.

- Bilgilerinizi cüzdanınızda ya da çantanızda yazılı olarak taşımayın. Kart şifrenizi kartınızın üzerine yazmayın. Mutlaka ezberleyin ve şifre bilgilerinin yazılı olduğu belgeleri başkalarının ulaşabilecekleri yerlerde saklamayın.
- TOM BANK mobil uygulamasına giriş yaparken ekranı izleyen kişilerin varlığına dikkat edin.
- Uygulama üzerinde 5 dakika boyunca herhangi bir işlem yapmazsanız oturumunuz güvenliğinizi amacıyla sonlandırılacaktır.
- TOM BANK hiçbir zaman müşterilerinin şifrelerini soran, kişisel bilgilerini talep eden veya güncellenmesini isteyen e-postalar göndermez.
- Kendisini TOM BANK veya şirket temsilcisi olarak tanıtır sizden para göndermenizi isteyen, şifre, hesap bilgilerinizi talep eden kişilere itibar etmeyin.
- Tanımadığınız kişilere kesinlikle para transferi yapmayın.
- Kartınızın ya da SMS şifresi gönderilen telefonunuzun kaybolma, çalınma, zorla alınma gibi herhangi bir nedenle elinizden çıkması halinde vakit kaybetmeden 0 850 762 42 34 numaralı çağrı merkezimizi arayarak bildirmeniz gerekmektedir.
- Hizmet alımında yaşadığınız aksaklıklara yönelik şikayetlerinizi 0 850 762 42 34 numaralı çağrı merkezimizi arayarak ya da destek@tombank.com.tr adresine mail atarak bildirebilirsiniz.
- Sunulan hizmetlere ilişkin bilgilendirmelere, kesintilere, duyuru ve uyarılara www.tombank.com.tr internet adresinden ulaşabilirsiniz ya da 0 850 -762 42 34 numaralı çağrı merkezimizi arayarak bilgi alabilirsiniz.
- www.tombank.com.tr internet adresimizden ya da 0 850 762 42 34 numaralı çağrı merkezimiz ve 0 850 757 42 34 operasyon birimlerimiz dışındaki herhangi bir kanal aracılığı ile gelen bilgilere itibar etmeyiniz.
- Mobil hizmetlerimiz 7/24 kullanıma açık olup bu kapsamda temsilcilerimiz aracılığı ile sunduğumuz hizmetler temsilcilerimizin mesai saatleri ile sınırlıdır.
- TOM BANK tarafından sunulan mobil uygulamaya, şifre ve TOM BANK'A bildirmiş olduğunuz cep telefonu numarasına gelecek güvenlik onay şifresini (SMS OTP) kullanmak suretiyle erişim sağlayabilirsiniz. İlk girişinizden sonra uygulama cihazınızı tanıyacak olup sonraki girişlerinizde cep telefonu numaranıza güvenlik onay şifresi (SMS OTP) olmadan giriş yapabileceksiniz.
- TOM BANK, hizmetlerinden faydalanmanız için sunduğu tüm hizmet kalemlerine ilişkin toplam maliyet ve kullanım miktarının görüleceği, tahakkuk ettirilen aylık ve yıllık ücretler, indirimler, kesintiler, işlem ücretleri, hesap işletim ücretleri, komisyonlar gibi kırımları ayrı ayrı içeren bir ekstreyi, tercihinize göre basılı olarak veya kalıcı veri saklayıcısı ile ve her iki durumda da ücretsiz olarak tarafınıza sunacaktır.

- İşletim sisteminizi düzenli olarak güncelleyin. En son çıkan güvenlik yamalarını (Security Patch) yükleyiniz. Böylece, olası güvenlik açıklarının kullanılmasını önleyebilirsiniz.
- Her zaman internet tarayıcınızın en güncel sürümünü kullanın.
- Telefonunuza kaynağı bilinmeyen, az sayıda kullanıcı, lisanssız programlar indirmeyin. Mutlaka bir anti virüs yazılımı kullanın ve bu yazılımı düzenli olarak güncelleyin.
- Bilgisayarınıza, bir güvenlik duvarı kurun ve etkinleştirin.
- Sadece güvenilir kaynaklardan temin ettiğiniz yazılımları kullanın.
- Halka açık kablosuz ağlar üzerinden bankacılık işlemlerinizi yapmayınız, Güvenliği düşük ve ortak kullanıma açık ağların farklı kişiler tarafından istismar edilebileceğini unutmayınız. Bankacılık işlemleri için kendi telefonunuzun interneti ile gerçekleştirin.
- Kullanmadığınız zamanlar telefonunuzun bluetooth, Airdrop özelliğini kapatınız. Bluetooth ve AirDrop özelliğinin kapanması siz farkında değilken telefonunuza yapılacak yetkisiz erişimleri engelleyecektir. Bluetooth üzerinden gelen kaynağını bilmediğiniz dosyaları kabul etmeyiniz.
- Mobil uygulamaları Apple, Google Play ve Windows store'lardan indiriniz. Bunların dışındaki kaynaklardan indirilmiş uygulamalar zararlı yazılım barındırabilir.
- Uygulama ve işlem güvenliğine yönelik, bilgisayar ve mobil cihazlarda kullandığınız uygulamaların erişim ve yetki isteklerini kontrol ediniz.
- Şifrelerinizi verirken aşağıdaki kurallara dikkat etmeniz gerekmektedir. Şifrenizin geçerli ve güvenli olması için aşağıdaki özelliklerde olmalıdır:
- Ardışık ya da tekrar eden rakamlardan (123456, 111111 gibi) oluşmamalıdır.
- Rakamlardan oluşmalı ve 6 haneli olmalıdır.
- T.C. kimlik, müşteri veya telefon numarası ya da doğum tarihi gibi kolay tahmin edilebilir bilgiler içermemelidir.
- Yeni şifreniz, son 3 şifrenizden farklı olmalıdır
- Şifrenizi bilgisayarınıza ve mobil cihazlarınıza kaydetmeyiniz. Bu bilgileri kartın üzerine yazmayınız, cüzdanınızda saklamayınız ve cep telefonunuza kaydetmeyiniz.
- Şifrenizi bilgisayarınıza ve mobil cihazlarınıza kaydetmeyiniz. Bu bilgileri kartın üzerine yazmayınız, cüzdanınızda saklamayınız ve cep telefonunuza kaydetmeyiniz.