

NXT Elektronik Para ve Ödeme Hizmetleri A.Ş. (Bundan böyle **“Onspay”** olarak adlandırılacaktır.)’de iş ihtiyaçlarına, kanunlara ve yasal düzenlemelere uygun şekilde bilgilerin güvenliğini sağlamak amacıyla üst yönetim gözetiminde bilgi güvenliği yönetim sistemi mevcuttur.

Şirket yönetimi, Onspay’de bilgi güvenliği yönetim sisteminin hayata geçmesi konusunda destek sağlar, gerekli durumlarda atama ve yönlendirme yapar. Bilgi güvenliği yönetim sistemi, tanımlı bir risk yönetim yaklaşımı ve temel kuralların belirlendiği bilgi güvenliği politikaları ile sağlanmaktadır. Bu politikalar, tüm Onspay çalışanlarının erişebileceği şekilde şirket içerisinde paylaşılmıştır. Bilgi güvenliği politikalarının amacı, Bilgi Güvenliği risklerinin yönetilmesi ve bilginin yeterli seviyede güvenliğinin sağlanmasıdır. Tüm şirket çalışanları, sorumlusu oldukları iş süreçleri ve bilgi varlıklarında bu politikalarda yazan kuralların uygulanmasından sorumludur. Şirketin bilgi güvenliği yönetim sisteminin uygunluğu, yeterliliği ve etkinliğinin bağımsız olarak gözden geçirilmesi sağlanır. Bağımsız gözden geçirme sonuçları, yönetime raporlanır ve ilgili kayıtlar saklanır.

Şirket yasal düzenlemeler doğrultusunda güvenlik gereksinimlerini belirler ve uygular. Onspay müşterilerine ait tüm kişisel bilgiler, Türkiye Cumhuriyeti kanun ve düzenlemelerine uygun şekilde korunur. Kişisel bilgilerin kaydedilmesinde, işlenmesinde ve paylaşılmasında veri gizliliği ilkesine uygunluk için yürürlükteki yasa ve mevzuata uygun hareket edilir. Onspay’in önemli kayıtları, kayıp ve bozulmalara karşı koruma altına alınır. Kayıtların saklama süreleri belirlenirken mevzuattaki yükümlülükler dikkate alınır.

GÜVENLİK İPUÇLARI

- Kişisel Bilgilerinizi ve Şifrenizi Bilgisayarınızda/Cep Telefonunuzda Saklamayın Kimliğiniz son derece önemli bir belgedir. Bu nedenle, taranmış görüntüsünü bilgisayarınızda saklamayın.
- Şifrelerinizin Güvenlik Seviyelerini Yükseltin
- Gerçekleştirdiğiniz finansal işlemlere ilişkin referans numarası, tutar, alıcı vb. bilgileri asla üçüncü kişilerle paylaşmayınız.
- Onspay hesabınızda kullanıcı adı/şifre belirlerken isim, doğum tarihi gibi kolay tahmin edilebilir bilgilerden şifre belirlemeyin. Kişisel bilgilerinizi vey Şifre’nizi gizli tutun, kimseyle paylaşmayın. Bu bilgileri herhangi bir yere yazmayın.
- Bilgilerinizi Paylaşmayın
- Onspay sözlü ya da yazılı olarak hiçbir zaman e-posta, SMS ya da telefon aracılığıyla Onspay Şifre’nizi sormaz veya talep etmez. Bu nedenle sizden Onspay Şifre’nizi ve talep eden 3. şahıslara şifrenizi açıklamayınız.
- Kişisel bilgilerinizi veya şifrenizi göndermenizi talep eden bir e-posta Onspay’e aitmiş gibi görünen bir adresten gelirse, bu e-postaya cevap vermeyin. (Onspay) sözlü veya yazılı olarak hiçbir zaman e-posta, SMS ya da telefon aracılığıyla şifrelerinizi sormaz veya talep etmez.
- Kişisel Bilgisayarlarınızın Güvenli Olmasına Dikkat Edin
- Bilgisayarınızda mutlaka lisanslı programlar ve işletim sistemi kullanın. İşletim sisteminizi ve programlarınızı sürekli güncelleyin.

- Antivirüs, anti spyware ve kişisel firewall gibi koruma kalkanları kullanmaya özen gösterin.
- İnternette indirdiğiniz ya da bilgisayarınıza yüklemek istediğiniz programları mutlaka virüs taramasından geçirin. Kaynağını bilmediğiniz programları bilgisayarınıza yüklemeyin. Özellikle “.exe” uzantılı dosyalara dikkat edin.
- Uygulamalar açıkken bilgisayar başından kalkmamanızı tavsiye ederiz.
- Güvenliğinden Emin Olunmayan Kablosuz Ağları Kullanmayın
- İnternet erişiminizi ADSL ile sağlıyorsanız, interneti kullanmadığınız zamanlarda bağlantınızı kapatın.
- Wi-Fi, Bluetooth, kızılötesi gibi kablosuz yöntemler cep telefonlarına yetkisiz erişim riski doğurabilmektedir. Bu nedenle güvenliğinden emin olmadığınız kablosuz ağları kullanmayınız.
- Bluetooth üzerinden gelen, kaynağını ve güvenilirliğini bilmediğiniz dosyaları da kabul etmeyin; ihtiyaç duymadığınız zamanlarda bu uygulamaları kapalı tutun.
- İnternet sitemizi kullanmak için herhangi bir linki tıklamak yerine www.onspay.com adresini tarayıcınızın adres çubuğuna yazarak giriş yapın.
- www.onspay.com uzantılı olmayan hiçbir mail adresine itibar etmeyiniz
- Gerçekleştirdiğiniz işlemlere ait dekontlar, talebiniz durumunda sistemimize kayıtlı e-posta adresinize ya da iletişim adresinize iletilir

OLASI TEHLİKELER

- İnternette güvenlik konusunda merak edilen virüs saldırıları ve benzeri diğer tehlikelere karşı önlem alabilmek için bilgi sahibi olun.
- Virüs Saldırıları Bilgisayarlarınız, akıllı telefonlarınız ve tabletleriniz çeşitli yollarla virüslere maruz kalabilir:
 - Sahte e-posta linkleri,
 - Arama motorlarında listelenen sahte sayfa linkleri,
 - İnternet sitelerindeki güvenli olmayan reklam ve sponsor linkleri
 - Onspay tarafından gönderiliyormuş algısı verilen SMS’ler içerisindeki linkler

Phishing (Oltalama) Saldırıları: Oltalama saldırıları olarak da bilinen bu saldırı türünde genel olarak kullanıcıların e-posta hesaplarına; yüksek fatura bilgileri, hediye, indirim, kampanya, ödül gibi cezbedici sahte iletiler gönderilir ve kredi kartı bilgileri, kimlik bilgisi, TCKN, müşteri numarası gibi hassas verilerin çalınması amaçlanır. Dolandırıcılar bu bilgileri farklı amaçlar için kullanabilir. Maddi ya da manevi zarar verme amaçlanır. Phishing (Olta) Saldırıları, çeşitli finans kurumları tarafından gönderilmiş gibi görünen, acil ve çok önemli konular içeriyormuş gibi duran sahte e-postalardır.

Oltalama Saldırılarına Karşı Alınabilecek Önlemler: Oltalama saldırılarından korunma yöntemlerinden en etkiliisi; gelen eposta sizi bir siteye yönlendiriyor ise, bu sitelerin https(s) takılı olup olmadığına bakılır. Güvenlik sertifikası olan bir site https takısı alır. Şüpheli görülen e-postalardaki URL linkleri tıklanmamalıdır.

Herhangi bir dolandırıcılık veya şüpheli işlemle karşılaşmanız durumunda bize iletişim kısmına yer alan iletişim formunu doldurarak ya da iletişim numaralarımızdan ulaşabilirsiniz.