

Sosyal Medya Çalışma Soruları ve Cevapları

2.1. Etik ve Bilişim Etiği

1. **Bilişim temel hak ve özgürlükleri** → İfade özgürlüğü, bilgiye erişim hakkı, özel hayatın gizliliği.
 2. **Kişisel verilerin korunması** → Bireyin mahremiyetini ve güvenliğini sağlamak için bilişim etiğinin parçasıdır.
 3. **Sosyal medya etiğinde saygı** → Başkalarının görüşlerine, kimliğine ve özel hayatına zarar vermemek.
 4. **İnternet etiği vs medya etiği** → İnternet etiği küresel, hızlı ve anonim ortamda geçerlidir; medya etiği daha sınırlıdır.
 5. **Bilişim etiği ihlali örneği** → Korsan yazılım kullanmak, sahte haber yaymak.
 6. **Yanlış bilgi paylaşımı** → Toplumsal kargaşa, güven kaybı, hukuki sorumluluk doğurur.
 7. **Anonimlik sorunları** → Kimlik gizleme ile hakaret, dolandırıcılık, siber zorbalık artabilir.
 8. **Erişim hakkı** → Her bireyin bilgiye ve internete eşit şekilde ulaşabilmesi.
 9. **Nefret söylemi** → Sosyal medya etiğinde etik dışı ve hukuka aykırı kabul edilir.
 10. **Telif hakları** → İnternet etiğinde içerik üreticisinin emeğini korur.
-

2.2. Bilgi Güvenliği ve Hukuki Kurallar

11. **Bilgi güvenliği önemi** → Bilgi çağında en değerli varlık bilgidir; korunmazsa zarar oluşur.
12. **CIA üçlüsü** → Confidentiality (Gizlilik), Integrity (Bütünlük), Availability (Erişilebilirlik).
13. **Hukuki kurallar ilişkisi** → Bilgi güvenliği ihlallerine yaptırım uygular, düzen sağlar.
14. **KVKK amacı** → Kişisel verilerin işlenmesini düzenlemek ve bireyleri korumak.
15. **İhlal sonuçları** → Para cezası, hapis cezası, itibar kaybı.
16. **Hukuki kurallar olmadan** → Güvenlik sağlanamaz; yaptırım eksikliği ihlalleri artırır.

17. **Gizlilik** → Bilginin sadece yetkili kişilerce erişilebilir olması.
 18. **Sosyal medya sorumlulukları** → Hakaret, iftira, yasa dışı içerik paylaşımı hukuki sorumluluk doğurur.
 19. **Bilgi güvenliği politikaları** → Kurum içi kurallar, şifre politikaları, erişim yetkileri.
 20. **Hak arama yolları** → Mahkemeye başvuru, BTK, KVKK kurumu.
-

2.3. Siber Zorbalık

21. **Tanım** → İnternet ortamında bireylere zarar vermek amacıyla yapılan saldırgan davranışlar.
 22. **Yaygın türler** → Hakaret, tehdit, iftira, özel bilgileri ifşa etme.
 23. **Farkı** → Geleneksel zorbalık fiziksel ortamda, siber zorbalık dijital ortamda gerçekleşir.
 24. **Psikolojik etkiler** → Kaygı, depresyon, özgüven kaybı.
 25. **Örnekler** → Sosyal medyada alay etmek, sahte hesap açmak.
 26. **Kimlik gizleme rolü** → Zorbaların kendini gizleyerek daha rahat saldırması.
 27. **Ailelerin rolü** → Çocukları bilinçlendirmek, destek olmak, iletişim kurmak.
 28. **Okulların sorumluluğu** → Eğitim vermek, rehberlik sağlamak, disiplin önlemleri almak.
 29. **Hukuki yollar** → Savcılığa suç duyurusu, mahkemeye başvuru.
 30. **Uluslararası düzenlemeler** → Avrupa Birliği Dijital Hizmetler Yasası, ABD’de siber suç yasaları.
-

2.3.1. Güvenlik Yazılımları

31. **Antivirüs işlevi** → Virüsleri tespit edip silmek.
32. **Firewall işlevi** → Yetkisiz erişimleri engellemek.
33. **Antispyware işlevi** → Casus yazılımları engellemek.
34. **Güncel tutma önemi** → Yeni tehditlere karşı koruma sağlar.
35. **Sınırlılıkları** → %100 koruma sağlamaz, kullanıcı hatalarını engelleyemez.

- 36. **Mobil örnekler** → Avast Mobile, Kaspersky Mobile.
 - 37. **Politikalarla ilişkisi** → Yazılımlar güvenlik politikalarının teknik ayağını oluşturur.
 - 38. **Kullanıcı alışkanlıkları** → Güvenlik yazılımı olsa bile bilinçsiz kullanım risk yaratır.
-

2.3.2. Siber Zorbalıktan Korunma Yöntemleri

- 39. **Güçlü şifre önemi** → Hesapların ele geçirilmesini zorlaştırır.
 - 40. **Bilinçli paylaşım** → Kişisel bilgileri sınırlı ve dikkatli paylaşmak.
-