GÜVENLİK BİLGİLENDİRMESİ

**Faturakom Ödeme Hizmetleri A.Ş. aşağıdaki bilgilendirme metninde "Faturakom" olarak anılacaktır.

Faturakom Ödeme Hizmetleri A.Ş. (**"Faturakom"**) olarak kullanıcılarımızın sistemlerimize ve hizmetlerimize ilişkin bilgilendirilmelerini sağlamak adına gerekli her türlü özeni gösteriyoruz. Bu kapsamda, 01.12.2021 tarih ve 31676 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri ile Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğ'in 17. maddesi kapsamında hazırladığımız bilgilendirme metni aşağıda kullanıcılarımızın bilgisine sunulmaktadır.

GÜVENLİK BİLGİLENDİRMESİ

Bilgi güvenliğine dair en güncel teknolojileri ve akımları takip ederek sistemlerimizin en güncel güvenlik uygulamalarıyla korunması sağlıyoruz. Verilerinizin güvenliği için;

- Faturakom, TCMB'ye bağlı olarak faaliyet gösteren bir ödeme kuruluşudur. Bu kapsamda TCMB tarafından yetkilendirilmiş bağımsız denetim firmaları tarafından düzenli olarak bilgi sistemleri denetiminden geçmektedir. Bu denetim sonucu oluşturulan raporlar TCMB ile doğrudan paylaşılmaktadır.
- Tüm sistemlerimiz yıllık periyotlarda güvenlik yazılımları ve bilgi güvenliği konusunda uzman bağımsız firmalar tarafından, yılda en az altı defa kuruluş içi IT ekibimiz tarafından güvenlik testlerinden geçirilmektedir.
- Tüm sistemlerimiz en gelişmiş ve güncel güvenlik donanımları ve yazılımları ile 7/24 korunmaktadır ve gözetim altında tutulmaktadır.
- Sistemlerimiz üzerinde yapılan tüm değişiklikler sürekli olarak kayıt altında tutulmaktadır.

- Kullanıcılarımız ile sistemlerimiz arasındaki tüm iletişim güncel şifreleme yöntemleriyle şifrelenmektedir.

Faturakom olarak verilerinizin güvenliği için en üst düzeyde çaba göstermemize rağmen kullanıcılarımız açısından gerçek anlamda güvenli bir sistem, kullanıcılarımızın da riskler ve güvenli işlem yapma konusunda bilgi sahibi olmasıyla mümkün olmaktadır. Bu amaçla Güvenlik Uyarıları kısmında verdiğimiz bilgileri dikkatle okuyup sistemlerimizi kullanırken dikkate almanızı önemle rica ederiz.

DİĞER BİLGİLENDİRMELER

Faturakom sistemlerinden 7/24 faydalanabilirsiniz. Faturakom tarafından sunulan hizmetlere ilişkin şartlar ile kullanıcı/müşteri/temsilci ve Faturakom'un verilen hizmete ilişkin hak ve sorumluluklarına, bir örneği tarafınızla paylaşılan Faturakom ile akdettiğiniz ödeme hizmeti temsilcilik sözleşmesi ve sistemimiz üzerinden dilediğiniz zaman erişebileceğiniz Faturakom Ödeme Hizmetleri Şirketi Portal Kullanım Hüküm ve Koşullarından ulaşabilirsiniz. İlgili belgelere ulaşmakta herhangi bir sorun yaşamanız halinde bilgi@faturakom.com elektronik posta adresinden veya 0312 955 0 955 numaralı telefondan bizimle iletişime geçiniz.

GÜVENLİK UYARILARI

Zararlı Yazılım Kaynaklı Dolandırıcılıklar

Zararlı yazılım, programlanabilir herhangi bir aygıta, hizmete veya ağa zarar vermek veya bunlardan yararlanmak üzere tasarlanmış her türlü kötü amaçlı yazılım için kullanılan kapsamlı bir terimdir. Siber suçlular genellikle bunu, mali kazanç için mağdurlardan veri elde ederek baskı yapmak üzere kullanır. Bu veriler finansal verilerden sağlık kayıtlarına, e-postalara ve parolalara kadar değişebilir. Finansal kuruluşların müşterileri, gelişen teknolojiler ile ortaya çıkan zararlı yazılımların en büyük hedeflerindendir.

Zararlı Yazılım Türleri

İnternet bilgi hırsızları çeşitli yöntemlerle müşterilerin özel bilgilerini ele geçirmektedirler. Bu yöntemlerden en çok kullanılanlar aşağıda yer almaktadır:

1. Truva Yazılımları (Trojan)

Truva yazılımları ismini “Truva Atı”ndan almaktadır. Bir bilgisayar programına bağlanarak saklanan, tahribatını yaparken ise, programın olağan çalışmasına izin veriyormuş gibi gözüken virüslere “Truva atı” denir. Truva atları çoğunlukla, bulaştıkları bilgisayarlarda kullanılan şifre, kullanıcı adı gibi özel bilgileri ele geçirmek amacıyla kullanılır. Tespit edilmesi oldukça zor olan Truva atı, genellikle sistemlere e-posta yoluyla bulaşmaktadır. Bunun dışında yoğun disklerden (cd), sayısal çok yönlü disklerden de (DVD), e-posta ekindeki (.jpg, .gif, .txt, .doc, .xls gibi) dosyalara, bilgisayar oyunlarındaki “.exe” uzantılı uygulama dosyaları gibi pek çok yere gizlenebilir.

2. Tuş ve Ekran Kaydediciler (Keylogger ve Screenlogger)

Tuş kaydediciler, bilgisayarda, klavye vuruşlarını anlık olarak kopyalayabilen ve bunları kaydederek e-posta yoluyla korsanın eline geçmesini sağlayan programlardır. Bu tür programlar klavye ile yazılan her şeyi kaydedebilme yeteneğine sahiptir. Elde edilen kayıtlar sistemde “.txt” uzantılı metin dosyası olarak tutulur. Yapıları itibariyle kurbanların her türlü şifre ve özel yazışmalarını ele geçirmek için kullanılabilir

Ekran kaydediciler ise, ekran görüntülerini kopyalayan ve bunları e-posta ile saldırgana ulaştıran programlardır. Yakalanan anlık görüntüler sayesinde, o anda ekranda ne yapıldığı veya şifrelerin nereye yazıldığı kolaylıkla görünebilir. Tuş kaydediciler ve ekran kaydediciler dolandırıcılık eylemlerinde birbirlerini tamamlayan iki bileşen gibi çalışırlar.

3. Pop-Up Ekranlar

Bir arıza, geliştirme, erişim sorunu, yardım teklifi gibi içerikle kullanıcı karşısına çıkarılan ekranlara, kullanıcı kodu ve şifresi girilmesi istenerek erişim yetkileri çalınır. Bu dolandırıcılık tipinde, kullanıcı bir pop-up mesajı ile makinesinde tespit edilen bir eksiklikten dolayı bazı programların çalışmayacağına dair bir mesaj çıkarır. Aynı mesaj kendisine “şimdi yükleyin” diye ücretsiz yardımcı bir program teklif eder.

4. Spam E-Postalar

Çoğu zaman istenmeyen mesajlar olarak adlandırılan bu elektronik postalar, içeriğinde zararlı yazılımlar taşıyabildiği gibi, zararlı yazılım yayan sitelere de yönlendirme yapabilmektedirler.

5. Teknolojik Donanımlar

Kötü niyetli kişiler, size ait özel bilgileri zararlı yazılımlar ve diğer farklı teknolojik imkânlar kullanarak ele geçirir. Bunun hedefi kişinin kendine özel finansal işlemleri için kullandığı kişisel bilgileri ile kendisi tarafından belirlemiş olduğu şifrelerdir. Bu bilgileri ele geçiren dolandırıcının ayrıca müşterinin telefonuna giden tek kullanımlık SMS OTP bilgisini de ele geçirmesi gerekmektedir. Güncel yasal düzenlemelere göre ödeme hizmet sağlayıcıları tarafından bu riski önlemeye yönelik birkaç tedbir birden alınmaktadır.

Mobil Güvenlik

Kullandığınız bilgisayar, tablet veya cep telefonu gibi mobil cihazlarınızda üreticinin sunduğu en güncel güvenlik yamalarının kurulu olduğundan emin olunuz. Bu cihazlara orijinal üreticinin sunmadığı veya onaylamadığı işletim sistemlerini veya sistem yazılımlarını kurmayınız. Eğer kullandığınız cihazlar için anti virüs yazılımları gibi güvenlik yazılımları mevcutsa bu yazılımları mutlaka kullanınız ve bunların sürekli olarak aktif ve güncel olduğunu kontrol ediniz.

Bağlantınız Güvenli Olsun

Faturakom uygulamalarını kullanırken her zaman bizimle güvenli bağlantı kurduğunuzdan emin olunuz. Güvenli bağlantı kurup kurmadığınızı kontrol etmek için web tarayıcınızın adres çubuğunda yazan adresi kontrol ederek https:// ile başladığını kontrol ediniz. Ayrıca adres çubuğunuzun sol veya sağ ucunda bağlantınızın şifreli olduğunu gösteren bir kilit ikonu bulunduğunu kontrol ediniz. Güncel tarayıcılar eğer bağlantınızdaki şifrelemede bir hata varsa sayfamızı açmadan önce veya adres çubuğunda size bir uyarı gösterir. Sistemlerimizi kullanırken böyle bir uyarı görürseniz ekranınıza hiçbir bilgi girmeyip bilgi@faturakom.com elektronik posta adresinden veya 0312 955 0 955 numaralı telefondan bizimle iletişime geçiniz.

Bilgilerinizi Koruyun

Şifrelerinizi, kredi kartı bilgilerinizi, Faturakom tarafından elektronik posta (e-mail) adresinize gönderilen içerikleri ve kimlik doğrulama amacıyla cep telefonunuza gönderilen kodları hiçbir sebeple Faturakom personeli ve şirket içi de dahil olmak üzere kimseyle paylaşmayınız. Şirket içinde paylaşmanız gerektiğini düşündüğünüz bir durum ortaya çıkarsa firmanızın Faturakom

ile iletişime geçmesi ve şirketinizdeki diğer kişiye ayrı bir kullanıcı kaydı açılması için gereken işlemleri tamamlaması gerekir.

Sahte E-postalara Kanmayın

Faturakom, hiçbir zaman elektronik posta (e-mail) adresinize sizden kişisel bilgilerinizi veya şifrenizi isteyen elektronik postalar (mailler) göndermez! Böyle bir elektronik posta (e-mail) aldığınızda hiçbir bilgi girmeden bilgi@faturakom.com e-posta adresi veya 0312 955 0 955 numaralı telefondan bizimle iletişime geçiniz.

Güçlü Şifre Kullanın

Şifrelerinizi hiçbir sebeple bilgisayarınızda, cep telefonunuzda, elektronik posta kutunuzda, mail adresinizde açık olarak bulundurmayınız. Şifrelerinizi ezberinizde tutmak veya bu amaç doğrultusunda geliştirilmiş güvenli bir şifre saklama uygulamasında tutmanız en güvenli yoldur.

İnternet Güvenliği

Cihazlarınızla kamuya açık alanlarda kablosuz ağlar üzerinden internete bağlanırken daha dikkatli olunuz. Bu alanlarda internete bağlanırken kişisel verileriniz veya şifreniz gibi bilgileri girdiğiniz web sitelerine güvenli bağlantı kurduğunuzdan ve cihazınızdaki güvenlik yazılımlarının aktif olduğundan emin olunuz.

Güncel Kalın

Faturakomun sistemlerine sadece web uygulamalarımızı kullanarak web tarayıcınızla erişebilirsiniz. Uygulamalarımıza erişirken güncel versiyona sahip web tarayıcılarını kullanınız.

Hesabınızı Güvende Tutun

Faturakom uygulamalarını kullandıktan sonra bilgisayarınızı terk edecekseniz sağ üst bölümde bulunan kullanıcı menüsündeki seçeneği kullanarak güvenli çıkış yaptığınızdan emin olunuz.

Şifreleriniz Koruyun

Şifrelerinizi hiçbir sebeple bilgisayarınızda, cep telefonunuzda, elektronik posta kutunuzda, mail adresinizde açık olarak bulundurmayınız. Şifrelerinizi ezberinizde tutmak veya bu amaç doğrultusunda geliştirilmiş güvenli bir şifre saklama uygulamasında tutmanız en güvenli yoldur.

Aramalara Karşı Dikkatli Olun

Sizi Faturakom'dan aradığını iddia ederek sizden bilgi isteyen kişilere karşı dikkatli olunuz. Arayan numaranın Faturakom'a ait olduğunu teyit ediniz. Faturakom tarafından müşterilerimiz/temsilcilerimiz ile sadece ilgili Faturakom personeli iletişime geçer. Eğer sizi arayanı tanımayıp şüpheye düşerseniz görüşmeyi sonlandırıp müşteri temsilcisiyle iletişime geçip durumu bildiriniz. Müşteri temsilcisine ulaşamıyorsanız bilgi@faturakom.com elektronik posta adresinden veya 0312 955 0 955 numaralı telefondan bizimle iletişime geçiniz.

Şifrelerinizi oluştururken;

Kısa şifreler yerine uzun şifreler oluşturunuz. En az 8 karakterden oluşan şifreler önerilmektedir.

Şifrelerinizde en az birer küçük harf, büyük harf, rakam ve özel sembol olduğundan emin olunuz. Bunu yaparken sadece ilk harfi büyük yapmak; şifrenin sonuna ünlem veya nokta koyma gibi birçok kullanıcı tarafından alışkanlık haline getirilmiş davranışlardan uzak durunuz.

Şifrelerinizde aynı karakteri veya rakamı ikiden daha fazla tekrar etmeyiniz.

Şifrelerinizde ardışık rakam serileri ("123" gibi), alfabetik seriler ("abc" gibi) veya klavye düzenine bağlı seriler ("qwerty" gibi) kullanmayınız.

Şifrelerinizde isminizi, doğum tarihiniz veya evcil hayvanınızın ismi gibi çevreniz tarafından veya sosyal medya hesabınızdan yola çıkılarak bulunabilecek bilgileri kullanmayınız.

Şifrelerinizi en fazla üç aylık dönemlerde değiştiriniz. Değiştirdiğiniz şifrelerinizin öncekilerle ortak karakter sayısının az olmasına özen gösteriniz. Örneğin şifre yenilemelerinde şifrenizin sonuna değiştirdiğiniz yıl ve ayı ekleyerek aynı şifreyi uzun süre kullanmayınız.

Birden fazla sistemde aynı şifreyi kullanmayınız. Gizli verinizi tutan her sistem için farklı bir şifre belirleyiniz.

Şifrelerinizin veya kişisel bilgilerinizin yetkisiz kişilerin eline geçtiğinizi düşünüyorsanız bilgi@faturakom.com elektronik posta adresinden veya 0312 955 0 955 numaralı telefondan bizimle iletişime geçiniz.

Finansal sistemleri güvenli kullanmanıza katkısı olacağını düşündüğümüz aşağıda web bağlantısı verilen Türkiye Bankalar Birliğinin hazırladığı Dolandırıcılık Eylemleri ve Korunma Yöntemleri adlı belgeyi okumanızı tavsiye ederiz.