BANKAMIZ MOBİL ŞUBE & İNTERNET BANKACILIĞI & ÇAĞRI MERKEZİ & ATM GÜVENLİK UYGULAMALARI BİLGİLENDİRME DOKÜMANI

Bankamız tarafından sunulan elektronik bankacılık hizmetlerine ilişkin şartlar, güvenlik riskleri ve bu risklerden korunmak için alınması gereken önlemler konusunda bilgilendirme amacıyla hazırlanan işbu doküman siz müşterilerimizin dikkatine sunulmuştur.

Bankamız Ticaret Ünvanı: Türkiye Finans Katılım Bankası Anonim Şirketi

Genel Müdürlük Adresi: Saray Mahallesi Sokullu Caddesi No:6 Ümraniye/İstanbul

Mersis No: 0068006387095226

Bankacılık Düzenleme ve Denetleme Kurumu (BDDK) İletişim Bilgileri:

Posta adresi: Büyükdere Cad. No: 106 Esentepe Şişli/İSTANBUL

Telefon: (212) 214 50 00

Çağrı Merkezi: 0850 222 23 35

Web Sitesi: www.bddk.gov.tr

1) GÜVENLİ DİJİTAL BANKACILIK

Bankacılık işlemlerinizi en kolay ve en hızlı biçimde gerçekleştirmeniz için farklı Dijital Bankacılık uygulamalarını kullanıyor ve işlemlerinizi güvenle gerçekleştirebilmeniz için teknolojinin bize sunduğu bütün olanaklardan yararlanıyoruz. Bununla birlikte Dijital Bankacılık uygulamaları üzerinden yapılan dolandırıcılık işlemlerinde farklı birçok yöntem kullanılmaktadır. Şüphe duyduğunuz bir durumla karşı karşıya kalırsanız veya şifrelerinizin, kişisel bilgilerinizin üçüncü şahıslarca öğrenildiğini düşünüyorsanız vakit kaybetmeden 0850 222 22 44 numaralı telefondan Müşteri İletişim Merkezimiz ile görüşmenizi rica ederiz.

Dijital bankacılık kanallarımız üzerinden Hesap İşlemleri, Kredi Kartı İşlemleri, Para Transferi İşlemleri, Yatırım İşlemleri, Ödeme İşlemleri (Fatura, Vergi, vb.), Finansman İşlemleri bu işlemlere özelinde geçerli olan kısıtlamalar hariç 7/24 gerçekleştirilebilmektedir. İşlemlerin limit ve saatlerine ait tüm detaylara www.turkiyefinans.com.tr web sitemizin Dijital Bankacılık menüsünden ulaşabilirsiniz.

Aşağıdaki bilgilendirmeleri okuyarak nelere dikkat etmeniz ve nasıl önlemler almanız gerektiğini öğrenebilirsiniz.

Telefon Dolandırıcılarına İnanmayın!

- Telefon dolandırıcıları polis, savcı, avukat ya da bankacı arıyor izlenimi oluştururlar.
- Arka planda sizi inandıracak ve endişelendirecek telsiz, telefon gibi ortam seslerini kullanırlar.
- Amaçları kişisel ya da finansal bilgilerinizi paylaşmanızı sağlamaktır.

Sosyal Medya Dolandırıcılarına Çok Dikkat Edin!

- Sosyal medya dolandırıcıları Facebook, YouTube, Twitter, WhatsApp, Messenger gibi çeşitli sosyal ağlar aracılığıyla size ulaşmaya çalışırlar.

- Akrabalarınızın, arkadaşlarınızın ya da sizin adınıza kopya hesaplar oluşturarak ve yakınlık durumunuzdan yararlanarak farklı senaryolarla para talebinde bulunurlar.
- Bu senaryolar genellikle kaza, hastane masrafları ve benzeri acil durum mesajları içerir.

E-Posta, SMS ve Sosyal Medya Dolandırıcılarına İnanmayın!

- Oltalama adını verdiğimiz bu yöntemde dolandırıcılar sosyal medya, e- posta ve kısa mesajlar aracılığı ile bankaların unvanlarını ve logolarını kullanarak sahte kampanya ve reklam linklerine tıklamanız için çalışırlar.
- "İnternet Bankacılık Süreniz Dolmuştur", "Bilgilerinizi Güncellemeniz İstenmektedir", "Hesaplarınızda Şüpheli İşlemler Tespit Edilmiştir", "Araba Çekilişine Katılmak İçin Tıklayın", "Kart Aidatınızı Geri Almak İçin Tıklayın" gibi mesajlar ve yönlendirmeler kullanırlar.
- Bu linklere tıklamanız durumunda sizi sahte banka hesaplarına yönlendirebilir, güvenliğiniz açısından kritik bilgileri paylaşmanıza neden olabilirler.

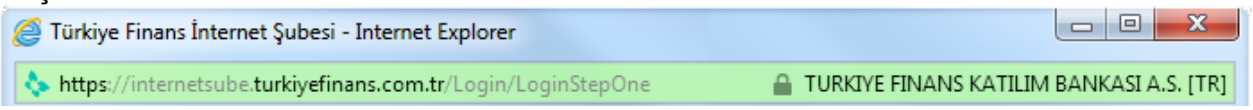
İnternet ve Mobil Cihaz Dolandırıcılarına Karşı Önlem Alın!

- Virüsleri, kötü amaçlı yazılımları ve truva atı ve buna benzer zararlı programları bilgisayar ya da cep telefonunuza bulaştırma yöntemiyle çalışırlar.
- Bu zararlı yazılımları cihazınıza yüklemek için bankadan, resmi ve özel kurumlardan gönderiliyor izlenimi veren, ekinde dosya (.vbs, .bat, .exe, .scr, .jar, .xls, .doc, .js uzantılı) ve link içeren e-postalar, SMS mesajları, hatta WhatsApp mesajları gönderebilirler.
- Mobil cihazınızda Türkiye Finans Mobil Şube'den geldiği izlenimi veren bildirim görüntüleri paylaşabilirler.

2) GÜVENLİĞİNİZ İÇİN YAPMANIZ GEREKENLER

- İnternet Şube'mize www.turkiyefinans.com.tr adresindeki alana tıklayarak giriş yapınız. Tarayıcınızın adres satırında https://internetsube.turkiyefinans.com.tr yazdığını ve güvenlik sertifikası bulunduğunu kontrol ediniz. Başka bir yönlendirme ile ulaştığınız web sayfalarını lütfen kullanmayın.
- Mobil cihazınıza uygulama indirirken her zaman resmi uygulama mağazalarını kullanın. Resmi uygulama marketleri kötü amaçlı yazılımları uzak tutmak için gelişmiş güvenlik mekanizmaları kullanırlar. Bu nedenle Google Play, AppStore, Windows Store dışındaki ortamlardan uygulama indirmeyin.
- Türkiye Finans İnternet Şubesine girişte kullandığınız şifre, parola, kullanıcı kodu vb. bilgilerinizi, klavye ve ekran hareketlerinizi takip eden zararlı yazılımlara karşı koruyacak Anadolu Hisarı uygulamasını İnternet Şubesi Giriş ekranını açtığınızda sol alt köşede yer alan "Anadou Hisarı Yükle"ye tıklayarak bilgisayarınıza yükleyiniz.
- E-postaları açmadan önce içeriğinin güvenilirliğini kontrol etmeyi ihmal etmeyin. Tanımadığınız kişilerden gelen (özellikle ilişiğinde dosya bulunan) e-postaları açmayın ve bankanızdan gelmiş gibi görünüp, size kullanıcı kodu /parola/kredi kartı ya da banka kartı numarası soran ya da kişisel bilgilerinizi güncellemenizi isteyen e-postaları asla dikkate almayın.
- İnternette girdiğiniz sitelere, tıkladığınız linklere ve indirdiğiniz dosyalara dikkat etmeyi alışkanlık haline getirmelisiniz.
- Anti-virüs programları, bilgisayarınızı bilinen virüslerden korur. Bilgisayarınıza anti-virüs programı yüklemeniz güvenliğinizi artıracaktır. Sürekli yeni virüslerin piyasaya çıkması ve anti-virüs programının bu virüsleri tanımama ihtimaline karşı anti-virüs programını düzenli olarak güncellemenizi öneririz.

- Bilgisayarınızda orijinal yazılım kullanın. Kopya yazılımlar, bilgisayarınıza virüs bulaşma ihtimalini yükseltmektedir.
- İşletim sisteminizin güncellemelerini yapmayı ihmal etmeyin. İşletim sistemleri de düzenli olarak (sonradan keşfedilen güvenlik boşluklarını gidermek için) güncellenmesi gerekir. Lütfen bu güncellenmeleri düzenli olarak yapmaya özen gösteriniz.
- Şifrenizi gizli tutunuz, bankamız çalışanları dahil hiç kimseye söylemeyiniz ve herhangi bir yere yazmayınız. Türkiye Finans personeli hiçbir zaman sizden İnternet Şubesi şifrenizi, parolanızı sözlü, yazılı, telefon, mektup ya da e-mail aracılığı ile bildirmenizi talep etmemektedir.
- Unutmayın, Türkiye Finans personeli hiçbir zaman sizden internet şubesi şifrenizi, parolanızı sözlü, yazılı, telefon, mektup ya da e-mail aracılığı ile bildirmenizi talep etmemektedir.
- İnternet şubesinden çıkmak için mutlaka "Çıkış" butonunu kullanın. "Çıkış" butonu; oturumunuzun ve internet şubesi işlem penceresinin güvenli bir şekilde kapatılmasını sağlayacaktır.
- İnternet Şubesi açıkken bilgisayarınızın başından kısa süreli bile olsa ayrılmayınız, eğer ayrılacaksanız da şifreli ekran koruyucusunu kullanınız.
- Bilgisayarınıza güvenlik duvarı kurmalı ve aktif olup olmadığını kontrol etmelisiniz. Güvenlik duvarı, gelen ve giden ağ trafiğini kontrol ederek bilgisayarınıza ya da bilgisayar ağınıza yetkisiz veya istemediğiniz kişilerin çeşitli yollardan erişim sağlamasını engellemeye yarayan yazılım veya donanımdır.
- İnternet Şubemizde, işlemlerinizde en yüksek güvenliğin sağlandığı 256-bit SSL şifreleme kullanılır. SSL, gönderilen bilginin sadece doğru adreste deşifre edilebilmesini sağlar. Kullandığınız web tarayıcısı bu özelliği destekliyorsa İnternet Şubemize girişinizde tarayıcınızın adres satırı yeşil renkte görünecek ve turkiyefinans.com.tr' nin güvenilir bir site olduğuna ilişkin sertifika detaylarına adres satırına tıklayarak ulaşabileceksiniz.



Eğer sitenin dolandırıcılık amaçlı sahte bir site olduğu önceden tespit edilmişse, adres satırı kırmızı renge dönüşecektir. Kırmızı adres çubuğu ile karşılaşıldığında site üzerinde hiçbir işlem yapılmamalı ve 0850 222 22 44 numaralı Müşteri İletişim Merkezimize haber verilmelidir. Bazı tarayıcılar ise bu sertifikayı tanır ancak SSL sertifikalarının sunmakta olduğu özelliklerden faydalanamayarak tarayıcıların adres satırını yeşil renge çeviremezler. Bu durum, bu tarayıcıları kullanmanın güvensiz olduğunu göstermemekte olup sahte siteleri gerçek sitelerden ayırt etmeye yarayan uyarıları desteklemediğinin bir göstergesidir.

VeriSign Extended Validation (EV) SSL sertifika uygulamamızı kullanabilmeniz için öncelikle, bu özelliği destekleyen güncel bir web tarayıcıyı bilgisayarınızda kurulu olmalıdır. Sorunsuz işlem yapabilmek için tarayıcınızın en kısa sürede yazılımcı firmaların resmi sitelerinden ücretsiz olarak güncellenmesi faydalı olacaktır.

İnternet ve Ağ Güvenliği

- İnternet Şubesi'ne girişlerinizde parola sayfasındaki kilit () sembolünün üzerine bir kez tıkladığınızda "Verisign has identified this site as: TURKIYEFINANS KATILIM BANKASI A.S." ibaresinin bulunup bulunmadığını kontrol ediniz. Güvenlik sertifikasındaki isim alanını kontrol ederek, güvenlik sertifikasının gerçekten Türkiye Finans'a ait olup olmadığını kontrol ediniz.
- Arama motorlarını kullanarak gelen linklerden İnternet Şubesi'ne girmeyiniz.

- Hem internette hem de gerçek hayatta özel bilgilerinizi gizli tutunuz.
- Kullanılmadığı zamanlarda kablosuz modemleri kapalı tutunuz.
- Modem yönetim paneli için güçlü ve kendinize özgün bir parola kullanmanız güvenliğinizi artıracaktır.
- Modeme kablosuz bağlantı parolasını koymayı unutmayınız.
- Bilgisayar ile ADSL modem arasındaki iletişimin şifrelenmesini (WPA / WPA2) aktif hale getiriniz.
- Evinizde ya da ofisinizde kablosuz ağınıza sizin isteğiniz dışında aygıtların bağlanmasını engellemek için, kendi bilgisayarınızın adresini modeme tanıtarak MAC adres filtresini açabilirsiniz. Bu durumda sizin bilgisayarınız dışındaki bilgisayarların modeminize wireless üzerinden bağlanması engellenmiş olacaktır.

3) GÜVENLİK UYGULAMALARIMIZ

İnternet / Mobil şubeye girdiğinizde son başarılı ve başarısız giriş tarihleriniz gösterilir, bu bilgilerin doğruluğunu kontrol etmeyi unutmayın. Ayrıca, İnternet şubemizde Profil>Güvenlik Ayarları menüsünden aşağıdaki güvenlik uygulamalarımızı kullanarak dijital güvenliğinizi en üst düzeye çıkarabilirsiniz.

3.1) Giriş/İşlem Güvenliği

İnternet/Mobil şube giriş/işlem güvenliği için aşağıda uygulamalardan birini kullanabilirsiniz.

3.1.1) Cep Onay

Cep Onay; Türkiye Finans İnternet Şubesi, Mobil Şube ve TFXTARGET platformlarına sadece parolanızı kullanarak, SMS Şifre girmenize gerek kalmadan hızlı giriş yapmanızı sağlayan güvenlik uygulamasıdır. Cep Onay'a geçiş yapmak için iOS veya Android işletim sistemine sahip cep telefonu veya tabletinize yukle.turkiyefinans.com.tr adresinden Türkiye Finans Mobil Şube uygulamasını yüklemelisiniz ve Mobil Şube'ye giriş yaptığınızda Cep Onay özelliği aktif hale gelecektir.

Cep Onay Kullanarak Nasıl Giriş Yaparım?

Mobil Şube ve TFXTARGET Uygulamaları İçin;

Cep telefonunuzda bulunan Türkiye Finans Mobil uygulaması güncellendikten sonra Mobil Şube için Cep Onay giriş yönteminiz aktif hale gelecektir. Mobil Şube girişinizi tek kullanımlık şifre girmenize gerek kalmadan sadece parolanızı kullanarak doğrudan yapabilirsiniz.

İnternet Şubesi ve TFXTARGET Uygulamaları İçin;

Türkiye Finans İnternet Şubesi ve TFXTARGET girişlerinizde ise müşteri numaranızı ve parolanızı girdikten sonra sadece tanımlı mobil cihazınıza gelecek olan mobil bildirimi onaylayarak güvenli bir şekilde giriş yapabilirsiniz.

3.1.2) SMS Şifre

- SMS Şifre İnternet Bankacılığında müşteri bilgilerinin güvenliğini sağlamaya yönelik olarak geliştirilmiş, süreli ve tek kullanımlık şifre üreten ileri düzey güvenlik sistemidir.

- SMS Şifre, mevcut güvenlik yapısına ek olarak geliştirilen ve cep telefonunuza gönderilen tek kullanımlık şifre ile en üst güvenlik seviyesinde internet/mobil bankacılığı kullanımınızı sağlayan bir güvenlik uygulamasıdır. SMS'le cep telefonunuza gönderilen altı haneli SMS Şifre tek kullanımlık ve sürelidir. İkinci bir kez daha siz ya da bir başkası tarafından kullanılamaz.

3.1.3) Anahtar Şifre

- Fiziki token cihazı üzerinden tek kullanımlık şifre oluşturulmasını sağlayan uygulamadır.

3.1.4) Mobil İmza

- Mobil İmza, elektronik ortamda kimliğinizi doğrulayarak ıslak imza ile eşdeğer işlem yapabilmenize olanak sağlayan bir hizmettir. Mobil İmza, 5070 sayılı Elektronik İmza Kanunu'nda tarif edilen ve ıslak imza ile aynı sonucu doğuran Elektronik İmza' nın GSM SİM kartları kullanılarak atılmasını sağlayan bir uygulamadır.

    - İnternet Şubesi'ne girmek istediğinizde Mobil İmza uygulaması sayesinde, sisteme daha önce tanımladığınız numaranın kullanıldığı cep telefonunun ekranına bir mesaj gönderilir. SMS olarak gönderilmediği için güvenlik sorunu olmayan bu mesajda, İnternet Şubesi'ne girmek için onayınız istenir. Gelen mesaja onay vermeniz halinde İnternet Şubesi'ne giriş yapılabilir. Mobil İmza uygulaması ile telefonunuz aracılığıyla onay vermediğiniz sürece hesabınıza ulaşım engellenmiş olur.

3.2) Özel Soru Uygulaması

- Türkiye Finans İnternet Şubesi'ne giriş için gerekli olan şifre ve parolanıza ek olarak Özel Soru uygulamasını aktif hale getirebilir ve güvenliğinizi artırabilirsiniz. Uygulama; İnternet Şubesi giriş ekranında şifre ve parolanızın yanı sıra yanıtını sadece sizin bilebileceğiniz sorularla kimliğinizi onaylar.

3.3) Erişim Güvenliği Uygulamaları

3.3.1) Zaman Ayarları

İnternet Şubesini kullanmak istediğiniz zaman periyotlarını tanımlayarak, sadece belirlediğiniz zamanlarda İnternet Şubesine girişinizin aktif olmasını sağlayabilirsiniz.

3.3.2) IP Sınırlama

İnternet Şubesini kullanacağınız IP numaralarını/aralığını tanımlayarak diğer IP'lerden girişlere kapatabilirsiniz.

3.3.3) Tatil Ayarları

Tatil başlangıç ve tatil bitiş zamanlarınızı girerek; tanımlı süre içinde İnternet Şubenizi kapatabilirsiniz. Tatil sürenizin sonunda İnternet Şubeniz otomatik olarak kullanımınıza açılacaktır.

3.3.4) Bilgisayar Tanımlama

İnternet Şubesini kullanacağınız bilgisayar/bilgisayarları tanımlayarak, farklı bir bilgisayardan İnternet Şubesinize girilmesini engelleyebilir, yüksek güvenlik sağlayabilirsiniz. Bilgisayar Tanımlama'nın kullanılabilmesi için Anadolu Hisarı' nın seçilmek istenen bilgisayarlarda yüklü olması gerekmektedir.

İnternet Şubesinde "Güvenlik Ayarları / Bilgisayar Tanımlama" adımından istediğiniz bilgisayar veya bilgisayarları seçerek işleminizi yapabilirsiniz. Anadolu Hisarı programını Türkiye Finans İnternet Şubesi giriş ekranından indirebilirsiniz.

3.4) Güvenlik Resmi Seçimi

İnternet şubemize giriş yaptığınızda daha önce seçmiş olduğunuz “güvenlik resmi” gösterilir, güvenlik resminizin doğruluğunu kontrol edin farklı bir güvenlik resmi görürseniz kesinlikle giriş yapmayın.

4) Diğer Güvenlik Uygulamaları

Hesap Sınırlama

İnternet Şubesinde kullanmak istemediğiniz veya sadece görüntüleme amacıyla kullanmak istediğiniz hesaplarınızı belirleyerek güvenliğinizi daha da artırabilirsiniz.

Sanal Klavye

Parolanız ile birlikte kullanacağınız şifrenizi sanal klavye ile girmeniz güvenliğinizi daha da artıracaktır.

4) ATM BANKACILIĞI

İşlemlerin limit ve saatlerine ait tüm detaylara www.turkiyefinans.com.tr web sitemizin Dijital Bankacılık menüsünden ulaşabilirsiniz.

4.1) ATM Kullanımında Kendi Güvenliğiniz İçin Dikkat Etmeniz Gereken Noktalar

- Şifrenizi belirlerken, başkaları tarafından kolayca tahmin edilebilecek olan, telefon numaranız, doğum tarihiniz vb. gibi kişisel bilgilerinizi içermemesine, aynı veya ardışık rakamlar (2222, 4567 vb.) olmamasına özen gösteriniz.
- Şifrenizi başkalarının görmesine izin vermeyiniz, kimseye söylemeyiniz.
- ATM'de işlem yaparken kart şifrenizi başkalarının göremeyeceği şekilde, tuş panelini diğer elinizle kapayarak girin.
- Şifrenizi kartınızın üzerine veya başka bir kağıda yazıp, üzerinizde saklamayınız. Şifrenizin sorumluluğunun sadece size (kart sahibine) ait olduğunu unutmayınız.

- İşlem yaptığınız ATM'de şüpheli bir durumla karşılaştığınızda (özel olarak yerleştirilmiş bir cihaz vs.) işlem yapmayarak derhal 0850 222 22 44 numaralı telefondan Müşteri Hizmetleri' ni arayınız ya da Şubenize başvurunuz. Bu bildirimlerde tanımadığınız kişilere ait telefonları kullanmayınız.
- İşlem yaparken tanımadığınız kişilerden kesinlikle yardım almayınız, yardım tekliflerini geri çeviriniz.
- Kartınızın ATM'de sıkışması, alıkonulması gibi durumlarda size yardımcı olmak isteyen kişilere dikkat edin. Kötü niyetli kişiler, ATM'de kartınız sıkıştığında ATM'ye tekrar şifrenizi girmeniz halinde kartınızın iptal edileceğini belirtebilir ve hatta kendi cep telefonları ile bankanızı aramanıza yardımcı olmayı teklif ederek kart şifrenizi elde edebilirler. Bu tür durumlarda, tanımadığınız kişilerden yardım almayın. Varsa kendi cep telefonunuzla veya en yakındaki güvenli bir telefonla bankanıza derhal haber verin.
- Şifrenizi bankanızın bile -ne sebeple olursa olsun- bilmesine gerek olmadığını unutmayınız

Şifrenizin başkası tarafından öğrenilmesi, kartınızın kaybolması/çalınması veya olağan dışı bir durumdan şüphelenirseniz işleminizi bitirdikten sonra zaman geçirmeden 365 gün 24 saat hizmetinizde olan 0850 222 22 44 numaralı telefondan Müşteri Hizmetleri' ni arayınız ya da Şubenize başvurunuz. Bu bildirimlerde tanımadığınız kişilere ait telefonları kullanmayınız.

5) MÜŞTERİ İLETİŞİM MERKEZİ

0850 222 22 44 numaralı Müşteri İletişim Merkezimiz kanalı ile 7 gün 24 saat, istediğiniz yerden, sadece bir telefon aracılığı ile tüm bankacılık işlemlerinizi gerçekleştirebilirsiniz.

Müşteri İletişim Merkezimiz Türkçe, Arapça ve İngilizce olmak üzere 3 farklı dil desteği ile tüm müşterilerimize hizmet vermektedir. Türkçe hizmetimizden 7/24, Arapça ve İngilizce hizmetlerimizden ise 08:30-17:30 (Mesai saatleri içinde) saatleri arasına yararlanabilirsiniz.

Güvenlik Akışlarımız

1- Sesli Yanıtlama Sisteminde, biyometrik ses tanıma teknolojimiz Ses İmzası ile çok daha hızlı ve güvenli hizmet alabilirsiniz.
2- Müşteri İletişim Merkezi kanalımızdan hizmet alırken;
   a. Finansal olmayan veya Finansal Risk içermeyen işlemlerinizde, Kayıtlı cep telefonunuzdan aramanız durumunda “Kart Şifresi” , "Dijital Şifre" veya “Sesli İmza” güvenlik doğrulamalarından herhangi birini gerçekleştirmeniz yeterli olacaktır.
   b. Finansal olan veya Finansal Risk içeren işlemlerinizde;
      i. Mobil Şube kullanıcısı iseniz, "Dijital Şifre" veya “Sesli İmza” güvenlik doğrulamasından sonra bankamızda kayıtlı cep telefonunuza gönderilecek olan “Mobil Onay” bildirimini sesli yanıtlama sisteminde onaylamanız,
      ii. Mobil Şube kullanıcısı değilseniz, "Dijital Şifre" veya “Sesli İmza” güvenlik doğrulamasından sonra cep telefonunuza SMS ile gönderilecek olan işlem onay şifrenizi sesli yanıtlama sisteminde tuşlamanız gerekmektedir.
3- Kayıp, çalıntı ve şüpheli işlem durumlarında Müşteri İletişim Merkezi’ne güvenlik doğrulama adımları uygunmadan hızlıca bağlanabilirsiniz.
4- Kullanmış olduğunuz şubesiz bankacılık ve kredi kartı şifreleri size özeldir. Başkaları ile paylaşılmaması gerekmektedir.
5- Hizmet almak için aradığınızda, müşteri numaranızı / kredi kartı numaranızı ve şifrenizi, telefonunuzun tuşlarını kullanarak girmeniz istenecektir. Böylece şifrenizi sizden başka herhangi birinin duyma şansı olmayacaktır.

6- Güvenlik adımlarında Bankamızda kayıtlı bilgilerinizin doğrulaması yapılmaktadır. Bu nedenle bilgilerinizin güncel olması önemlidir.

7- Güvenliğiniz, yapmak istediğiniz işlem türüne göre belirlenmiş farklı güvenlik adımları ile sağlanmaktadır.

8- Müşteri temsilcisi ile yapılan görüşmeler güvenlik nedeniyle kayıt altına alınmaktadır.

9- Müşteri İletişim Merkezi'ni aradığınızda ya da sizi aradığımız da şifrenizi sesli olarak paylaşmanız istenmez.

10- Şifrelerinizin veya kişisel verilerinizin 3. şahısların eline geçmesi halinde zaman kaybetmeden Müşteri İletişim Merkezi'ni arayarak gerekli güvenlik önlemlerinin alınabilmesi için bildirimde bulunulmalıdır.

6) SORUMLULUKLARINIZ

Bankamız adına aradığını ileterek sizden kimlik bilgilerinizi, şifrenizi, tek kullanımlık işlem şifrenizi isteyen kişilerle bilgilerinizi paylaşmayınız. Güvenliğinizle ilgili konularda sorularınız ve tereddüt ettiğiniz hususlar için Bankamızla iletişime geçebilirsiniz.

Güvenliğiniz için dikkat etmeniz gerekenler:

- Şifrenizi Bankamız çalışanları dâhil hiç kimseyle paylaşmayınız.
- Şifrelerinizi sizi tanıyanların kolayca tahmin edebileceği rakamlardan oluşturmayınız.
- Şifrelerinizi herhangi bir yere yazmayınız. Telefonunuza, bilgisayara vs başkalarının ulaşabileceği alanlara kayıt etmeyiniz.
- Şifrenizi kartınızın üzerine veya herhangi bir yere yazmayınız. Cüzdanınızda bulundurmayınız.
- Şifreniz ile ilgili her türlü soru ve sorunlarınız için 0850 222 22 44 numaralı telefondan Müşteri İletişim Merkezimiz ile görüşmenizi rica ederiz.
- Kayıp, çalıntı ve şüpheli işlem durumlarında Çağrı Merkezimizi arayarak (0 tuşlayarak) hızlıca bildirimde bulunabilirsiniz.

Dolandırıcılık aramaları kendilerini avukat, polis, savcı, bankacı olarak tanıtan veya sosyal medya/e-posta üzerinden arkadaşınız ya da ticaret yaptığınız şirket gibi davranan dolandırıcılar olabilir. Bu kişilerin amacı size ait internet/mobil bankacılık şifrelerinizi, kimlik bilgilerinizi ya da erişim bilgilerinizi ele geçirerek dolandırıcılık faaliyetleri yürütmektir.

Şifre ve bilgi güvenliğiniz için Bankamız tarafından hiçbir koşul ve durumda müşterilerimizden sözlü veya yazılı olarak bu bilgiler talep edilmemektedir. Dolayısıyla, sizi arayan ve bilgilerinizi paylaşmanızı isteyen kişilere cevap vermemenizi önemle rica ederiz.

Çağrı Merkezi Telefonlarımız

Türkiye'nin ve Kuzey Kıbrıs Türk Cumhuriyeti'nin her yerinden sabit hatlardan ve tüm cep telefonu operatörlerinden alan kodu eklemeden 0850 222 22 44 numaralı telefondan Müşteri İletişim Merkezimizi arayabilirsiniz.

Müşteri İletişim Merkezimizi yurtdışından sabit veya cep telefonlarınızdan +90 0850 222 22 44 numarasından ulaşabilirsiniz.