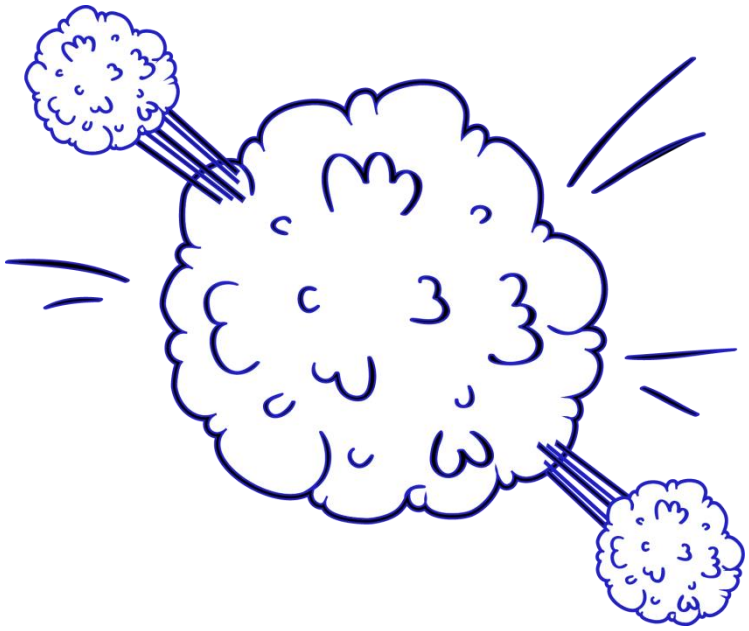
E-GÜVENLİK
FARKINDALIK MESAJLARI

TELEFONDA KRİTİK BİLGİ PAYLAŞMAYIN

- Yöneticileriniz de dahil hiç kimse ile kurum ve personele ait kritik bilgiyi telefondan paylaşmayın.
- Telefon ile aranarak acil olduğu belirtilse dahi bütün iş süreçlerinizi yazılı olarak işleterek kayıt altına alın.

ARTIK SAVAŞLAR SİBER ALEMDE

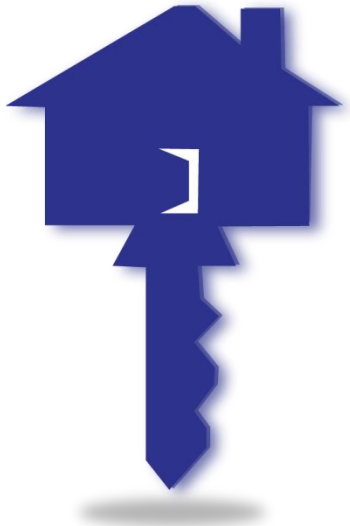


- 21. yüzyıl teknolojileri her anlamda dünyanın geleceğine şekil vermeye devam ediyor.
- Teknolojinin ulaştığı nokta artık onun doğrudan bir silah olarak da kullanabileceğini göstermekte.

27001 STANDARDI İLE GÜVENLİĞİNİZİ ARTTIRIN

- 27001 sadece iş süreçlerinizin profesyonel ve güvenli yürütülmesini değil sizlerin de güvenliğini sağlar.
- Kurumunuzun belirlediği politika ve prosedürleri uygulayın ve uygulatın.

EVİNİZİN KAPISINI AÇIK BIRAKIP GİDER MİSİNİZ?



- Bilgisayarınızın ekranını açık bırakmayın!
- Bilgisayarınıza erişim sağlayan kötü niyetli kullanıcılar, size ait bilgilere erişebilir bilgilerinizi değiştirebilir, çalabilir ya da suç oluşturacak bir işlem yaparak sizi zor durumda bırakabilir.

ANTİVİRÜS PROGRAMI

- Bilgisayarın sürekli korunmasını sağlamak için devamlı güncel virüs veritabanına sahip olan bir antivirüs programı kullanınız.
- Anti virüs programınızın sürekli güncel olmasını sağlayın.

E-POSTA EKLERİNE TIKLARKEN DİKKATLİ OLUN

- E-posta iletilerindeki yanıltıcı linkler, sıklıkla kimlik avı veya casus yazılım yüklemek için, bazen de virüs iletmek için kullanılabilir.
- E-postanız ile gelen yanıltıcı bir linki tıkladığınızda, bilgisayarınıza kötü amaçlı yazılı yüklemeye çalışan bir internet sayfasına yönlendirilebilirsiniz.

KURUMSAL BİLGİLERİNİZİ TAŞINABİLİR MEDYAYA KAYDEDİLMESİ RİSK İÇERİR

- USB Bellek, harici disk, tablet ve dizüstü bilgisayarlar vb.. taşınabilir medya araçlarında; kişisel bilgilerinizi ve çalıştığınız kuruma ait gizlilik içeren bilgilerinizi bulundurmayınız.

DOSYA PAYLAŞMAYIN!

- Dosya paylaşımı, yetkisiz erişime olanak sağlamaktadır.
- Zorunlu haller dışında dosyalarınızı paylaşıma açmayın.
- Zorunlu hallede yapılan dosya paylaşımlarında, herkese değil sadece gerekli kişilere erişim izni verin.

ŞİFRELERİNİZİ PAYLAŞMAYIN!

- Şifreler hangi yetki ve rolde kullanıcıya ait olursa olsun kişiye özeldir ve hiç kimseyle paylaşılamaz,
- Hiçbir birim, yönetici ya da sistem yöneticisi şifre talebinde bulunmaz/bulunamaz,
- Şifrenin herhangi bir şekilde ele geçirilmesinden şifre sahibi sorumludur.
- Şifrelerinizi belirli aralıklarla değiştiriniz.
- İki adımlı doğrulama imkanı varsa muhakkak kullanın!

SOSYAL MEDYA ORTAMLARINA DİKKAT!

- Sosyal medya ortamları, insanların arkadaşlarıyla iletişim kurmasını ve bilgi alışverişi yapmasını amaçlayan paylaşım web siteleridir.
- Sosyal paylaşım siteleri doğası gereği şahsımızla ilgili birçok bilgi barındırmaktadır.
- Bu bilgiler kötü niyetli kişilerin elinde çok ciddi güvenlik açıklarına sebebiyet vermektedir.
- Unutulmamalıdır ki güvenlikle ilgili ortaya çıkan sorunların büyük kısmı makinelerden değil insanlardan kaynaklanmaktadır.