

# BU BÜLTEN HEM ETKİLİ VE VERİMLİ BİR ÇEVİRİM İÇİ ÖĞRENME DENEYİMİNİN SAĞLANMASI HEM DE GÜVENLİ BİR İNTERNET DENEYİMİ İÇİN ÖNERİ VE İPUÇLARINI KAPSAMAKTADIR.

KAYNAK: ÖRAV

Çevrim içi öğrenme ortamlarında başarılı olabilmek için öneriler Çevrim içi öğrenmenin iki önemli avantajı esneklik ve zaman uygunluğudur. Bu iki avantajın dikkatli bir şekilde kullanılmadığında bir dezavantaja dönüşebilir; motivasyonunuzun kaybolması, takip edememe, dikkat dağınılığı ve hedefe yabancılaşma ile sonuçlanabilir. Diğer bir deyişle çevrim içi öğrenme görüldüğünden çok daha zorlayıcı olabilir. Öğrenme modelleri örgün, uzaktan ya da çevrim içi olarak çeşitlenerek değişse de değişmeyen şeyler var aslında. Öğretinin ve öğrenenin sorumlulukları... Hangi modelde, hangi rolde yer alırsa alsın tarafların bu modelden yararlanması için bazı sorumlulukları üstlenmesi gerekiyor. Tabii sorumluluktan bahsediyorsak bu sorumlulukları yerine getirebilecek bazı becerilere de sahip olmak gerekiyor. İlk olarak hedefinize ulaşmaya ve başarmak için hazır olduğunuza emin olmanız gerekmektedir. Uzaktan öğrenme deneyimi ilk etapta kulağa heyecan verici gelse de bazı gerçeklerden haberdar olmakta fayda var. Bu gerçekliklerin en başında gelen şey çevrim içi öğrenme de en az yüz yüze öğrenme ortamları kadar enerji, çaba ve zaman gerektirdiğidir. Bunun yanında da bazı bilgisayar/internet bilgi ve becerileri de cabası. Ama en önemlisi kendi öğrenme sorumluluğunuzu almak. Eğer hazırsanız, başarınızı artıracak bazı önerileri şu şekilde sıralayabiliriz:

## TİCARET VE SANAYİ ODASI ORTAOKULU



### ÇEVİRİM İÇİ ÖĞRENME ORTAMLARINDA BAŞARILI OLABİLMEK İÇİN ÖNERİLER



## **GÜVENLİ BİR İNTERNET DENEYİMİ İÇİN 10 KRİTİK NOKTA**

KAYNAK: ÖRAV

Güvenli bir İnternet Deneyimi için 10 Kritik Nokta Artık hayatımızın her noktasında bulunan internet, üzerine bıraktığımız dijital ayak izlerimizi pek de silemediğimiz bir ağ olarak karşımıza çıkmaktadır. Her an yaşanan gelişmeler ile büyük bir hızla gelişen internet, hayatlarımıza kattığı kolaylıkların yanı sıra tehlikeleri ve riskleri de beraberinde getirmektedir. Bazen bilerek bazen de bilmeyerek yapabileceğimiz bazı hatalar istemediğimiz ve üzücü sonuçlara sebebiyet verebilmektedir. Elbette anti-virüs programları kullanmak gibi bazı güvenlik önlemleri olsa da bu içerikte sizlerle güvenli bir internet deneyimi için on kritik noktayı şu şekilde özetledik.



**BAZEN BİLEREK  
BAZEN DE  
BİLMEYEREK  
YAPABİLECEĞİMİZ  
BAZI HATALAR  
İSTEMEDİĞİMİZ VE  
ÜZÜCÜ SONUÇLARA  
SEBEBİYET  
VEREBİLMEKTEDİR.**



# 1. WEB ARAÇLARI ÜYELİKLERİ İÇİN AYRI BİR E-POSTA ADRESİ EDİNİN.

KAYNAK: ÖRAV

Eğitim için kullanabileceğiniz yüzlerce hatta binlerce web araçları mevcuttur. Bunların birçoğunu kullanabilmeniz için bir üyelik şartı istemektedir. Bu web araçlarının çoğunun ise güvenli olup olmadığını takip etmek de mümkün olmayabilir. O nedenle bu ve bu gibi durumlar için resmi ve kredi kartı işlemleri gibi ciddi işleriniz için kullandığınız kişisel e-posta adresiniz yerine, bu işler için aldığınız bir e-posta adresiniz olsun. Örneğin: Adınız Xxx olsun. O zaman şöyle bir adres alabilirsiniz:  
XXX\_web@gmail.com  
/x\_web@gmail.com ( adresler temsilidir.)



**EĞİTİM İÇİN  
KULLANABİLECEĞİNİ  
Z YÜZLERCE HATTA  
BİNLERCE WEB  
ARAÇLARI  
MEVCUTTUR.**



## **2. ÜYELİK İSTEYEN WEB SAYFALARINA SOSYAL MEDYA HESAPLARINIZLA ÜYE OLMAKTAN KAÇININ.**

KAYNAK: ÖRAV



**SOSYAL MEDYA  
HESAPLARINIZLA  
DEĞİL, E-POSTA  
ADRESİ YOLU İLE  
GELENEKSEL KAYIT  
İŞLEMİNİ TERCİH  
EDEREK GÜVENLİK  
İŞİNİ RISKE  
ATMAYINIZ.**

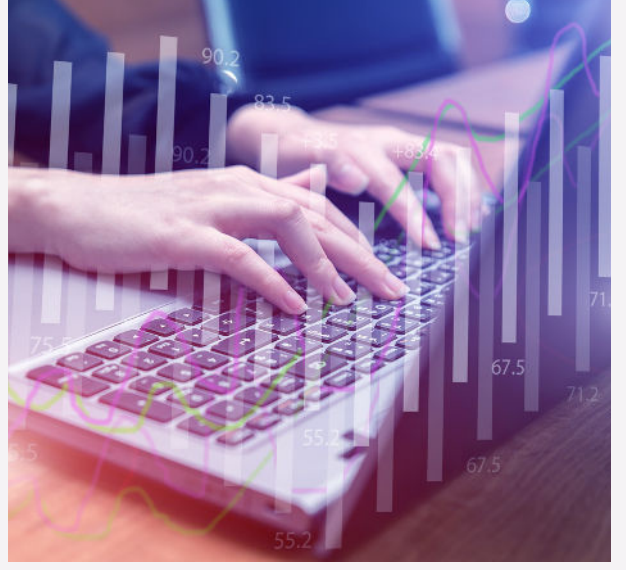
Bazı web siteleri üyelik isterken sizi uğraştırmamak için “sosyal medya hesaplarınızla bağlan” seçeğini sunar. Kayıt olmanızı kolaylaştıran bu işlem ile neleri kabul ettiğinizi bilmelisiniz. Hem sizin hem de arkadaşlarınızın güvenliğini riske atma ihtimalinizin olabileceğini bilerseniz sanırım bunu yapmazdınız. O nedenle, sosyal medya hesaplarınızla değil, e-posta adresi yolu ile geleneksel kayıt işlemini tercih ederek güvenlik işini riske atmayınız.



### **3. DOĞUM TARİHİ GİBİ KİŞİSEL BİLGİLERİNİZİ PAYLAŞMAMAYA ÇALIŞIN.**

KAYNAK: ÖRAV

Kişisel bilgileriniz sizin hakkınıza çok bilgi verir. Siber güvenlik açısından da bu verile oldukça önemlidir. Oluşabilecek güvenlik risklerini azaltmak istiyorsanız, kişisel bilgilerinizi nereye yazdığınıza çok ama çok dikkat edin.



**OLUŞABİLECEK  
GÜVENLİK  
RİSKLERİNİ  
AZALTMAK  
İSTİYORSANIZ,  
KİŞİSEL  
BİLGİLERİNİZİ  
NEREYE YAZDIĞINIZA  
ÇOK AMA ÇOK  
DİKKAT EDİN.**



## **4. ONLİNE ALIŞVERİŞ YAPIYORSANIZ: E-TİCARET SİTELERİNİN SSL SERTİFİKASININ BULUNMASINA DİKKAT EDİN.**

KAYNAK: ÖRAV

SSL Sertifikası, (Secure Sockets Layer), bir web sitesinin sunucusu ile kullanıcılar arasındaki veri akışını şifrelemeye yarayan bir protokoldür.



**DİKKAT!**



## **6. SOSYAL MEDYADA FOTOĞRAF PAYLAŞIRKEN EN AZ İKİ KERE DÜŞÜNÜN.**

KAYNAK: ÖRAV

Unutmayın ki dijital ayak izleriniz silinmez. Siz silseniz de siz göremeyebilirsiniz ama bu dijital ayak izlerinizin silindiği anlamına gelmez. O nedenle kendinizin ve özellikle de başkalarının fotoğraflarını paylaşırken çok dikkatli olun. Kişisel verileri koruma kanunundan haberdar olmakta fayda var.



**KİŞİSEL  
VERİLERİ  
KORUMA  
KANUNUNDAN  
HABERDAR  
OLMAKTA FAYDA  
VAR.**



## **5. GÜVENLİ BİR ŞİFRE VE ŞİFRELEME SİSTEMİ OLUŞTURUN.**

KAYNAK: ÖRAV

Belki de net bildiğiniz ama fazlaca sayıda şifre oluşturmanız gerektiği için en can sıkıcı güvenlik önlemlerinden biri olarak görünen konulardan birisi güvenli şifre oluşturmaktır. Bu konuda iki öneride bulunmak isteriz. Bunlardan ilki; risk seviyesi yüksek şifrelerinizde sayı, harf ve sembol kullanmayı ihmal etmeyin. İkinci öneri ise, web araçları üyelikleri için farklı şifrelemeler için bir sistem oluşturmanız. Örneğin: “Mutlu Güzel” arkadaşımız Kahoot aracına kayıt olacak. Bunu için şöyle bir şifreleme sistemi ile şifre oluşturabilir: MGkt74\* (sistem: ad soyad baş harfi büyük harflerle /aracın ilk ve son harfi küçük harflerle/memleketinin plakası/ yıldız sembolü) Aynı kişi diyelim facebook’a üye olacak, şifresi MGfk74\* olurdu. ( siz de kendinize uygun bir şifre sistemi oluşturarak şifre unutma sorunundan kurtulabilirsiniz.



**RİSK SEVİYESİ  
YÜKSEK  
ŞİFRELERİNİZDE  
SAYI, HARF VE  
SEMBOL  
KULLANMAYI İHMAL  
ETMEYİN.**





## **7. BANKA VE KREDİ KARTI BİLGİSİ GİRECEĞİNİZ SİTELERİN GÜVENLİK SERTİFİKASI OLMASINA DİKKAT EDİN.**

KAYNAK: ÖRAV



**UNUTMAYIN Kİ  
DİJİTAL AYAK  
İZLERİNİZ  
SİLİNMEZ.**

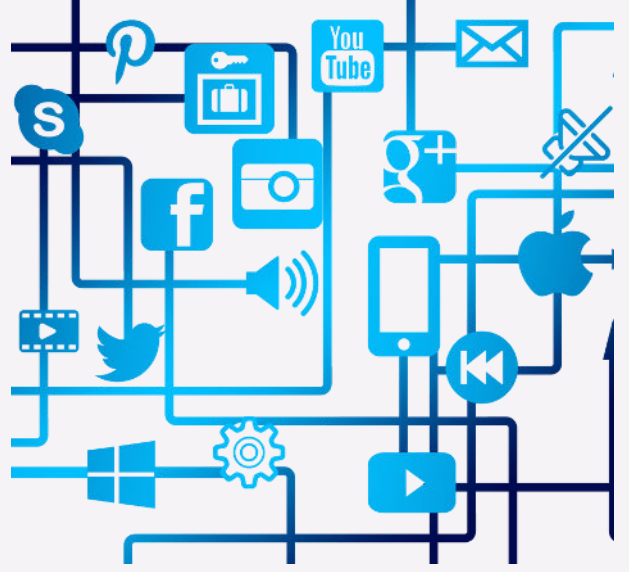
Banka ve kredi kartı bilgisi gireceğiniz sitelerin güvenlik sertifikası olmasına dikkat edin. Güvenlik değeri yüksek bilgilerinizi girmeniz gereken web sitelerin adres çubuğunda <https://..> ile başlamasına dikkat edin.



## TİCARET VE SANAYİ ODASI ORTAOKULU

### 8. GÜVENMEDİĞİNİZ KİŞİLERDEN GELEN E- POSTALARI AÇMAYIN/DOSYALARI İNDİRMEYİN.

KAYNAK: ÖRAV



**SOSYAL MEDYA  
HESAPLARINIZLA  
DEĞİL, E-POSTA  
ADRESİ YOLU İLE  
GELENEKSEL KAYIT  
İŞLEMİNİ TERCİH  
EDEREK GÜVENLİK  
İŞİNİ RISKE  
ATMAYINIZ.**

Sizi cezbeden ve hediye vaad edenler de dahil olmak üzere bu konuya dikkat edin.



## **9. EMİN OLMADIĞINIZ VE TEYİT EDİLMEMİŞ BİLGİLERİ PAYLAŞMAYIN.**

KAYNAK: ÖRAV



**İNTERNET  
KURALLARI  
BELİRLEYİN VE  
BUNLARA ÖNCE SİZ  
UYUN.**

Bu sadece sizin değil, başkalarının da güvenliğine saygı duymayı gerektiren etik bir kuraldır.



## **10. ŞU SÖZÜ HEP AKLINIZDA TUTUN:**

KAYNAK: ÖRAV

Eğer bir ürüne para  
ödemiyorsanız asıl  
ürün sizsiniz.”

GÖRSEL KAYNAK:  
Pixabay



**ÇOCUK PROFİLİ İLE  
ERİŞEBİLECEĞİNİZ  
TÜM SİTELER  
UZMAN  
KONTROLÜNDEN  
GEÇMİŞ BELİRLİ  
KRİTERLERE GÖRE  
ONAYLANMIŞ  
SİTELERDİR.**



# GÜVENLİ İNTERNET HİZMETİ

KAYNAK:Başvuru - GüvenliNet  
(guvenlinet.org.tr)

Aİle Profilini seçerek müstehcenlik, şiddet, ırkçılık,kumar gibi yasadışı ve zararlı içerikleri barındıran siteler; Sağlık Bakanlığı'nın zararlı olduğunu açıkladığı ürünlerin siteleri ve dolandırıcılık sitelerinin önüne geçmiş olursunuz.

**TİCARET VE SANAYİ ODASI  
ORTAOKULU**



**GÜVENLİ İNTERNET  
HİZMETİ :  
ÜCRETSİZDİR.  
KOLAYDIR,  
ABONELİK BİR  
KISA MESAJ(SMS)  
İLE MÜMKÜNDÜR  
VE PROGRAM  
KURMAYA GEREK  
YOKTUR.**



**HAZIRLAYAN:  
ŞÜKRAN KOCABEY TİRYAKİ**

OCAK 2023