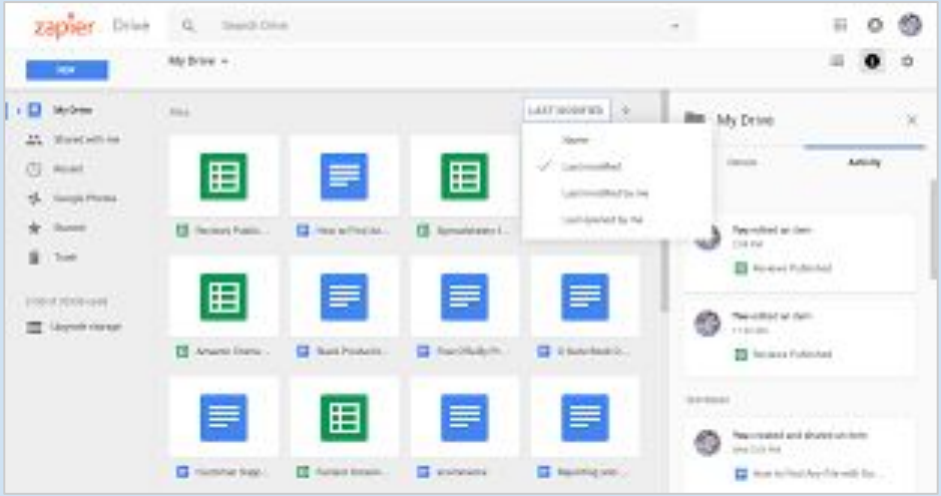
# Dosya Erişim ve Paylaşımı

- Dosyalarımızı Ortak Paylaşımda tutmalıyız.
- Dosya yetkilendirmesine dikkat etmeliyiz.
- Yetkisiz erişime izin vermemeliyiz. Kendimiz de yapmamalıyız.
- Önemli bilgileri (Özellikle Kişisel Verileri) şifreleyerek paylaşmalıyız.



# e-postalar

- Virüslerin en az %30 u e-postalardan bulaşır.
- Gelen e-postaların adreslerinin doğruluğu kontrol edilmelidir.
- e-postalarda en sıklıkla yapılan hata: Gönderdiğimiz kişiyi seçerken dikkat etmemek.
- Yanlış adrese göndermek kişisel/gizli bilgileri açığa çıkarır. Hukuken sorumluluk bulunmaktadır.
- Linkler tehlikelidir.
- Dosya ekleri virüs içerebilir.
- Sıkıştırılmış dosyalar tehlikelidir.
- Gizli dosyalar (özellikle Kişisel Veriler)şifrelenerek gönderilmelidir.

# Mobil cihazlar

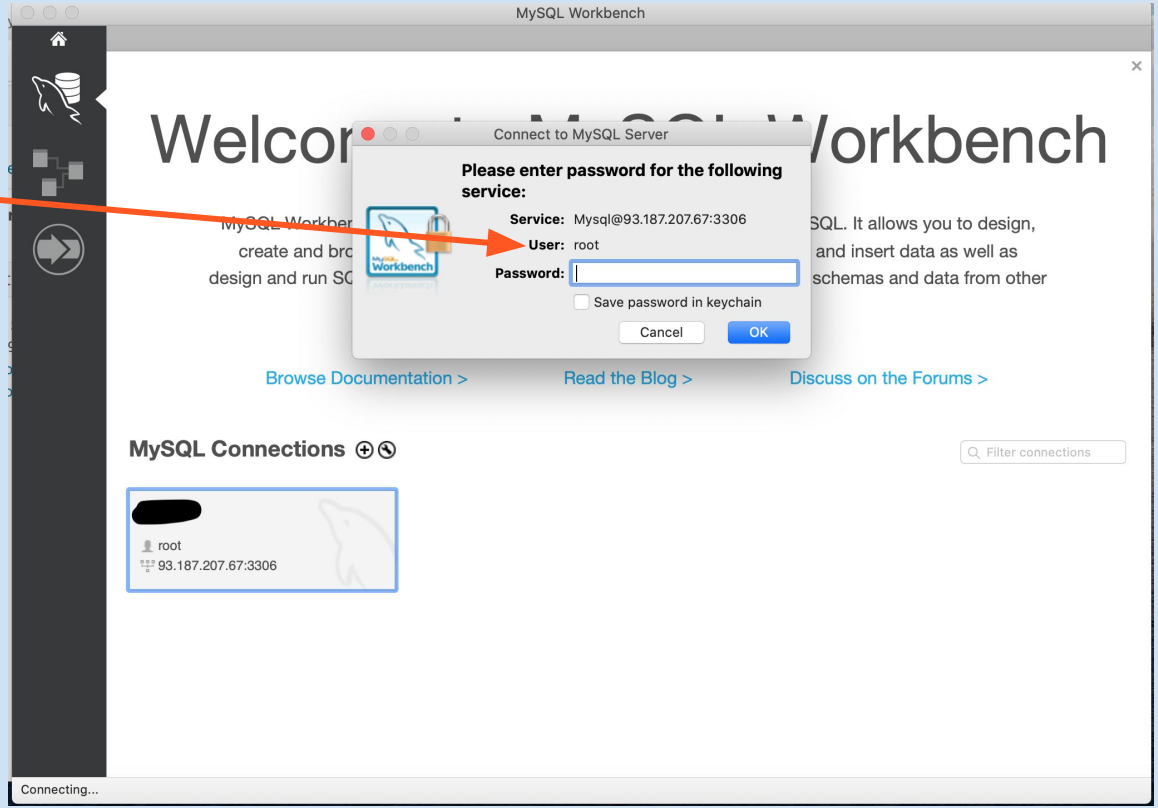
- Mobil telefonlardaki uygulamalardaki reklamlar virüs bulaştırabilir.
- Mobil telefonlarımızın ekran şifresi çok önemlidir.
- Günümüzde günlük yaşamımızdaki bir çok ihtiyacımızı ve işlemlerimizi mobil telefonlar ile karşılıyoruz. Her gün onlarca uygulama kullanıyoruz.
- En tehlikeli bilgi güvenliği riskleri ve açıklıkları mobil telefonlardadır.
- Mobil cihazlarımızı ortada bırakmamalıyız. Notebooklarımızı araç bagajında taşımalıyız.

# Halka açık ağlar

- Halka açık ağlar tehlikelidir.
- İzlenebilir, hırsızlık yapılabilir.
- Kopyalanabilir


# Uzaktan Erişim

- Sadece gerekli kişiler uzaktan erişmelidir.
- Sadece gerekli uygulama ve hizmetlere erişim sağlanmalıdır.
- Sadece güvenli bir VPN bağlantı yolu ile erişime izin verilmelidir.
- Mümkün olduğu durumlarda OTP/OAUTH şifreleme kullanılmalıdır..



# USB Bellek Kullanımı

- USB bellekler virüs bulaştırılması ve bilgi hırsızlığı için en ideal araçtır.
- USB bellekler çalınabilir.
- USB bellekler kolaylıkla arızalanabilir.
- En az ölçüde USB bellek kullanımı sağlanmalıdır.

# Kağıt öğütücü kullanımı

- Kişisel veri/gizli veri içeren dokümanları imha ederken kağıt öğütücü kullanmalıyız.
- Müsvedde yaptığımız kullanılmış dokümanları kontrol etmeliyiz.


# Depo ve Sevkiyat Güvenliği

- Depo ve sevkiyat güvenliği şirketimizin envanter kontrolününün sağlanması için çok önemlidir.
- Depo ve sevkiyat alanına görevliler dışında kimse izinsiz giremez.
- Girenler uyarılır ve Yönetici bilgilendirilir.

# Yazıcı kullanımı

- Doküman çıktılarını tam aldığımızı, eksik olmadığını kontrol etmeliyiz.
- Yazıcı hatası veya vazgeçme olabilir. Yine de gönderdiğimiz dokümanı iptal etmeli ve yazıcıdan basılmadığını kontrol etmeliyiz.
- Çıktının yazıcıda basılması anında cihazın başında bulunmalıyız.
- Yazıcıdan çıktıları alırken yanlışlıkla kendimize ait olmayan dokümanları almadığımızı kontrol etmeliyiz.

# Internet tehditleri

- Mutlaka adresi elle yazmalıyız.
- Reklamlardaki linklere dikkat etmeliyiz.
- Anahtar işaretine dikkat etmeliyiz.
- Kredi kartlarımızı bilmediğimiz sitelerde kullanmamalıyız.
- Banka kartlarımıza alışveriş limiti koymalı, SMS ile bilgilendirme istemeliyiz.
- Alışverişlerde 3D sistemini kullanmalıyız.

trendyol.com

hepsiburada

# Siber saldırı

# KVKK ve ISO 27001 Standardı İlişkisi

- ISO 27001 kurumsal bilgi varlıklarının kişilerden korunmasını ele alır.
- KVKK kişilerin verilerini bilgi varlığı olarak kabul eder. Kurumun bu varlıkları korumasını ele alır.
- ISO 27001 uygulamaları gönüllülük esasi ya da kurumsal tercihler ile belirlenir.
- KVKK uygulamaları zorunludur.
- Her ikisi de sistematik bir organizasyon gerektirir.
- Veri koruma açısından her ikisi de çok sayıda ortak önlem almayı gerektirir.
- ISO 27001 yasalara uyum gerektirir, KVKK ise yasanın kendisidir