SİBERAY PROJESİ

Siber Suç Nedir ?

Kurum veya kullanıcıları hedef alan ve bilişim sistemleri üzerinden işlenen suçlardır.
Siber suç, bir bilişim sistemlerine izinsiz olarak hukuka aykırı bir şekilde girilmesi, verileri şifreleme, ele geçirme, yerini değiştirme, sistemlerin erişiminin engelleme gibi siber suç teşkil eden durumun elektronik ortamda gerçekleştirilmesi ile ortaya çıkmaktadır. Basit gibi görülebilir fakat başkasına ait bir sosyal medya hesabına veya e-posta adresine bilgisi ve rızası dışında erişim yapmak suçtur. Siber suçun, fiziksel olarak işlenen tehdit, şantaj, hakaret gibi suçlardan hiçbir farkı yoktur.

SİBERAY Projesinin Amacı Nedir ?

SİBERAY programının temel amacı güvenli internet kullanımı için kullanıcılara ve vatandaşlara yol göstermektir.

Ulusal ve uluslararası platformlarda, siber güvenlik, teknoloji kullanımı, sosyal medya kullanımı, siber zorbalık ve teknoloji bağımlılığı gibi konularda farkındalık oluşturarak; internet, ekran, teknoloji bağımlılığı gibi kişiye ve topluma zarar veren alışkanlıklarla, siber zorbalıkla ve her türlü siber suçlarla eylem daha oluşmadan mücadele etmektir.

Programın amacı, toplumun her bir ferdinin interneti ve teknolojiyi güvenli, faydalı, etkili şekilde kullanmalarını sağlamaya yönelik faaliyetler, içerikler, çalıştaylar, çevrimiçi ve çevrimdışı konferanslar, ürünler geliştirerek bu sayede örf, adet ve milli kültüre bağlı nesiller yetiştirilmesine katkı sağlamaktır.

Programın Hedefleri

- ✓ Toplumda farkındalık oluşturmak
- ✓ Güvenli internet kullanımını sağlamak
- ✓ Teknoloji bağımlılığının zararlarını önlemek
- ✓ SİBERAY mobil ve web uygulamaları ile hedef kitleye daha hızlı ulaşabilmek

GÜVENLİ İNTERNET ÖNLEMLERİ

Açık Kablosuz Ağları Mecbur Olmadıkça Kullanmayın

Mobil cihazınızın internet paketinin kotası kimi zaman can sıkıcı seviyelerde olabilir. Böyle bir durumda ulaşabilir durumdaki, parola gerektirmeyen, güvenlik seviyesi düşük bir açık kablosuz ağ hayat kurtarıcı gibi görünebilir. Ancak bu tip ağlar, yapılarından ötürü saldırıya da açıktır ve güçlü bir siber güvenlik uygulaması kullanmıyorsanız siber saldırganların açık hedefi haline gelebilirsiniz. Böyle bir durumda cihazınızdaki değerli veriler, belki parolalar saldırganların eline geçebilir. Bu nedenle, mecbur değilseniz açık kablosuz ağları kullanmamalısınız.

Önemli Verilerinizi Yedekleyin

Yedekleme söz konusu olduğunda çoğu birey bilgisayarın sabit diskine ya da telefonunun hafıza kartına güvenmekte. Ancak bu durum hem siber saldırıyla karşı karşıyayken hem de diskin ya da telefonun bozulması veya çalınması durumunda o çok değerli verileri bir daha kurtaramama riskiyle de karşı karşıya bırakmakta. Günümüzde yaygın olarak kullanılan ve hemen hepsini cüzi ücretlerle yüksek kapasiteye taşıyabildiğiniz bulut depolama alanları hayat kurtarıcı olabilir. Ancak burada da güvenlikten taviz vermemeli, yüksek güvenlik standartlarına sahip ve hesabınızın ele geçirilme ihtimaline karşılık çift faktörlü koruma sağlayan servisleri tercih etmelisiniz.

Bilgisayarınızın ve Telefonunuzun Ekranı Size Özeldir, Paylaşmayın

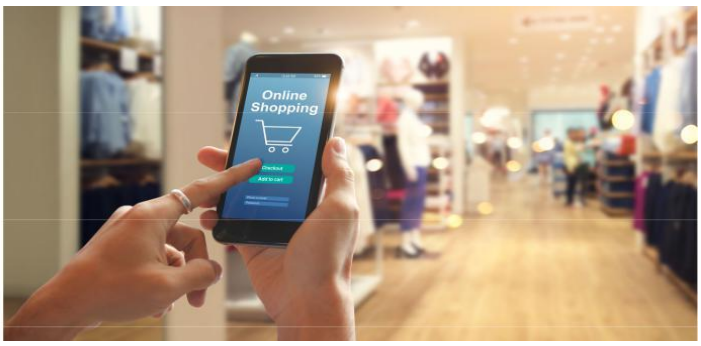
Kimi zaman açık havada bir kafede bilgisayarınızı açıp çalışmak ya da oyalayıcı bir şeyler yapmak oldukça keyifli olabilir. Ancak böyle ortamlarda meraklı gözlerin de dikkatini üzerine çekebilirsiniz. Böyle bir durumda ekranınıza girdiğiniz kişisel verileriniz bir anda o meraklı gözlerin sahiplerinin eline geçebilir. Bu nedenle cihazınızı sadece sizin görebileceğiniz şekilde konumlandırmalı, söz konusu cihazınız telefonunuzsa da aynı dikkati göstermelisiniz.

Güncellemeleri İhmal Etmeyin

Akıllı telefonlarla birlikte sıklıkla güncellenen uygulamalarla karşılaşır olduk. Eğer cihazlarınızın otomatik güncellemesi açıksa bu yenilikler otomatik olarak cihazınıza yüklenir. Ancak internet kotası ya da benzer endişelerle bunu erteliyorsanız sisteminize sızmak isteyenler için bir açık kapı da bırakmış olursunuz. Bu da cihazınızdaki verilerin ele geçirilmesine, sisteminize bir zararlı yazılım yüklenmesine ya da bir DDoS saldırısı için zombi bilgisayar olarak kullanılmasına neden olabilir.

Güvenli Olmayan Sitelerden Alışveriş Yapmayın

İnternetten alışveriş yapmanın artı yönlerinden biri kuşkusuz daha ucuza istediğiniz ürünü satın alabilmek. Ancak fiyat peşinde koşarken alışveriş yapacağınız sitenin güvenlik standartlarını incelemenizde fayda var. Bunun için adres satırının "http" yerine "https" ile başlamasına dikkat etmeli, sitenin ana sayfasında hangi güvenlik standartları tarafından korunduğu bilgisini -genelde en altta bulunur- incelemelisiniz.



Tüm Dijital Dünyanızı Tek Bir Parola ile Yönetmeyin

Söz konusu karmaşık parolalar olduğunda insan beyni yeterince verimli olmayabiliyor. Normalde güçlü bir parola harf (büyük ve küçük), sembol ve rakamlardan oluşan bir kombinasyona sahiptir. Ancak pek çok kişi bu tip bir parola kullanmaktansa doğum yılını da içeren parolalar kullanmayı tercih ediyor. "Kim benim doğum yılımı bilebilir ki?" diye düşünebilirsiniz. Burada önemli olan siber saldırganların yılı doğru bilmelerinden ziyade tahmin edilebilir bir parolayı daha kolay çözebilmeleridir aslında. Dikkat etmeniz gereken bir diğer nokta da her yerde aynı parolayı kullanmamanız. Kendinize uygun tipte bir kombinasyonu seçip, biri ele geçirildiğinde bile diğerlerinin tahmin edilemeyeceği bir kombinasyona sahip parolalar kullanmanız siber dünyadaki verilerinizi korumak için son derece önemlidir.