

• MÜŞTERİ BİLGİLENDİRME METNİ

Saygıdeğer Müşterimiz

BDDK nın "Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelerle İlişkin Tebliğ" i gereği tüm bankaların müşterilerini İnternet Şubesi güvenliği hakkında bilgilendirmesi gerekmektedir.

Bankamızın sağladığı güvenlik önlemleri ile birlikte sizin de kendi bilgisayarınızda gerekli güvenlik önlemlerini almanız, tedbirli davranmanız uygun olacaktır.

Bankamız İnternet Bankacılığı'ndan 7 gün 24 saat boyunca hesap bakiyelerinizi görüntüleyebilirsiniz.

Bankamız tarafından İnternet Bankacılığı sisteminde iki saatten uzun bir kesinti öngörülen planlı bakım ve değişiklikler öncesinde size bilgi verilecektir.

Bankamız İnternet Bankacılığı sisteminde herhangi bir sorun ya da dolandırıcılıkla karşılaşırsanız müşteri temsilcinizle veya (0216) 587 90 00 telefondan GSD Bank A.Ş. ile irtibata geçebilirsiniz.

• BİLGİ GÜVENLİĞİ POLİTİKASI

GSD Bank A.Ş.'de , Banka'nın stratejik planlarını destekler şekilde müşterilerimize güvenli bankacılık hizmeti verebilmek üzere Bilgi Güvenliği Yönetim Sistemi işletilir. GSD Bank üst yönetimi, bilgi ve bilgi varlıklarını koruyacak yapıları kurmak ve güvenlik önlemlerinin uygun düzeye getirilmesi amacıyla ilgili politikaları belirler, çalışmaları yönlendirir ve destekler.

GSD Bank, mülkiyetinde olan her türlü bilgi / bilgi varlığını hedef alan tehditlere karşı gerekli tespit ve engelleme yöntemleri hayata geçirir. Söz konusu yöntemlerin güncel tehditlere karşı etkin koruma sağlamasını teminen gerekli test ve iyileştirme faaliyetleri yürütülür. Bu kapsamda gerekli yatırım, proje ve insan kaynağı ihtiyaçlarını planlanarak hayata geçirilir.

Banka bilgi varlıkları belirlenerek, bu varlıklar üzerinde oluşabilecek potansiyel tehdit ve zafiyetler analiz edilir. Bu potansiyel tehdit ve zafiyetlerin etkilerini azaltmak için gerekli çalışmalar Risk Yönetimi süreçleri kapsamında yürütülür. Bilgi varlıklarının taşıdığı bilgi güvenliği risklerinin tamamen yok edilmesinin mümkün olmadığı ve her durumda "artık risk" olacağı bilinci ile mevcut risklerin yönetilmesi, söz konusu artık riski en aza indirecek düzeltici ve önleyici kontrollerin etkin şekilde uygulanması esastır.

Banka mülkiyetinde olan bilgiyi ve bilgi varlıklarını hedef alan siber saldırılar bilgi güvenliği olay yönetimi kapsamında değerlendirilir. Yapılan değerlendirmeler neticesinde, mevcut kontrollerin güncellenmesi veya yeni kontrollerin devreye alınması faaliyetleri en kısa zamanda gerçekleştirilir.

Bilgi güvenliği kapsamında yürütülen faaliyetlerin hedeflenen başarıya ulaşabilmesi için kullanıcıların konuya bilinçli yaklaşımı ve sorumluluk alanlarına düşen görevleri yerine getirmesi, yayınlanan politika, prosedür, kılavuz ve duyurulara azami derecede özen göstermesi esastır. Bu kapsamda; Banka, çalışanlarının bilgi güvenliği farkındalığını arttırmak ve bu farkındalığın Banka kültürünün bir parçası haline getirmek amacıyla çalışmalar yürütür.

Bilgi Güvenliği Politikamızda yer alan amaç ve hedefleri destekleyen çalışmalar, her yıl oluşturulan Bilgi Güvenliği Planında yer alır ve bu çalışmaların ilerleme durumları, yıl içinde takip edilir ve raporlanır. Bilgi Güvenliği Yönetim Sisteminin sürekli iyileştirilmesi sağlanır, sürekli iyileştirmeye yönelik çalışmalar yönetim tarafından gözden geçirilir.

• GÜVENLİK UYARILARI

GSD Bank ismini ve logosunu kullanarak, sizden kişisel ve finansal (hesap, müşteri veya TC numaranız gibi) bilgilerinizi isteyen e-postalara kesinlikle cevap vermeyiniz. İnternet Bankacılığı'na yapmış olduğunuz girişler güvenliğinizi için kayıt altına alınmaktadır.

İnternet Bankacılığı Güvenliği

- Tarayıcı adres çubuğuna "https://www.gsdbank.com.tr" yazarak erişim sağlanmalı, İnternet Şube adresinin "https://mbs.gsdbank.com.tr" ile başladığından emin olunmalıdır. İnternet Şubesi sayfalarının tümünde, tarayıcınızın sağ alt veya üst köşesinde bir kilit işareti bulunmalıdır. İşaretin üzerine tıkladığınızda, sayfanın SSL ile şifrelendiğini ve sitenin GSD Bank'a ait olduğunu belirten ifadeler yer almalıdır.
- İnternet Bankacılığı oturumunuz esnasında 5 dakika süreyle işlem yapmadığınız takdirde, bir ikaz penceresi çıkacak ve işlemlere devam etmek isteyip istemediğiniz sorulacaktır. 1 dakika içerisinde bu pencereye de herhangi bir yanıt vermediğiniz veya "Oturumu Kapat" seçeneğini tıkladığınız durumlarda oturumunuz kapatılacaktır. İşlemlere devam etmeyi seçerseniz, oturumunuz kaldığı yerden devam edecektir.
- İnternet bankacılığı işlemlerinizi, güvenliğinden emin olmadığınız halka açık alanlardan (internet cafe vb.) veya başkalarına ait bilgisayarlardan yapmayınız. Halka açık bilgisayarlarda, hesap bilgilerinizi ve kişisel şifrelerinizi ele geçirmek amacıyla kullanılan çeşitli programların yüklenmiş olması riski vardır.
- Son dönemde ortaya çıkan bazı yazılımlar, bilgisayar klavyesinde basılan her tuşu kaydedebilmektedir ("log"layabilmektedir). Özellikle bilgisayarların çoklu kullanıldığı yerlerde (internet cafe, işyeri gibi...) rastlanabilen bu tip yazılımlardan olumsuz etkilenmemek için İnternet Bankacılığı'na giriş sırasında "Sanal Klavye" güvenlik uygulamasının kullanılması tavsiye edilmektedir. Bu uygulama, İnternet Bankacılığı kullanıcı adı ve şifresindeki rakam bölümünü "sanal klavye" üzerindeki tuşları mouse ile tıklayarak girmenizi sağlar.
- İnternet Bankacılığı Kullanıcı Adı, ve Şifre gibi size özel bilgileri kesinlikle üçüncü kişilerle paylaşmayınız. Bu bilgileri yazılı olarak saklamayınız.
- İnternet Bankacılığı'ndan çıkarken mutlaka "Güvenli Çıkış" butonunu kullanınız ve İnternet Bankacılığı'ndan çıktığınızdan emin olduktan sonra pencereyi kapatınız.

İnternet Bankacılığı giriş, SMS Doğrulama

Müşterinin sistemimizde kayıtlı olan cep telefon numarasına "Güvenlik Kodu" SMS olarak gönderilir. Güvenlik Kodu, kullanıcı tarafından ekrana girilerek SMS Doğrulaması gerçekleştirilir.

- Güvenlik Kodu tek kullanımlıktır.
- 2 dakika içinde ekran girişinin yapılması gerekmektedir.

Neden Güvenlik Kodu?

- SMS Doğrulama'yı kullanabilmeniz için cep telefonunuzun yanınızda olması yeterlidir.
- Uygulama, kullanıcı bilgilerinizden bağımsız olup, Güvenlik Kodu kendi cep telefonunuza gönderileceği için belirlenmiş olduğunuz işlemler sizin dışınızda biri tarafından gerçekleştirilemez.

• İNTERNET KULLANIMINDA GÜVENLİK

Güvenli bir İnternet Şubesi ortamı oluşturmak, karşılıklı olarak alınacak önlemlerle mümkün olabilmektedir. Bankamızın sağladığı güvenlik önlemleri ile birlikte müşterilerimizin de kendi bilgisayarlarında gerekli güvenlik önlemlerini almaları, İnternet Şubemize bağlandıkları bilgisayarın güvenliğinden sorumlu olduklarını bilmeleri ve tedbirli davranmaları gerekmektedir.

Anti Virüs - Anti Spyware Yazılımları Kullanın

Bilgisayarınızda İnterneti güvenli bir şekilde kullanabilmeniz için öncelikle casus yazılımları tespit edebilen sizi zararlı virüs, parazit, Truva Atı ve diğer tehlikelere karşı koruyabilen güncel "Anti - Virüs" ve "Anti Spyware" programlarının yüklü ve interneti kullanıyorken açık olmasına dikkat etmeniz, sürekli bu programları güncelliyor olmanız gerekmektedir.

İnternet Güvenlik Duvarı (Firewall) Kullanın

Güvenlik duvarı yazılımları, bilgisayarınıza ve bilgisayarınızda tuttuğunuz bilgilere yetkisi olmayan kişilerin erişimini engeller, bu sayede bilginiz dışında dışarıya veri taşınmasına engel olabilirsiniz. Bu yüzden yasal ve güncel bir güvenlik duvarı programı kullanmanız gerekmektedir.

İşletim Sistemi ve Web Tarayıcınızı Güncel Tutun

Kullanmakta olduğunuz işletim sisteminiz ve tarayıcı programınız için üretici firma tarafından yayınlanan güvenlik güncelleştirmeleri ve yamalarını mutlaka kullanın.

Lisanssız yazılım kullanmayın

Lisanslı program kurulumlarında bilgisayarınıza virüs bulaşma riski çok düşüktür. Korsan CD veya DVD den yüklemiş olduğunuz güvenlik programlarında güvenlik açığı olabileceğinden korsan yazılım kullanmayınız.

Bilgisayarınızın Fiziki Güvenliği

İnternet Şubesi açık iken bilgisayarınızın başından kalkmamalı, başka kişilerin bilgisayarınızı kullanmasına izin vermemelisiniz.

Güvenli olmayan İnternet Sitelerinden Dosya - Program İndirmemelisiniz

Birçok internet sitesinden program ve dosya indirmesi yapılabilmektedir, indirilen dosyaların virüslü olma ihtimali oldukça yüksektir. Bu nedenle güvenli olmayan sitelerden dosya indirmekten kaçınmalısınız.

10 GÜVENLİK KURALLI

1. Kişisel bilgi veya şifre talep eden e-postalara kesinlikle yanıt vermeyiniz

Kişisel bilgileri elde etmeye yönelik kurum adına sahte gönderilen e-posta (Phishing) larda, Kullanıcı e-posta üzerinden sahte web sayfasına yönlendirilir. Kişisel bilgilerini girmesi istenir. E-postaların içeriği sahte kampanyalar, gelen sahte havale ihbarnamesi gibi bilgilendirici e-postalar yada yüksek kazanç vaad eden e-postalar olabilir. Bu şekilde kredi kart bilgileri, kart şifresi, banka hesap bilgileri, internet şifresi, parola gibi birçok özel bilgiler ele geçirilmeye çalışılır.

GSD Bank A.Ş., e-posta ile müşterilerinden kimlik bilgisi talebi, bilgi güncellemesi, şifre değişikliği gibi özel işlemler talep etmemekte, bu amaçla herhangi bir internet sayfasına link kesinlikle vermemektedir.

2. İşlem yaptığınız sayfaların GSD Bank A.Ş. ye ait olduğundan emin olunuz

GSD Bank A.Ş. İnternet Şubesine her zaman tarayıcınızın adres kısmına <https://www.gsdbank.com.tr> yazdıktan sonra açılan GSD Bank A.Ş. ana sayfasındaki İnternet Şubesi linklerini kullanarak girin. Açılan sayfalarda, tarayıcınızın sağ alt köşesinde bir kilit işareti bulunmalıdır.

(İnternet Explorer için, Netscape için, Mozilla için) İşaretin üzerine iki kez tıkladığınızda göreceğiniz "Issued To : *.gsdbank.com.tr, Issued by: GlobalSign ServerSign CA " mesajı veri iletiminin şifreli olarak yapıldığını ve sitenin gerçekten GSD Bank A.Ş. ye ait olduğunu teyit eder.

3. Kullanıcı bilgilerinin gizli kalmasına büyük özen gösteriniz

Kullanıcı bilgilerinizin gizli kalmasına özen gösterin. Şifre ve kullanıcı adınızı belirlerken doğum tarihi, evlilik yıldönümü gibi kolaylıkla tahmin edilebilecek bilgilerden oluşmamasına dikkat edin. Şifre ve Kullanıcı Adınızı bankamız personeli dahil başkalarıyla paylaşmayın, erişilebilecek yerlere not etmeyin, şifrenizi sık aralıklarla değiştirin.

4. Tanımadığınız e-postaları açmayınız

Tanıdığınız kişi ya da kurumlardan gönderildiğinden emin olmadığınız e-postaların içerisinde bulunan linkleri tıklamayın, ekleri bilgisayarınıza yüklemeyin. Spam dediğimiz bu tür e-postalarda kullanıcıların şifrelerine ele geçirmeye yönelik key - logger veya screen - logger gibi yazılımlar bulunabilir, e-postalarınızı virüs taramasından geçirmeden açmayın.

5. Son işlem tarihi ve saatini kontrol ediniz

Kullanıcı kodunuz ve şifreniz ile İnternet Şubesine giriş yaptıktan sonra ilk ekranda giriş yaptığınız tarih ve zamanı görebilirsiniz. Böylelikle en son ne zaman giriş yaptığınızı kontrol edebilir ve farklı bir tarih gördüğünüzde bankamıza haber verebilirsiniz.

6. Güvenli olmayan internet sitelerinden program ve dosya indirmemelisiniz

Birçok internet sitesinden program ve dosya indirmesi yapılabilmekte, indirilen dosyaların virüslü olma ihtimali de olabilmektedir. Programı ya da dosyayı indirdikten sonra kurulumu başlatmadan önce mutlaka virüs taramasından geçirin.

7. İnternet cafe gibi ortak kullanıma açık bilgisayardan İnternet Şubesine giriş yapmamaya özen göstermelisiniz

Ortak kullanımlı bilgisayarlar, özellikle İnternet cafeler Trojan, Spyware, Keylogger,Screenlogger ve virüs gibi zararlı yazılımların yoğun bulundukları yerlerdir. Bu tip bilgisayarlardan şifre girişi yaparsanız şifrelerinizin 3. kişilerin eline geçmesine yol açabilirsiniz. Daima güvenliğinden emin olduğunuz bilgisayarlardan İnternet Şubesine bağlanmalısınız.

8. Hesabınızı kontrol ediniz

İnternet Şubesi hesabınızı sık sık kontrol edin, hesabınızda olağan dışı bir hareket olduğundan şüpheleniyorsanız (0216) 587 90 00 GSD Bank A.Ş. telefonundan GSD Bank A.Ş. ile irtibata geçebilirsiniz.

9. "Güvenli Çıkış" butonunu kullanınız

İnternet Şubesinden çıkarken mutlaka Güvenli Çıkış butonunu kullanınız ve İnternet Şubesinden çıktığınızdan emin olduktan sonra pencereyi kapatınız.

10. Bankanızın uyarılarına uyunuz

Bankanızın size sunmuş olduğu ek güvenlik uygulamalarını maksimum düzeyde kullanın, güvenlikle ilgili yapmış olduğu uyarı ve bilgilendirmeleri takip edip, uygulayın.