Elektronik Bankacılık Hizmetlerinin Kullanımına İlişkin Riskler ve Korunma Yöntemlerine Dair Bilgilendirme

Fibabanka

KASIM 2020

Fibabanka Dijital Güvenlik Bölümü

Suistimal Nedir?

Suistimal; hileli davranışlarla bir kimseyi aldatıp, onun veya başkasının zararına olarak, kendisine veya başkasına bir yarar sağlayan kişinin yaptığı eylemdir. Teknolojinin gelişmesi ve tüm dünyada kullanımının artması ile dijital dolandırıcılık faaliyetlerinde de artış gözlemlenmektedir.

Fibabanka olarak, kullanmış olduğunuz elektronik bankacılık hizmetlerinde karşılaşabileceğiniz dijital dolandırıcılık faaliyetleri konusunda mağduriyet yaşamamanız için, yaygın olarak kullanılan suistimal yöntemleri, riskleri, korunma yöntemleri, hak ve sorumluluklarınız hakkında sizleri bilgilendirmek isteriz.

Mobil ve İnternet Bankacılığı Hizmetleri Nelerdir?

Bankamız tarafından Mobil ve İnternet Bankacılığı kanallarımız üzerinden 7/24 finansal olmayan işlemler, kendi hesaplarınız arasındaki işlemler, döviz ve yatırım işlemleri ile banka içindeki diğer hesaplara yönelik havale işlemleri yapılabilmektedir. EFT ve SWIFT hizmetleri ise hafta sonu ve mesai dışı kapalı olduğu için 7/24 hizmet verilememektedir. Ancak Nöbetçi Transfer hizmetimiz ile hafta içi mesai saatleri dışında ve hafta sonu dahil olmak üzere Mobil ve İnternet Bankacılığı kanallarımız üzerinden sisteme dahil bankalar arasında para transferi işlemi yapılabilmektedir.

Mobil ve İnternet Bankacılığı kanallarımızdaki hizmetlerimizden yararlanmak isteyen müşterilerimiz; şubelerimiz, www.fibabanka.com.tr veya Fibabanka Mobil Bankacılık uygulamamız üzerinden Fibabanka İnternet Bankacılığı ve Fibabanka Mobil Bankacılığını aktive edebilirler. Kanal aktivasyonu mevzuata uygun olarak müşterinin bildiği, sahip olduğu unsurdan en az 2 bileşenin doğrulaması ile yapılmaktadır. Bu süreçler tamamlanmadan bu kanallarımızdaki hizmetlerimizden yararlanılması mümkün değildir.

Mobil ve İnternet Bankacılığı Dolandırıcılık Yöntemleri

Sosyal Mühendislik

Sosyal mühendislik dolandırıcılığı yöntemi; dolandırıcıların, müşteriye ait kimlik, kart, elektronik bankacılık, telefon, tablet, bilgisayar şifreleri gibi bilgileri haksız kazanç elde etmek amacıyla ele geçirme yöntemidir. Suçlular, bu özel bilgileri elde etmek için kişiyle telefon, e-posta, sosyal ağlar hatta yüz yüze görüşerek güven suistimali yaparlar. Amaç, sahte bir senaryo / hikâye uydurarak bu senaryonun içine serpiştirilmiş tuzaklarla müşteriden istenilen bilgiyi almaktır.

Sosyal mühendislikte;

- Kişiyi hediye kazandığına ikna etme;
- Korkutma;
- Emniyet, asker, hâkim, savcı gibi resmi bir kuruma mensup olduğuna inandırma;
- Sosyal medya hesabı ele geçirilen bir yakın gibi davranma;
- Bir terör örgütünün hesaplarınızı ele geçirmiş olduğunu söyleyerek yardım isteme ya da sizi koruduğuna ikna etme

gibi yöntemler kullanılarak, Mobil ve İnternet Bankacılığı kanallarına ilişkin gerekli bilgi ve şifreleri ile kişisel veya finansal bilgilerini ele geçirerek finansal varlıklarınızı dolandırma işlemi gerçekleştirebilirler.

Nasıl korunursunuz?

- "Hediye & ödül kazandınız, kredi notunu düzeltme, yapılan masrafların iade alınması" gibi vaatler sonrası sizden para ya da yukarıda ifade olunan kişisel bilgilerinizin talep edilmesi halinde bu tür bildirimlere itibar etmeyiniz.
- Telefonla arayarak kendilerini kamu personeli (polis, asker, savcı, hâkim vb.) olarak tanıtan kişiler sizden para, altın veya kişisel bilgilerinizi, şifrelerinizi talep ediyor ise itibar etmeyiniz.
- Sosyal medya üzerinden yapılan taleplerde, kişisel bilgilerinizi paylaşmayınız.
- Banka personeli dâhil hiç kimseyle şifre bilgilerinizi paylaşmayınız.

Önemli Bilgilendirme: Hiçbir kamu kurumu ya da banka, e-posta ya da telefon veya benzeri bir iletişim kanalı ile sizleri arayarak kart bilgi ve şifrelerinizi, İnternet ya da Mobil Bankacılık şifreniz ile size ait kişisel bilgileri talep etmez.

Oltalama (Phishing)

Oltalama (phishing) saldırıları, çeşitli banka ve finans kuruluşu veya farklı bir güvenli kuruma aitmiş gibi görünen, acil veya çok önemliymiş izlenimi verebilen, amacı hassas bilgilerinizi (kart ve elektronik bankacılık şifreleri, SMS şifresi, kart bilgileri, kimlik bilgileri gibi) ele geçirmek olan saldırılardır. Bu yöntemde gönderilen e-postalar veya SMS'ler ile hassas bilgileri ele geçirmek için kullandığınız bilgisayara veya mobil cihaza uygulama kurulması istenebilmekte veya sahte bir siteye yönlendirme yapılabilmektedir.

Oltalama (Phishing) vakalarında aşağıdaki kanallar kullanılabilir:

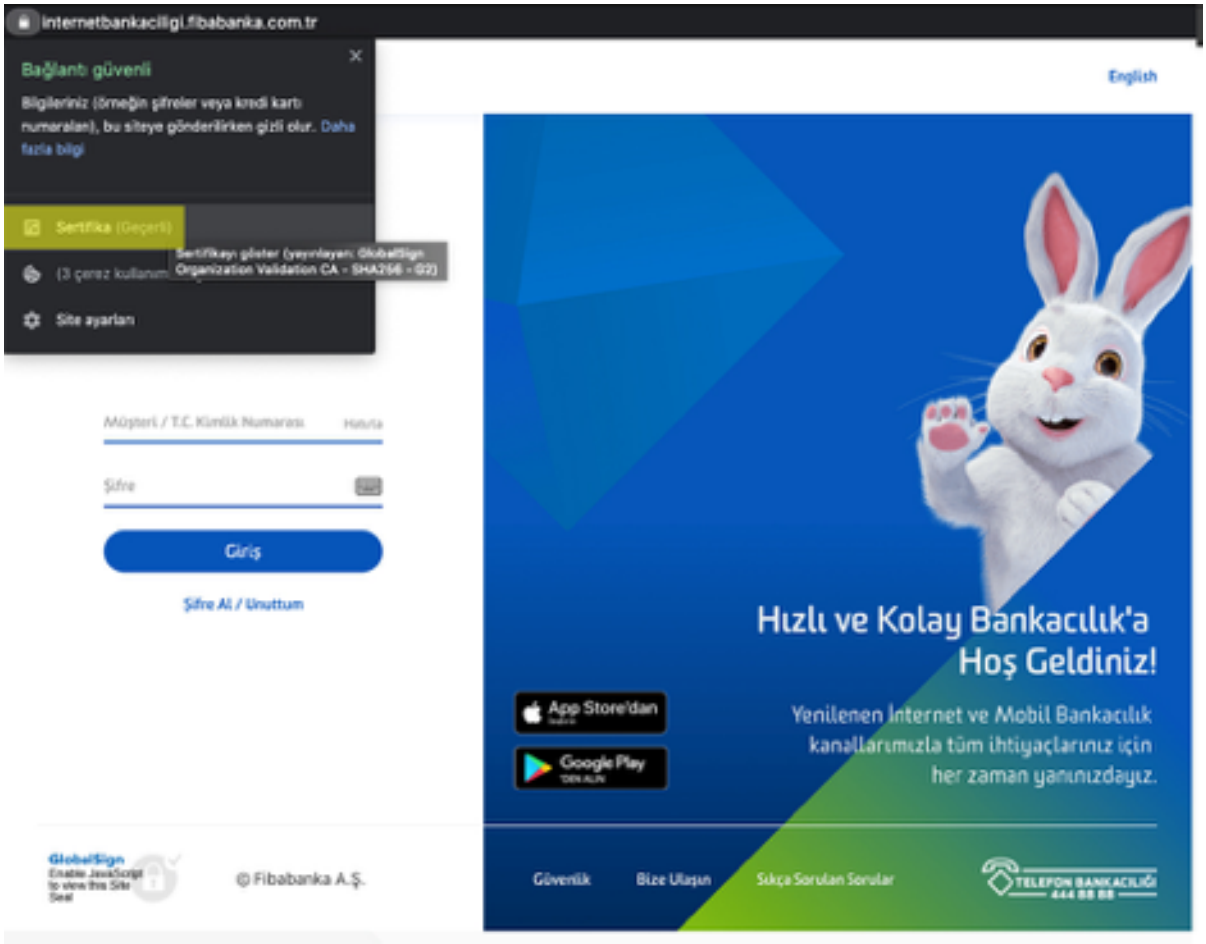
- SMS
- E-posta
- Web Sitesi
- Mobil Uygulama

Amaç hepsinde ortaktır: Finansal fayda sağlamak veya kişisel verilerinizi elde etmek.

- Sahte e-postalarda gönderici adı, taklit edilen gönderici adına yakın bir ada sahiptir.
- Çok sayıda kullanıcıya hitap eden bir ifadeyle başlayabilirler (Örneğin "Sayın Kullanıcı" gibi).
- Yazım hataları içerebilirler.Aciliyet ya da önemli hissiyatı uyandırma amacında olabilirler.

Nasıl korunursunuz?

- Bankamız internet sitesine ulaşmak için arama motorları kullanılmamalıdır. Sahte web siteleri arama motorları ile ekrana çıkabilir. Bu yüzden internet adres çubuğuna fibabanka.com.tr yazarak erişim sağlanmalıdır.
- Güncel bir anti-virüs yazılımı kullanılmalıdır.
- Kullanılan cihazın güncellemelerinin yapıldığından emin olunmalıdır.
- Sadece göndericisinden emin olunan e-postalar açılmalıdır.
- Emin olunmayan adreslerden gelen e-posta ve SMSlere eklenmiş dokümanlar açılmamalıdır.
- Mobil ve İnternet Bankacılığı kanallarımızın kullanımı için belirlenmiş olan güvenlik resminin, belirtilen kanallara her girişte aynı olduğundan emin olunmalıdır.
- Özendirici reklam içeriği ile ortaya çıkan ve Fibabanka reklamı gibi gözüken reklamlarda bulunan linklere tıklanmamalı, elektronik bankacılık şifresi veya kişisel bilgilerin girilmesi talep edilen reklamlardan uzak durulmalıdır. Özellikle, açılan internet sayfasının geçerli bir SSL sertifikasına sahip olduğuna emin olunmalıdır.



Zararlı Yazılımlar

Bilgisayarlar, akıllı telefonlar veya mobil cihazlara farklı yollar ile zararlı yazılım bulaştırılabilir. Bu yöntemde amaç, cihazlardaki bilgilerin veya cihazın yönetiminin ele geçirilmesidir. Böylelikle kişisel veriler elde edilebilir ve finansal kazanç sağlanabilir.

Zararlı yazılımlar ile:

- Cihazınızda yaptığınız klavye ya da fare hareketleri takip edilebilir;
- Cihazınızdaki kişisel verilere ulaşılabilir;
- Cihazlarınıza uzaktan komuta edilebilir;
- Size gelen SMSler ya da aramalar başka numaraya yönlendirilebilir.

Nasıl korunursunuz?

- Güncel bir anti-virüs programı kullanılmalıdır.
- Güvenlik duvarı (firewall) uygulaması kullanılmalıdır.
- Lisanslı yazılımlar kullanılmalıdır.
- Özellikle tanımadığınız göndericilerden gelen eklentiler açılmamalıdır.
- Herhangi bir eklenti açılmadan önce virüs taramasından geçirilmelidir.
- Güvenliğinden emin olunmayan uygulamaların cihaza indirilmesinden kaçınılmalıdır. Resmi marketlerden (Google Play Store, App Gallery ve App Store) uygulama indirilmesine özen gösterilmelidir. Uygulamamızı https://www.fibabanka.com.tr/mobil-bankacilik linkinden Mobil Bankacılık sayfamıza ulaşıp, açılan sayfada yer alan QR kodunu telefonunuzdan okutarak ya da uygulama indirme butonlarına tıklayarak indirebilirsiniz.

Telefon Bankacılığı Hizmetleri Nedir?

Çağrı Merkezi kanalımız aracılığıyla 7/24 finansal olmayan işlemler, kredi, atm ve kredi kartı işlemleri, şifre işlemleri, bilgi güncelleme işlemleri, dijital kanal aktivasyon ve kapama işlemleri, kendi hesaplarınız arasındaki işlemler, döviz ve yatırım işlemleri ile banka içindeki diğer hesaplara havale işlemleri yapılabilmektedir. EFT hizmeti, mesai günlerinde ve mesai saatleri içinde, yapılabilmektedir.

Telefon Bankacılığı Dolandırıcılık Yöntemleri

Sahte Çağrı Merkezi Dolandırıcılığı

Sahte çağrı merkezi dolandırıcılığı, bankaların telefon bankacılığı numaralarına benzer numaralar ile arama yapılarak müşterilere ait bankacılık şifreleri, kimlik bilgileri ve tek kullanımlık işlem şifrelerinin ele geçirilmesi yöntemidir.

Nasıl korunursunuz?

- Fibabanka Telefon Bankacılığına sadece 444 88 88 ve 0850 222 77 77 numaralarından erişim sağlayabilirsiniz. Farklı numaralardan gelen aramalara itibar etmeyiniz.
- Başkalarının telefonu veya kamuya açık telefonlardan Fibabanka telefon bankacılığına ulaşmak istediğinizde numarayı kendiniz çeviriniz. Numaranın doğru çevrildiğinden emin olunuz.

ATM Bankacılığı Hizmetleri Nedir?

Fibabanka ATMlerinden 7 gün 24 saat para çekme, bakiye sorgulama, hesaplar arası havale, kart şifre değişikliği işlemleri gerçekleştirilebilir.

Fibabanka ATMlerinin yanı sıra Türkiye'deki tüm ATMlerden de günün 24 saati para çekme ve bakiye görüntüleme işlemleri gerçekleştirilebilir. İş Bankası Bankamatiklerinden dilendiği kadar, PTTMatik'lerden ise aylık 5 işleme kadar para çekme, dilendiği kadar para yatırma ve bakiye sorgulama işlemleri yapılabilir.

Maestro amblemi olan tüm yurt dışı ATMlerden, bulunduğunuz ülkenin para birimi cinsinden nakit çekim işlemi yapılabilir.

ATM Dolandırıcılık Yöntemleri

Kart Kopyalama

Kart kopyalama dolandırıcılığı, ATM kart giriş haznesine monte edilen düzenek vasıtasıyla ATMde kullanılan kartın manyetik şeridinde yer alan verilerin kopyalanması yöntemidir.

Kart kopyalama düzeneği takılan ATMlere klavyeyi görebilecek bir konumda gizli kamera da yerleştirilerek kartın şifresi ele geçirilmektedir.

Kopyalanan kart bilgileri manyetik şeride sahip başka bir karta aktarılarak gizli kamera ile ele geçirilen şifrelerle kullanılmaktadır.

Nasıl korunursunuz?

- İşlem yaptığınız ATMde olağan dışı bir durum olduğunu fark ederseniz 444 88 88 ve 0850 222 77 77 Fibabanka Telefon Bankacılığımızı arayarak bildirimde bulunabilirsiniz. Bankamız gerekli tedbirlerin alınmasını hızlıca sağlayacaktır.
- ATMde işlem yaparken kart şifrenizi kimsenin göremeyeceği şekilde ve tuş panelini diğer elinizle kapayarak giriniz.

Kart Sıkıştırma

Kart sıkıştırma dolandırıcılığı, ATM kart giriş haznesine yerleştirilen işlem yapılmak istenen kartın ATM tarafından okunması ya da geri verilmesini engelleyen düzeneklerin kullanılması ile kartın sıkıştırılması yöntemidir.

Kart kopyalama yönteminde olduğu gibi ATM klavyesini görebilecek gizli kamera ile kart şifresi ya da kartın ATMde sıkışması sonucu yardım etmek amacıyla yanınıza gelen kişilerin işlem esnasında klavyede tuşlanan şifrenin görülmesi ile kart şifresi ele geçirilmektedir.

Sıkıştırılan kart, kart hamili ATMden ayrıldıktan sonra dolandırıcılar tarafından alınarak şifre ile kullanılmaktadır.

Nasıl korunursunuz?

- ATMde işlem yaparken kimseden gelen yardım taleplerini kabul etmeyiniz.
- Eğer kartınız ATM tarafından alıkonuldu ise veya sıkıştı ise 444 88 88 ve 0850 222 77 77 Fibabanka Telefon Bankacılığımızı arayarak bildirimde bulunabilirsiniz. Bankamız gerekli tedbirlerin alınmasını hızlıca sağlayacaktır.
- ATMde işlem yaparken kart şifrenizin kimsenin göremeyeceği şekilde ve tuş panelini diğer elinizle kapayarak giriniz.

Para Sıkıştırma

Para sıkıştırma dolandırıcılığı, ATM para verme haznesinin kapağının önüne yerleştirilen düzenek ile ATM para verme haznesinin kapağı açılıp içerisindeki parayı dışarı ittiğinde yerleştirilen düzeneğe banknotların yapışması yöntemidir.

Müşteri ATM para verme haznesinde arıza olduğunu düşünüp ATMden ayrıldığında dolandırıcılar tarafından yerleştirilen düzeneğe yapışan banknotlar ele geçirilmektedir.

Nasıl korunursunuz?

- İşlem yaptığınız ATMde olağan dışı bir durum olduğunu fark ederseniz 444 88 88 ve 0850 222 77 77 Fibabanka Telefon Bankacılığımızı arayarak bildirimde bulunabilirsiniz. Bankamız gerekli tedbirlerin alınmasını hızlıca sağlayacaktır.
- Eğer para çekme işleminde kartınızı aldıktan sonra ATM para vermez ise 444 88 88 ve 0850 222 77 77 Fibabanka Telefon Bankacılığımızı arayarak bildirimde bulunabilirsiniz. Bankamız gerekli tedbirlerin alınmasını hızlıca sağlayacaktır.

Elektronik Bankacılık Hizmetlerinin Kullanım Riskleri

Mobil, İnternet, Telefon veya ATM Bankacılığı kanallarımız aracılığıyla, müşterilerimizin finansal hayatını kolaylaştıran çözümler sunarak banka şubesine uğramadan istedikleri finansal hizmeti bulundukları yerden yapmalarını ve maliyet avantajından faydalanmalarını sağlarız. Ancak bu kolaylaştırıcı çözümler, gerekli tedbirler alınmadığı durumlarda maalesef bünyesinde riskler de taşımaktadır. Bilinmelidir ki; dolandırıcılar, müşterilerimizin İnternet ve Mobil Bankacılık hizmetlerinin kullanımının yaratacağı zafiyeti tereddüt etmeden kendi menfaatleri için kullanacak kişilerdir. Bunun için kullanılan yöntemlere ve bu risklerden müşterilerimizin korunması için alınması gereken tedbirlere ayrıca aşağıda yer verilmiştir.

Mobil, İnternet, Telefon veya ATM kanallarımızın kullanımının taşıdığı riskleri aşağıdaki gibi özetleyebiliriz:

- Finansal zarar
- Zararın geriye döndürülmesi için gösterilecek çaba
- Müşteriye özgü bilgilerin geri dönülemez bir şekilde açığa çıkması
- Hukuki mücadele
- İtibar kaybı

Elektronik Mobil Bankacılık Önerilen Güvenlik Unsurları ve Banka Güvenlik Prensipleri

- Fibabanka Mobil ve İnternet Bankacılığı kanallarımız veya Telefon Bankacılığımız üzerinden erişim ve işlem onayları için kullandığınız müşteri numaranızı, şifrenizi, doğrulama kodlarını kimseyle paylaşmayınız.
- Kredi kartı ve banka kart numaranızı, son kullanma tarihini ve kartınızın arkasında bulunan güvenlik kodunu (CVV2/CVC2) ve şifrelerinizi kimseyle paylaşmayınız. Cüzdanınızda veya mobil cihazlarınızda yazılı olarak saklamayınız.
- Şifrelerinizi düzenli olarak değiştiriniz.
- Fibabanka Mobil ve İnternet Bankacılığı kanallarımıza bağlı iken cihazınızı başkasına kullandırmayınız.
- İşleminizi tamamladıktan sonra 'Çıkış' seçeneğini tıklayarak oturumu sonlandırınız.
- Mobil ve İnternet Bankacılığı kanallarımıza girişlerinizde "Son Başarılı Giriş" ifadesi ile en son işlem yaptığınız tarih ve saati kontrol ederek, sizden başka üçüncü bir şahsın hesaplarınızı kullanıp kullanmadığını kontrol ediniz. İradeniz dışında bir erişim var ise Bankamızı bilgilendiriniz.
- Halka açık bilgisayarlardan bankacılık işlemleri yapmayınız. Halka açık bilgisayarlarda, hesap bilgilerinizi ve kişisel şifrelerinizi ele geçirmekte kullanılan çeşitli zararlı yazılımlar kullanılabilir.
- Bankamız internet sitesine ulaşmak için arama motorları kullanılmamalıdır. Sahte web siteleri arama motorları ile karşınıza çıkabilir. Bu yüzden internet adres çubuğuna https://www.fibabanka.com.tr/ yazarak erişim sağlayınız.
- Elektronik posta aracılığıyla veya başka bir ortamda sunulan web sayfalarını kullanmamaya özen gösteriniz. Farklı sayfalardan Fibabanka İnternet Bankacılığı'na yönlendirilme yoluyla giriş yapmayınız.
- Herhangi bir şüpheli durumla, sorunla ya da dolandırıcılık vakası ile karşılaşmanız halinde Bankamız şubelerine ziyaret ederek ya da 444 88 88 ve 0850 222 77 77 Fibabanka Telefon Bankacılığımızı arayarak bildirimde bulunabilirsiniz. Bankamız gerekli tedbirlerin alınmasını hızlıca sağlayacaktır.
- Herhangi bir dolandırıcılık vakası yaşamanız durumunda, size en yakın Cumhuriyet Başsavcılığı'na bildirimde bulununuz.
- Mobil veya İnternet Bankacılığı kanallarımız üzerinden yapmış olduğunuz her borçlandırıcı finansal işleminizde Bankamızda tanımlı olan cep telefonu numaranıza SMS gönderilerek işlem hakkında bilgi verilmektedir. Size ait olmadığını düşündüğünüz bir SMS bilgilendirmesinde şubelerimizi ziyaret ederek veya 7/24 hizmet veren 444 88 88 ve 0850 222 77 77 Fibabanka Telefon Bankacılığımızı arayarak bildirimde bulunabilirsiniz.
- İnternet Bankacılığı kanalımız üzerinden kendinize fazladan güvenlik yöntemleri tanımlayabilir ve gerektiğinde değişiklikler yapabilirsiniz. İnternet Bankacılığına giriş yaptıktan sonra "Güvenlik" menüsünden aşağıdaki güncelleme işlemlerinizi yapabilirsiniz:

  - Şifre Değiştirme
  - Yurt Dışı Erişim Kısıtlama
  - İşlem Yetki ve Limit Yönetimi: Fibabanka İnternet Bankacılığı'ndan yapacağınız işlemlerde, (örneğin başka hesaba havale, EFT ve SWIFT gibi) işlem limitinizi ve günlük limit tutarlarını Banka minimum tutarlarını düşürebilirsiniz. İşlem yapmak istemediğiniz işlem setleri için bu limiti en alt seviyeye çekmek suretiyle, söz konusu işlemin gerçekleştirilmesini engelleyebilirsiniz.
  - Bilgilendirme Mesajları: Bildirim listesinde belirtilen işlemler için, bankanın alt limitleri dahilinde, kayıtlı cep telefonunuza bilgilendirme SMS'i ve/veya kayıtlı e-posta adresinize bilgilendirme e-postası gönderilmesini sağlayabilirsiniz.
  - Tarih/Saat Kısıtlama: Bu uygulamamız ile Mobil ve İnternet Bankacılığı kanallarımızdaki işlemlerinizin sadece sizin belirlediğiniz gün ve saatlerde gerçekleştirilebilmesine olanak verirsiniz.
  - IP Erişim Kısıtlama: IP kısıtlama seçeneği, sizin belirleyeceğiniz IP veya IP aralıklarından yapılan bağlantılar ile Mobil ve İnternet Bankacılığı kanallarımıza giriş izni gerçekleşecektir.

- Tarayıcı Desteği: Microsoft Edge, Google Chrome 69 ve üzeri, Mozilla Firefox 62 ve üzeri ve Safari 10 ve üzeri tarayıcıları olan tüm ziyaretçilerimiz ve müşterilerimiz internet sitemizden verdiğimiz hizmetlerimizden problemsiz olarak yararlanabilirler.
- Cihaz Desteği: iOS 11 ve üzeri, Android için ise 5 ve üzeri mobil işletim sistemi kullanan müşterilerimiz, Fibabanka Mobil Bankacılık uygulamamızdan verdiğimiz hizmetlerimizden problemsiz olarak yararlanabilirler.
- Bankamız tarafından Dijital Güvenlik Birimi kurulmuştur. Elektronik bankacılık işlemlerindeki riskli işlemleri tespit etmek için uluslararası kabul görmüş yazılım kullanmakta ve yeterli sayıda personel ile 7/24 işlemler izlenmektedir.
- Banka bünyesinde bilgi güvenliğini sağlanmak amacı ile Bilgi Güvenliği Birimi görev yapmaktadır.
- Fibabanka'da saklanan müşteri kişisel verilerine erişim sadece tanımlı süreçlere göre yetkilendirilmiş personel tarafından gerçekleştirilebilmektedir. Hassas ve kritik verilere erişim için denetim izleri oluşturulmaktadır.
- Fibabanka, Bankacılık Kanunu ve ilgili diğer mevzuat hükümlerinde belirtilen sorumluluklarını karşılayacak şekilde müşterilerini ve müşteri verilerini siber tehditlere karşı etkin bir şekilde korumak amacıyla en gelişmiş güvenlik teknolojilerini kullanmaktadır.
- İlgili kanun ve yönetmelikler kapsamında zorunlu tutulan risk değerlendirmeleriyle alınan önlemler sürekli değerlendirilmektedir. Uygulamaya alınan önlemler minimum olarak mevzuat hükümleri kapsamında tanımlanmış test çalışmalarıyla değerlendirilmektedir. Bu sayede Bankamızda saklanan hassas ve kritik verilerin güvenliği makul derecede sağlanmaktadır.
- Mobil ve İnternet Bankacılığı kanallarımızın teknik altyapısı düzenli olarak gerçekleştirilen risk değerlendirmeleri kapsamında incelenmekte ve saptanan iyileştirmeler uygulanmaktadır. İş sürekliliğini sağlayabilmek için yedekli bir sistem mimarisine sahip olan Telefon ve İnternet/Mobil Bankacılık kanallarımız olası bir kesintiye karşı iki farklı lokasyondan hizmet verebilecek şekilde tasarlanmıştır.
- ATMlerimizde kart kopyalama ve kart sıkıştırma ataklarının engellenmesi için gerekli güvenlik donanımları kullanılmaktadır.
- Güvenlik Alt Yapısı

  - Fibabanka Mobil ve İnternet Bankacılığı kanallarımızdayaptığınız bankacılık işlemlerinin güvenliğini en üst düzeyde sağlamak amacıyla, dünyanın önde gelen teknoloji şirketleri ile ortak çözümler üretilmiştir ve en güvenli internet teknolojileri kullanılmaktadır.
  - Fibabanka Mobil ve İnternet Bankacılığı kanallarımıza giriş yaptığınız bilgiler, Bankamıza bilgi transferi sırasında minimum 256-bit SSL şifreleme ile korunmakta ve bu şifreleme sayesinde 3. şahısların bu bilgileri görmesi engellenmektedir. SSL, internete erişmekte kullanılan en yeni internet tarayıcılarında uygulanan bir şifreleme teknolojisidir. Bağlantınızın güvenlik durumunu SSL aracılığıyla kontrol edebilirsiniz.

- İşlem Süresi: Fibabanka Mobil ve İnternet Bankacılığı kanallarımıza girdikten sonra 570 saniye içinde işlem yapmazsanız, sizin güvenliğiniz için otomatik olarak oturumunuz sonlanır. Yeniden işlem yapmak için tekrar müşteri numaranızı (veya T.C. kimlik numaranız) ve şifrenizi girmeniz gerekir. Böylece bilgisayarınızın başından ayrılsanız bile sistem bir başkasının işlem yapmasını engeller. Tek kullanımlık şifrelerin sisteme giriş süresi ise 3 dakika ile sınırlandırılarak güvenlik seviyesi arttırılmıştır.
- İki Seviyeli Kimlik Doğrulama: Banka mevzuatlarına uygun olarak, kişisel bilgilerinizi korumak,Mobil ve İnternet Bankacılığı kanallarımız üzerinden güvenli bir şekilde finansal işlem yapabilmenizi sağlamak için aşağıdaki kimlik doğrulama metotlarının bir arada kullanılması gerekmektedir.

  - Bilinen faktör (örn: şifre, parola ve pin numarası)
  - Sahip olunan faktör (örn: cep telefonu)

Sistem tasarımlarımız kimlik doğrulama için minimum iki kimlik doğrulama metodu kullanacak şekilde tasarlanmıştır. (Bilinen faktör ve sahip olunan faktör)

Bankamız tarafından Mobil Bankacılık kanalında, cihaz tanıma özelliği bulunan ve güvenli bir kanaldan müşteri doğrulamasını sağlayan uygulama ile daha yüksek güvenlik seviyesi sağlanmaktadır. Akıllı cihazı bulunan ve Fibabanka Mobil uygulamasını yükleyen müşterilerimiz İnternet Bankacılığı kullanımlarında SMS ile gönderilen onay şifresi yerine bu uygulama üzerinden işlem onayını vermektedirler. İşlem onaynın 60 saniye içerisinde verilmesi gerekmektedir.

- Güvenlik Resmi: Mobil ve İnternet Bankacılığı kanallarımızın ilk kullanımında güvenlik resmi seçme prosedürü uygulanmaktadır. Güvenlik resmi seçildikten sonraki giriş işlemlerinde Fibabanka İnternet Bankacılığı veya Mobil Bankacılık uygulamasının kullanıldığından emin olunması için bu resmin kontrol edilmesi gerekmektedir.

Müşteri Sorumlulukları

Müşterilerimiz, güvenli bir elektronik bankacılık hizmeti kapsamında aşağıda belirtilen sorumlulukları yerine getirme yükümlülüğündedir:

- Mobil ve İnternet Bankacılığı kanalına bağlanılan cihazın fiziksel güvenliğini sağlamak, cihazda güncel anti virüs yazılımlarını ve firewall (ateş duvarı) uygulamalarını kullanmak, bu cihazlarda kopya veya lisansı olmayan yazılım kullanmama ve kullanılan işletim sistemlerini güncel tutmak.
- Ortak kullanıma veya başkalarının erişimine açık cihazlarda İnternet Bankacılığı işlemleri yapmamak.
- Kişisel verilerin, banka ve kredi kartı bilgi ve şifrelerini, İnternet Bankacılığı, Mobil Bankacılık, Telefon Bankacılığı şifre ve kullanıcı bilgilerinin güvenliğini sağlamak, bu bilgileri aile üyeleri ile bile paylaşmamak.
- İnternet Bankacılığına giriş için, internet tarayıcısından arama yapmak yerine, adres çubuğuna www.fibabanka.com.tr adresini yazarak, Bankamız internet sayfasına ulaşmak.
- Bankamız tarafından yapılan genel güvenlik bilgilendirmelerini okuma ve verilen bilgiler doğrultusunda hareket etmek.
- Gerektiğinde Bankamızın İnternet Bankacılığı kanalında "Güvenlik" menüsü altında sunmuş olduğumuz güvenlik ayarlamaları (para transferi limiti değişikliği gibi) hizmetini kullanmak.
- Bankamız tarafından gönderilen bilgilendirme ve uyarı mesajlarını okuyup, gereğini yerine getirmek.
- İnternet Bankacılığı kanalına giriş işleminde, tarafınıza gösterilen son giriş ve hatalı giriş bilgilerini kontrol etmek ve tarafınıza ait olmayan giriş veya giriş denemesi olması halinde Bankamızı bilgilendirmek.
- Kart bilgilerini ve şifrelerini 3.kişilerle paylaşmamak, yazılı olarak cüzdanında veya mobil cihazlarında bulundurmamak.
- ATMde işlem yaparken kart şifresini kimsenin göremeyeceği şekilde ve tuş panelini diğer eliyle kapatarak girmek.
- 444 88 88 ve 0850 222 77 77 Haricinde numaralardan gelen aramalara itibar etmemek.
- Başkalarının telefonu veya kamuya açık telefonlardan Fibabanka Telefon Bankacılığımıza ulaşmak istendiğinde numaranın tarafınızca çevrilmesi ve numaranın doğruluğundan emin olunması.
- Herhangi bir şüpheli durum yaşanması halinde zaman kaybetmeden şubelerimize ya da 444 88 88 ve 0850 222 77 77 Fibabanka Telefon Bankacılığımıza bildirimde bulunmak.
- Herhangi bir dolandırıcılık olayına maruz kalınması halinde, en yakın savcılığa başvurarak suç duyurusunda bulunmak.

Müşteri Hakları

- Elektronik bankacılık kanallarınızı şubelerimize uğrayarak ya da 444 88 88 ve 0850 222 77 77 Fibabanka Telefon Bankacılığımızı arayarak istediğiniz zaman kapatabilirsiniz.
- Bankamız nezdindeki hesaplarınızdan işlem yapılmaması için hesaplarınızı geçici ya da sürekli olarak kapatabilirsiniz.
- Bankamız nezdindeki müşteri kimlik ve iletişim bilgilerinizi güncelleyebilirsiniz.
- Gerektiğinde Fibabanka İnternet Bankacılığı kanalında "Güvenlik" menüsü altında sunmuş olduğu güvenlik ayarlamaları (para transferi limiti değişikliği gibi) hizmetini kullanabilirsiniz.
- Kredi kartı, banka kartı, İnternet Bankacılığı, Mobil Bankacılık, Telefon Bankacılığı şifrelerinizi değiştirebilirsiniz. Kredi kartı ve banka kartını e-ticaret, mail order ve telefon order işlemlerine kapatabilir, kart yenilemesinde bulunabilirsiniz.
- Hesap hareketlerinizin incelenmesini Bankamızdan talep edebilirsiniz.
- Bankamız talebiniz olmadan herhangi bir elektronik bankacılık hizmetini kullanımınıza açamaz. Herhangi bir elektronik bankacılık hizmetine erişiminiz kapatılmışsa veya kapattırmışsanız, yeni bir talebiniz olmadan ilgili hizmet kullanımınıza açılamaz.

Fibabanka

444 88 88

fibabanka.com.tr