

# SİBER GÜVENLİK VE ÇEVİRİMİÇİ GÜVENLİK

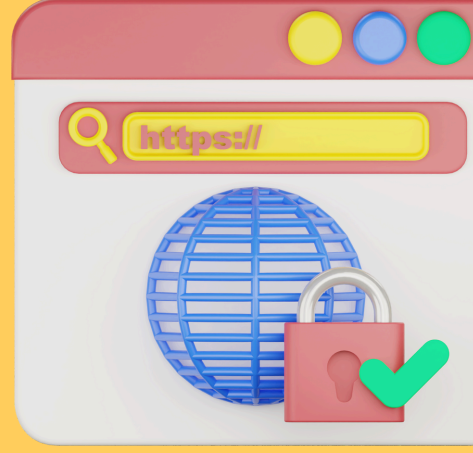
## Cihazınızı güvence altına alın



- Güvenlik açıklarını yamamak için işletim sisteminizi düzenli olarak güncelleyin.
- Güvenilir antivirüs yazılımı kullanın ve ekstra koruma için cihazınızın güvenlik duvarını etkinleştirin.
- Güçlü cihaz erişim kontrolleri kurun - özellikle cihazınızı başkaları kullanacaksa parmak izi tanıma veya güvenli bir parola kullanın.

## Çevrimiçi güvende kalın

- Daha güvenli gezinme için yaygın olarak tanınan ve güncel web tarayıcılarını kullanın.
- Uygulamaları yalnızca resmi uygulama mağazaları veya doğrulanmış geliştirici web siteleri gibi güvenilir kaynaklardan indirin.
- Bağlantınızın daha güvenli olduğu anlamına geldiği için web sitesi URL'lerinde https:// adresini kontrol edin.



## Bağlantınızı koruyun

- Halka açık veya güvenli olmayan Wi-Fi ağlarında hesaplara giriş yapmaktan veya kişisel bilgilerinizi paylaşmaktan kaçının.
- Her hesap için kolayca tahmin edilemeyecek güçlü, benzersiz parolalar kullanın ve bunları güvende tutmak için bir parola yöneticisi düşünün.



## Tehditleri tespit edin ve durdurun

- Virüs ve solucan gibi kötü amaçlı yazılımlar cihazınıza zarar verebilir veya verilerinizi çalabilir - güncel güvenlik araçlarıyla korunmaya devam edin.
- Beklenmedik e-postalar, spam veya pop-up reklamlara karşı dikkatli olun - bunlar genellikle dolandırıcılık veya kimlik avı girişimleri içerir.
- Bilinmeyen göndericilerden gelen mesajları veya ekleri açmayın. Şüpheye düştüğünüzde silin.



Daha fazla eğitim kaynağı için şu adresi ziyaret edin  
[digi-aware-elearninghub.com](https://digi-aware-elearninghub.com)