



SOSYAL MEDYA KULANIMI

KUMLUCA KIZ ANADOLU İMAM HATİP LİSESİ

2022-2023 EĞİTİM ÖĞRETİM YILI



GİRİŞ

Hayatlarımızı devasa bir bilgi ağının içinde sürdürüyoruz. Dijital ortamda kurulan cümlelerin, yapılan ticaretin, oluşturulmaya çalışılan algının ve nihayetinde kurulmak istenen hegemonyanın hakim olduğu bir süreci yaşıyoruz. Mesele çok açık. İletişim araçları geliştikçe, iletişim kurmak zahmetsiz bir hale geldikçe ve buna dayalı teknolojiler ilerledikçe insanoğlu daha önce hayal bile edilemeyen bir tecrübeyi yaşayarak öğrenmeye başladı.

Vazgeçilmez bir parçamız olan sosyal medya araçlarının; kişiliğimizin, yaşam biçimimizin, ailelerimiz ile olan ilişkilerimizin ve devlet yönetimlerinin belirlenmesinde etkili araçlar haline gelmesi aynı zamanda hayati bir riski de beraberinde getiriyor. Her gün, her saat, her dakika ve her saniye yeni bir bilginin ortaya dökülmesi, var olan bilginin yeniden üretilmesi, oluşan bu “büyük veri”nin (big data) iyi veya kötü niyetli yaklaşımlarca kullanılması bu mecraların nasıl doğru kullanılabileceği gibi bir soruyu ortaya çıkarıyor.

ACABA???

- Sosyal medya mecralarını doğru kullanabiliyor muyuz?
- Biz mi sosyal medyayı kullanıyoruz, yoksa o mu bizi şekillendiriyor?
- Seçtiklerimiz gerçekten bizim tercihlerimiz mi?

- Sosyal medya her türlü manipölasyona açık ve kişisel **bilgi güvenliğı açısından birbirinden farklı** tartışmalara sahne olan bir ortamdır.

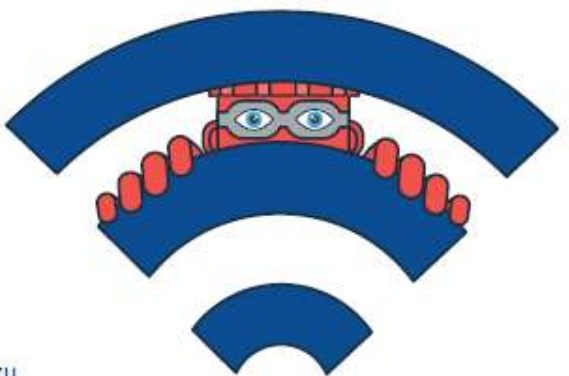
- Sosyal paylaşım ağlarına üye olan herkesin risk altında olabileceğini göz ardı etmemesi önemlidir. Zira kullanıcıların kabul ettiğı **hizmet sözleşmelerinde bilgilerin reklam amaçlı bir şekilde paylaşılabileceğı belirtilmektedir.**

- Sosyal medyadaki denetimsizlikten kaynaklanan **bilgi kirliliğı had safhada olduğı için** sahte sosyal sorumluluk kampanyaları gerçekleştirilebilmektedir.
 - **Örnek:** Geçmişte ölkemizde de maddi sıkıntı çeken öğrenci ve hasta adına para toplama gibi sahte sosyal sorumluluk kampanyaları yürütöldüğü bilinmektedir.



- Sosyal medyanın ücretsiz bir şekilde hizmet sunması ise **kullanıcıyı ürün durumuna getirebilmektedir**. Yani kullanıcıların bilgilerine istem dışı erişilebilir.

BİR ÜRÜNE PARA ÖDEMİYORSANIZ ÜRÜN SİZSİNİZDİR!



- Sosyal medyada bilgilerin paylaşılması esnasında dikkatli olunmalıdır. **Kişisel mahremiyet gözetilmeli, özel bilgiler, gidilen yerler, aile üyelerine yönelik içerikler mecbur kalınmadıkça paylaşılmamalıdır.**

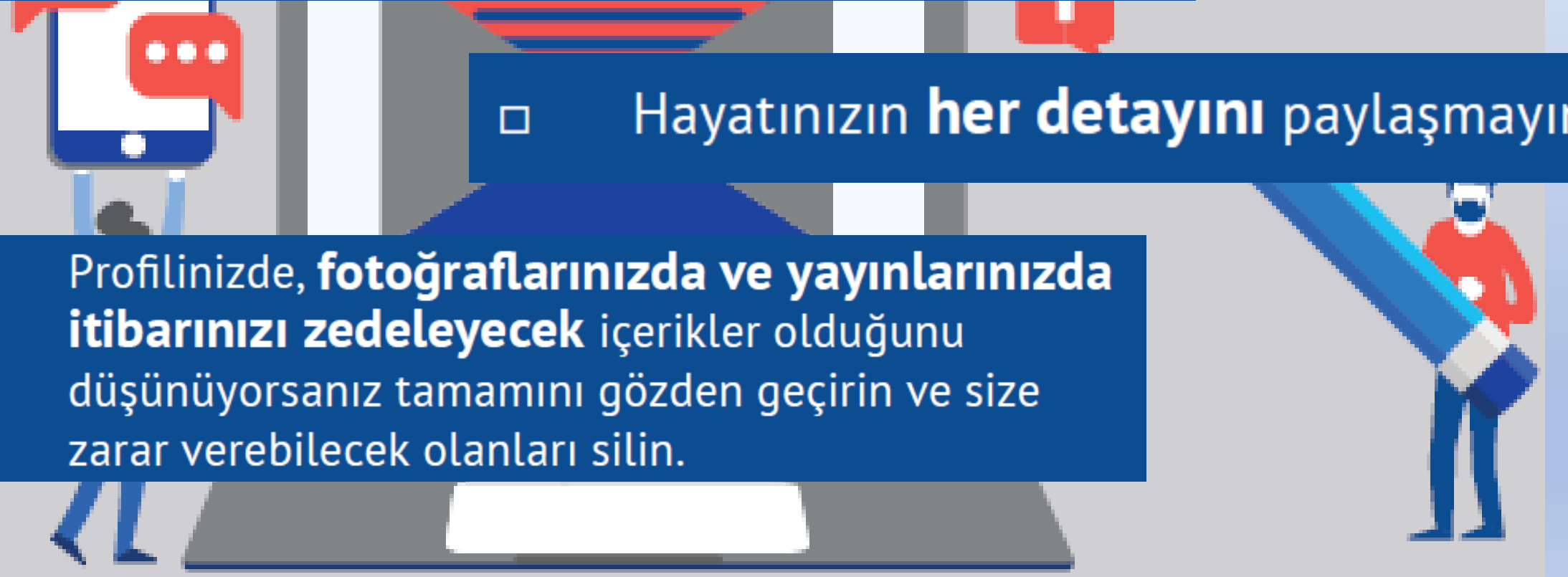
NELERE DİKKAT EDELİM?



- İnternetin gerçekte ne olduğunu unutmayın: devasa bir kayıt defteri. **Web'de yayınlanan hiçbir şeyin aslında silinemediğini** ve kişisel bilgilerinize ne kadar hızlı ve kolay bir şekilde erişilebileceğini aklınızdan çıkarmayın.

- Hayatınızın **her detayını** paylaşmayın.

- Profilinizde, **fotoğraflarınızda ve yayınlarınızda itibarınızı zedeleyecek** içerikler olduğunu düşünüyorsanız tamamını gözden geçirin ve size zarar verebilecek olanları silin.





☐ Şifrenizi kimseyle **paylaşmayın.**

☐ Yalnızca **tanıdığınız kişilerin** arkadaşlık isteklerini kabul edin.

☐ Ebeveynlerinizin, öğretmenlerinizin veya diğer büyüklerinizin **görmesini istemediğiniz** hiçbir şeyi paylaşmayın.

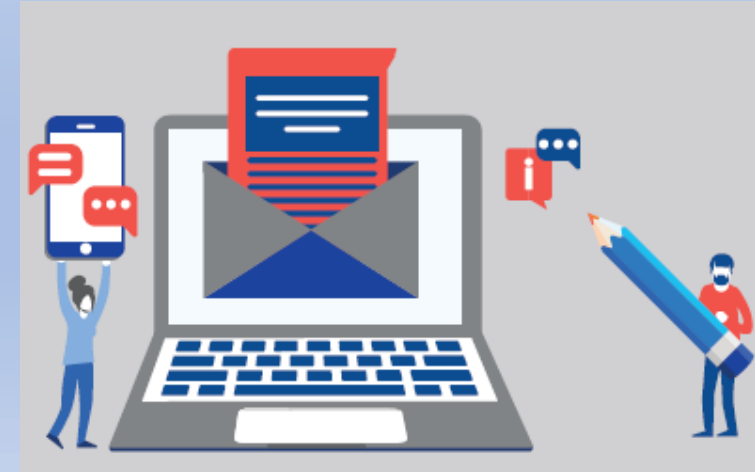
☐ **Gerçek** olun.

☐ Gizlilik ayarları hakkında bilgi edinin, kullandığınız sosyal ağların **gizlilik ayarlarını okuyun** ve bunları sık sık inceleyin.

- Çevrimiçi olarak söylediğiniz ve yaptığınız **her şey dijital ayak iziniz olarak internette ebediyyen kalacaktır.** Bu yüzden itibarınıza dikkat edin.

- Çevrimiçi olarak hoşunuza gitmeyen veya sizi **rahatsız eden bir durumla karşılaşırsanız,** bilgisayarınızı kapatın ve bir yetişkine anlatın.

- Paylaştığınız fotoğrafların artık yeni teknolojiler sayesinde **bozulabileceği ve değiştirilebileceğini** unutmayın. O yüzden paylaşacağınız fotoğrafı iyi seçin.



- Arkadařlarınızın kiřisel bilgilerine de zen gsterin. İzin almadan fotoğraf etiketlemeyin. Kiřisel bilgilerini dnyayla paylařmayın. **Herkesin mahremiyet hakkı vardır** ve bunu korumak sizin sorumluluęunuzdadır.



- evrimii ortamlarda tanıştıęınız hikimseye gvenmeyin. Hatta arkadaşlarınız tarafından onlara ait olduęu **onaylanmamıř ama arkadaşınız mıř gibi grnen sahte hesaplara** řphe ile yaklařın.

- Sizi evrimdiřı bulmak iin kullanılabilecek bilgileri yayınlamayın, ebeveyninize ait aracın plakasını ieren bir fotoğraf paylařmayın, her gn eve giderken kullandıęınız yol hakkında **ipuları ierecek bilgiler vermeyin**, hibir řekilde ev adresinizi paylařmayın.

- Lokasyon bazlı **paylaşımlar** yapmayın.

- Sizi taciz eden veya rahatsız hissettiren mesajlara cevap vermeyin! **Gerçekten cevap vermeyi isterseniz bile, siber zorbaların tam olarak istediğinin sizden etkileşim almak olduğunu unutmayın.** Kontrolü kaybetmeyin.

- Zorbaları **engelleyin.**

- İnsanlar sosyal mecralarda **göründüğü gibi değildir.** Kimseye güvenmeyin.



SOSYAL MEDYA HESABININ GÜVENLİĞİ





- Sosyal medyada kişisel verileri korumak adına şifre ve hesap güvenliği önemlidir.

- Kafeterya, alışveriş merkezleri, oteller, restoranlar gibi kamuya açık internet bağlantısı sunan mekânlardaki kablosuz ağ noktaları bazen sosyal medya ile erişim izni verir. Bu durum bazı güvenlik sorunlarını beraberinde getirebilir.

- Uygulama mağazalarından indirilen bazı uygulamalar sosyal medya hesaplarıyla erişim izni isteyebilir, bu işlem gerçekleştirilmediği takdirde uygulama kilitlenir. Bu uygulamaların dönem dönem kişisel verileri izinsiz bir şekilde kullandığı görülmüştür.

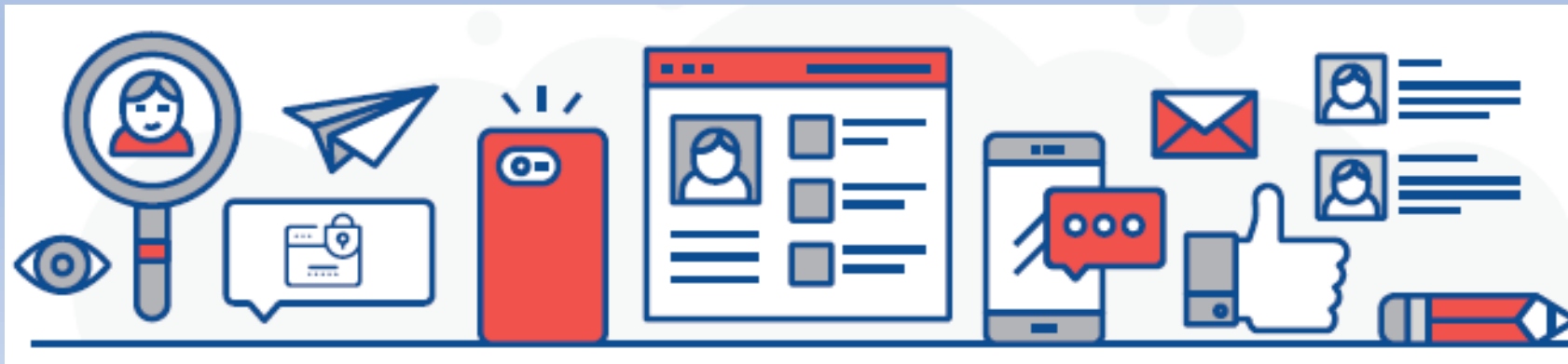
- Üçüncül parti uygulamalara erişim izni verildiğinde kişi adına beğeniler, paylaşımlar gerçekleştirilebilir, hesaplar otomatik olarak bir havuza dahil edilip istenmeyen hesaplar takibe alınabilir.

- Kullanıcılar hızlı bir şekilde uygulamaları kullanıp giriş yapmak istediği için nelere izin verip vermediğine dikkat etmeyebilir. Kullanıcı sözleşmeleri okunmalıdır.

- Sosyal medyada büyük küçük harf, özel karakter ve rakamlardan oluşan uzun parolalar oluşturmak, çift faktörlü koruma seçeneğini aktif hale getirmek, şüpheli durumlar ve erişimler için güvenlik SMS bildirimlerini açık tutmak güvenliğinizi maksimum seviyeye ulaştıracaktır.

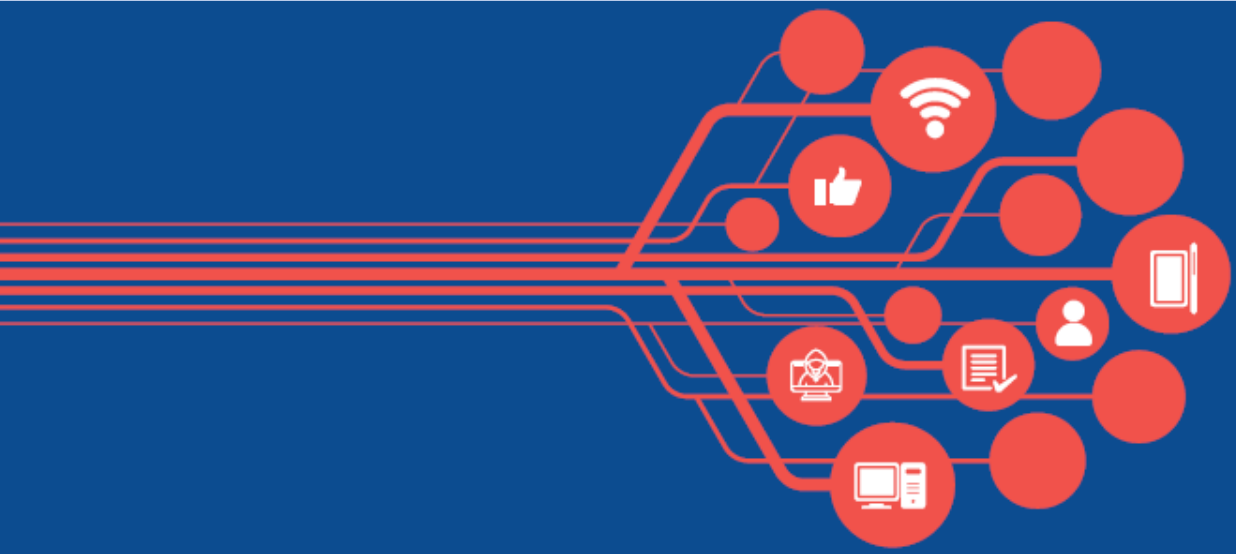
- Kurtarma e-postası ve telefon numarası kullanmanız hesabınızın başkaları tarafından ele geçirilmesini engelleyecektir.

- ❑ Sosyal medyada %100 güvenlik söz konusu değildir. Bu nedenle kişisel ve mahrem bilgilerin dijital ortamda paylaşılmaması, görsellerin ve içeriklerin aktarılmaması art niyetli kişilere ve siber saldırganlara karşı alınabilecek kişisel önlemlerdir. Düzenli periyodlarla şifrelerin değiştirilmesi ve güncellenmesi gerekir.



SOSYAL MEDYADA VERİ GÜVENLİĞİ

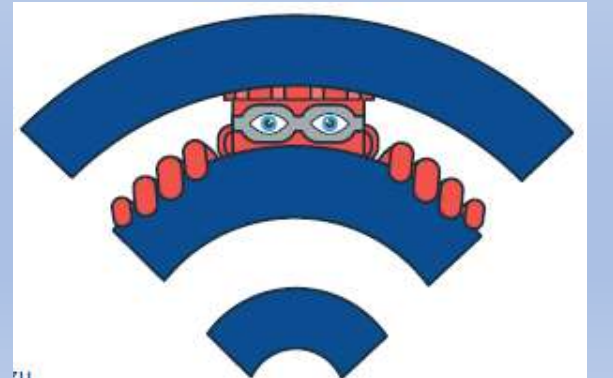
- KİŞİSEL VERİLERİN KORUNMASI



- Sosyal medyada **kişisel verileri korumak** oldukça zordur.

- Siber saldırganlar, **sanal korsanlar kullanıcıların güvenliğini tehdit etmekte**, bu durum telafisi imkânsız zararlara sebebiyet verebilmektedir.

- Sosyal medyada biyografik bilgilerin tümünün paylaşılması, özel bilgilerin eksiksiz bir şekilde doldurulması, **gizlilik ayarlarının gerektiği gibi yapılandırılmaması** veri güvenliği açısından tehdit oluşturabilmektedir.



- Sosyal medyada izin verilen üçüncül parti uygulamalar **veri güvenliğini tehdit etmekte**, bu durum kullanıcıların mağduriyet yaşamasına sebebiyet vermektedir.



Sosyal medya hesap ayarlarından uygulamalar sekmesine girerek izin verilen üçüncül parti uygulamaları görebilir ve izinleri geri alabilirsiniz!

- Sosyal medyada veri güvenliğinin sağlanabilmesi için **siber güvenlik alanında** bilgi birikimine sahip olmak gerekmektedir.

- Sosyal medya kullanıcılarının **gizlilik ayarları konusunda kendisini geliştirmesi** ve veri güvenliği konusunda gereken sorumluluğu üstlenmesi önemlidir.

KAYNAKÇA

- «Sosyal Medya Kullanım Kılavuzu», Cumhurbaşkanlığı İletişim Başkanlığı, 2020
- Güvenli İnternet Merkezi (www.gim.org.tr ve www.guvenliweb.org.tr) youtube kanalı, <https://www.youtube.com/watch?v=FHyDACGOQIY> (Sosyal Medya Platformlarında Dikkat Edilmesi Gerekenler)/<https://www.youtube.com/watch?v=yt2hFRK499Q> (Güvenli Sosyal Medya Kullanımının Altın Kuralları)

