

# GÜVENLİ GÜNLER BÜLTENİ



Bilgisayar kullanıcılarına yönelik hazırlanır. Her ayın 15'i çıkar. Bültenlerin her ay size ulaşması için üye olunuz: <http://eepurl.com/bP-tWn>

ŞUBAT 2017



## Güvenli e-ticaret

**TİCARETİN (ALIŞVERİŞİN) LİDYALILARIN PARAYI İCAT ETMESİYLE BAŞLADIĞI SÖYLENİR AMA TARİHTE ALIŞVERİŞ TAKASLA BAŞLAMIŞTIR. İkinci Dünya Savaşı sonrası gelişen teknoloji ve dünya ekonomisiyle birlikte de alışveriş alışkanlıkları değişmiştir: televizyon pazarlama programları, sadakat programları, CRM uygulamaları ile Diners Club ve banka kredi kartlarının yanı sıra süpermarketler ve AVM'ler.**

Alışveriş alışkanlıklarında gelinen son nokta (!) ise, İnternet üzerinden alışveriş yani e-ticarettir. Bundan 20 yıl önce 15 yaşındaki kızınızın beğendiği bir tişörtü Çin'den sipariş ederek alabileceğinizi söyleseydim ne derdiniz? Ya da sahip olduğunuz herhangi bir mal ve eşyayı İnternet üzerinden kolayca satabileceğinizi...

Ne var ki İnternet üzerinden alışveriş, sağladığı yararların yanında çeşitli riskleri de beraberinde getirmektedir. Bu amaçla yapılan her işlemde aslında bu riskler de satın alınmaktadır. Risklerin tamamen ortadan kaldırılması mümkün değildir ama azaltılabilirler. Gelin, nasıl minimize edebileceğimize ve mümkün olduğunca kontrol altında tutabileceğimize birlikte bakalım.

## 1. Doğru sayfada işlem yaptığınızdan emin misiniz?

Kötü niyetli kişilerin Internet üzerinde en sık başvurdukları yöntemlerden biri insanları farklı sayfalara yönlendirmektir. Bu tuzağa düşmemek için browser'da mutlaka adres bilgisini kontrol edin, doğru sayfada olduğunuzdan emin olun.

<https://www.amazon.com> web sayfası güvenilir mi?<sup>1</sup>

Alışveriş yapmak istediğiniz siteyi ne kadar taniyorsunuz. Amazon, hepsiburada, n11, gittigidiyor, eBay gibi bilindik siteler dışında bilmediğiniz bir siteden alışveriş yapacaksanız alışverişe başlamadan önce,

- » Site ile ilgili yorumları ve şikâyetleri Internet üzerinden kontrol ederek site hakkında gerekli bilgileri elde edebilirsiniz!
- » İlgilendiğiniz ürün hakkında bir e-posta ile soru sorabilirsiniz. Gelen yanıtın içeriği size site hakkında bilgi verecektir. Örneğin e-posta sitenin domain'i dışında başka bir domain üzerinden (@gmail, @hotmail vb) geliyorsa bir düşünün!
- » Yine de emin olamadıysanız öncelikle sadece küçük bir şey satın alın!
- » Fiyat çok çok ucuz ise, almadan önce iki kez düşünün!



<sup>1</sup> Dikkat ederseniz burada son harf tekrarlanarak yeni bir isim yaratılmış. Bunun gibi, çok bilinen şirketlerin isimlerinde fark edilmeyecek küçük değişikliklerle yeni alan adı yaratılması saldırganların çok kullandığı bir yöntemdir.

## 2. Garanti, iade ya da defolu ürünlerin iadesi koşullarını kontrol edin?

Dört gözle beklediğiniz ürün geldi ancak defolu ya da beklediğiniz gibi değil ya da taklit. Ne yapacaksınız?

Alışveriş yaptığınız sitenin yetkili satıcı olup olmadığını ve ürünle ilgili garanti ile iade koşullarını mutlaka kontrol etmelisiniz. Ürünü hangi koşullarda ve nasıl iade edeceğinizi de öğrenmelisiniz.

Tecrübeyle sabit, yıllar önce gittigidiyor üzerinde bir Montblanc kalem görmüştüm. Öncelikle ürünü satan satıcı ile iletişime geçtim; satıcı ürünün orijinal olduğunu belirtti. Ödemeyi yaparak ürünü satın aldım. Daha sonra ürün teslim edildiğinde hemen kontrol ettim ve orijinal ürün olmadığını fark ettim. Gittigidiyor politikası gereği alıcı onay vermeden satıcıya ödeme yapılmıyor. Siteye gerekli bilgilendirmeyi yaparak ürünü iade ettim onlar da paramı iade ettiler ona göre karar verin.

Doğru sayfa mı?

<http://amazon.com>



Hayır

Evet

Site güvenilir mi?

Google'a sor!



Hayır

Evet

Garanti ve iade koşulları uygun mu?



Hayır

Evet

Bilgisayarınız, mobil cihazınız güncel mi?



Hayır

Evet

Bağlantı güvenli mi?

<https://>



Hayır

Evet

Ödeme kredi kartı ya da kapıda yapılıbiliyor mu?



Evet



### 3. Alışveriş yaptığınız site ile paylaştığınız kişisel bilgileriniz ne kadar güvende?

Alışveriş yaptınız, mutlusunuz, ancak bir süre sonra size bir sürü spam e-posta gelmeye başladı, çünkü site sizin bilgilerinizi satmış. Böyle bir durumla karşılaşmamak için öncelikle firmanın gizlilik sözleşmesinin bulunup bulunmadığını, sonra da bilgilerinizi girerken genellikle seçili olarak gelen checkbox'ları mutlaka kontrol edin. İstemediğiniz şekilde bilgilerinizin paylaşılmasına izin vermeyin!

### 4. İşlem yaptığınız bilgisayar/telefon/tablet güvenli mi?

Asla güvenli olmayan bir cihazdan alışveriş yapmayın. İşletim sisteminin güncel versiyonunun yüklü olduğundan emin olun. Cihazınızda mutlaka bir güvenlik programı yüklü olmalı. Hiçbir zaman Internet kafe gibi yerlerde bulunan, farklı kişilerce kullanılan cihazlardan işlem yapmayın.

### 5. İnternet bağlantısı güvenli bir bağlantı mı?

Ödeme yapmadan ve kişisel bilgilerinizi paylaşmadan önce İnternet bağlantısının güvenli olduğundan emin olmalısınız. Bunu çok kolayca kontrol edebilirsiniz. İnternet browser'dan link'i kontrol edin. Link "https" ile başlamalıdır; "s" bağlantısı secure yani güvenli olduğunun göstergesidir. Sadece "http" ile başlaması, bağlantının güvenli olmadığını işaretidir; bilgileriniz iletilirken kolayca ele geçirilebilir demektir.

### 6. Kapıda ödeme mümkün mü?

Alışveriş yapmadan önce kapıda ödemenin mümkün olup olmadığını sorabilirsiniz. Kapıda ödeme yapma, hem kredi kartı bilgilerinizi paylaşma gereğini ortadan kaldırır hem de ürün teslim edildiğinde ödeme yapmadan kontrol etme şansını sağlar.

### 7. Ödeme

Asla banka havalesiyle ödeme yapmayın. Mutlaka ödemenizi kredi kartı (varsa sanal kredi kartını tercih edin) ya da PayPal ile yapın. Eğer bir sahtekarlık söz konusu olursa paranızı geri alabilme şansınız olur.

## YAZAR HAKKINDA

**BÜLENT DAĞ**, İTÜ İşletme Mühendisliğinden mezun olmuştur. Banka ve sigorta sektöründe süreç yönetimi, re-organizasyon, IT yönetimi-transformasyonu ve temel sigortacılık paketi devreye alınması konularında uzun yıllar tecrübe kazanmıştır.



## YASAL UYARI

Bu dokümanın tüm hakları Lostar Bilgi Güvenliği A.Ş.'ye aittir ve Creative Commons BY-NC-ND 4.0 (Attribution-NonCommercial-NoDerivatives 4.0 International - (CC BY-NC-ND 4.0) lisansı altında dağıtılır. Herhangi bir değişiklik yapmadan kaynak gösterilerek dağıtılabılır. Ticari olarak kullanılamaz.