

12. SINIF ETKİNLİKLERİ

FARK ET VE GÜVENLİĞİNİ SAĞLA

Gelişim Alanı	Sosyal Duygusal
Yeterlik Alanı	Kişisel Güvenliğini Sağlama
Kazanım/Hafta	Bilişim teknolojileri kullanımı konusunda kendini değerlendirir. / 5. Hafta
Sınıf Düzeyi	12. Sınıf
Süre	40 dk (Bir ders saati)
Araç-Gereçler	<ol style="list-style-type: none">1. Çalışma Yaprağı-12. Çalışma Yaprağı-23. Çalışma Yaprağı-34. Çalışma Yaprağı-45. Çalışma Yaprağı-56. Çalışma Yaprağı-67. Çalışma Yaprağı-78. 7 tane küçük not kâğıdı9. Kutu/torba
Uygulayıcı İçin Ön Hazırlık	<ol style="list-style-type: none">1. Küçük not kâğıtlarına ayrı ayrı 1'den 7'ye kadar sayılar yazılır ve kutu/torbanın içine atılır.2. Çalışma Yaprağı-1, Çalışma Yaprağı-2, Çalışma Yaprağı-3, Çalışma Yaprağı-4, Çalışma Yaprağı-5, Çalışma Yaprağı-6 ve Çalışma Yaprağı-7 birer adet çoğaltılır.3. Etkinlik Bilgi Notu önceden okunarak hazırlık yapılır.
Süreç (Uygulama Basamakları)	<ol style="list-style-type: none">1. Etkinliğin amacının bilişim teknolojileri kullanımı konusunda öğrencilerin kendilerini değerlendirmesi olduğu açıklanır.2. Öğrencilere aşağıdaki açıklama yapılarak süreç başlatılır: "Bugün sizinle bilişim teknolojileri kullanımı, karşılaşılabilecek riskler ve siber güvenlik ile ilgili bir etkinlik yapacağız. Etkinliğimize gruplara ayrılarak başlayacağız."3. Öğrenciler 7 gruba ayrılır. Her gruptan bir öğrencinin kutu/torbanın içinden bir kâğıt seçmesi istenir. Seçilen kâğıtta yer alan sayıya uygun çalışma yaprağı gruplara verilir. Örneğin kutu/torbadan 1 numarasını çeken gruba Çalışma Yaprağı-1 verilir.4. Gruplardan kendilerine denk gelen çalışma yaprağındaki ilgili bölümlere

Süreç (Uygulama Basamakları)

ilişkin bilgileri doldurmaları istenir.

5. Sonra her grup tamamlamış olduğu çalışma yaprağını diğer gruba verir. Bu döngü, çalışma yaprakları tüm gruplara ulaştığında tamamlanır.
6. Sonrasında grup sözcüleri tarafından çalışma yaprağına yazılanlar sınıfla paylaşılır.
7. Süreç aşağıdaki tartışma soruları kapsamında değerlendirilir:
 - Bu bilişim etkinliklerine ne kadar zaman ayırıyorsunuz?
 - Bu bilişim etkinliklerinin sana hangi faydalarının olduğunu düşünüyorsun?
 - Güvenli buluyor musun?
 - Daha güvenli olması için neler yapabilirsin?
 - Bilişim suçları hakkında neler biliyorsun?
 - Siber dünyada karşılaşılabilecek tehlikeler nelerdir?
 - Bu tehlikelere karşı alınabilecek önlemler neler olabilir?
8. Öğrencilerin paylaşımları alındıktan sonra Etkinlik Bilgi Notundan yararlanarak aşağıdakine benzer bir açıklama ile süreç sonlandırılır:

"Sevgili öğrenciler, bilişim teknolojilerinde karşılaşılan güvenlik problemlerini ve çözüm yollarını ifade ederek etkinliği sonlandırır."

Kazanımın Değerlendirilmesi

Öğrencilerin gelecek haftaya kadar bilişim teknolojilerini kullanırken alabilecekleri ek güvenlik tedbirleri hakkında araştırma yaparak (uzmanlarla görüşme, dergi, gazete, bilimsel makaleler v.b.) bunlara kendilerinin ne derece dikkat ettiklerini de içeren bir sunum yapmaları istenir.

Uygulayıcıya Not:

1. Öğrencilerin bilişim teknolojileri kullanımı konusunda kendini değerlendirmeleri sağlanırken karşılaşılabilecekleri riskler, alınabilecek önlemler konusunda farkındalık yaratmaya çalışılır.
2. Öğrenciler kullanım alanları ve sıklıkları konusunda emin olmadıklarını söyleyebilir. Cep telefonu uygulamaları, kullanıcının hangi uygulamayı ne kadar sıklıkta, hangi saatlerde kullandığına dair bilgi veriyor. Oradan yardım alabilirler.
3. Sınıfın iç mekânı uygunsa etkinlik çalışma yaprakları sınıf duvarlarına asılması, öğrencilerin gruplar hâlinde sınıfta dolaşarak her bir istasyonda durması şeklinde de yapılabilir.

Özel gereksinimli öğrenciler için;

1. Gruplar oluşturulurken uygun akran eşleştirmesi yapılarak sosyal çevre düzenlenebilir.
2. Tartışma soruları basitleştirilerek öğrenme süreci farklılaştırılabilir.

Etkinliği Geliştiren:

Güller SEZGİN

ETKİNLİK BİLGİ NOTU

Siber güvenlik: bilgisayarları, sunucuları, mobil cihazları, elektronik sistemleri, ağları ve verileri kötü amaçlı saldırılardan koruma uygulamasıdır.

Siber zorbalık: başka bir kişiyi taciz ya da tehdit etmek, utandırmak veya hedef almak için teknolojik platformların kullanımınıdır. Siber zorbalık tanımı gereği genç insanlar arasında gerçekleşir. Bir yetişkin söz konusu olduğunda buna siber taciz ya da siber saldırı denir ve bu, hukuki sonuçlara yol açabilecek ve hapis cezası gerektirebilecek bir suçtur.

Siber dünyada karşılaşılabilecek tehlikeler;

Uyumsuz içerikler: Pornografik içeriklerin yanında şiddet içerikli ve madde bağımlılığına özendirilen görsel ve videolar, çocukların istemeden de olsa karşılaşılabileceği içerikler olarak internette yoğun şekilde bulunuyor.

İstenmeyen iletişim: Siber zorbalık ve cinsel istismar olarak iki çeşidi olan istenmeyen iletişim ile çocuklar mesajlar ve e-postalarla ya hakarete uğruyor ya da cinsel olarak istismar edilmeye çalışılıyor.

Pazarlama ve reklam istismarı: İnternet üzerinde birçok ilgi çekici reklam mevcut. Bu reklamlarla kişisel bilgilerini veren çocuklara yönelik çöpçatanlık ve kumar siteleri gibi yerlerden uygunsuz içerikler ve reklamlar da paylaşılabilir.

Gizli web tehditleri: Zararlı yazılımlar, casus yazılımlar, virüsler, fidye yazılımları gibi birçok tehdit, bunlardan kaçınma yöntemlerini bilmeyen çocukları tehdit ediyor.

Bu tehlikelere karşı alınabilecek önlemler;

Lisanslı ürün kullanımı, sistem güncellemelerinin gününde yapılması, farklı karakterleri barındıran parola ve şifrelerin kullanılması ve kaynağı bilinmeyen bağlantıların açılmaması siber güvenlik açısından önemlidir.

Çalışma Yaprağı 1

OYUN



UYGULAMALAR	
RİSKLER	
GÜVENLİK TEDBİRLERİ	

Çalışma Yapağı 2

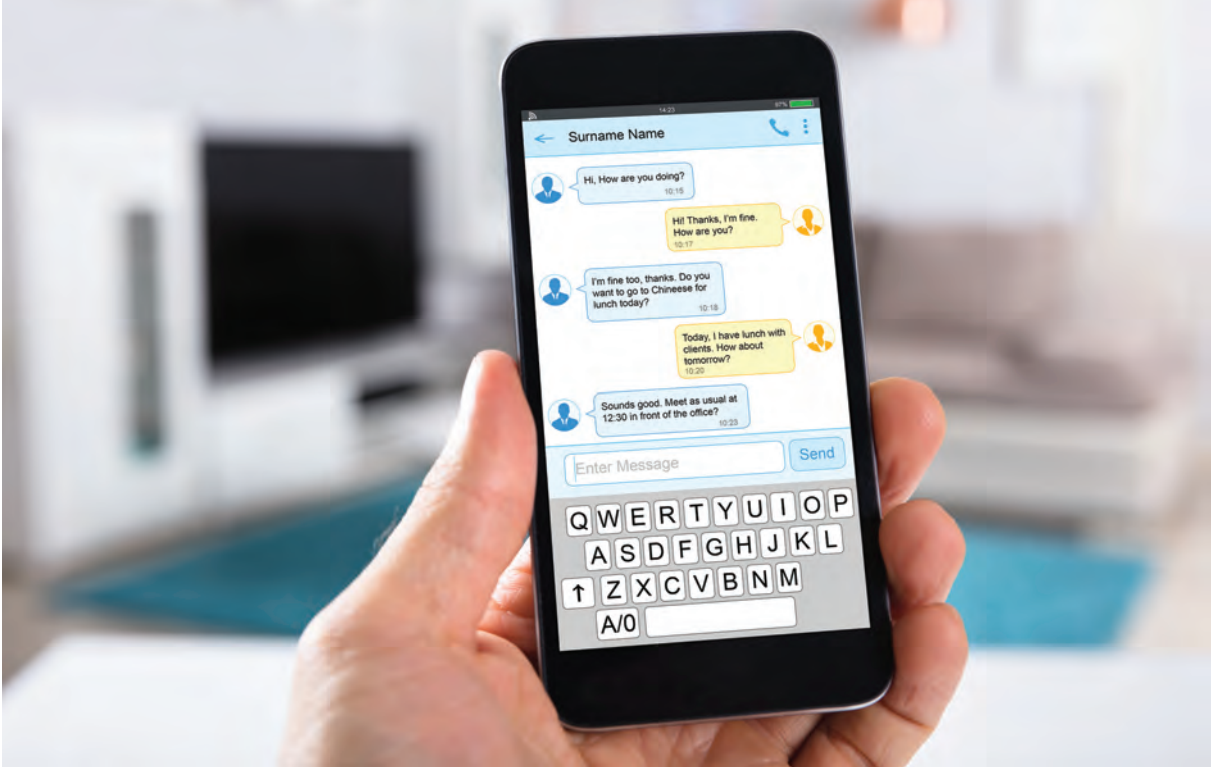
SOSYAL MEDYA



UYGULAMALAR	
RİSKLER	
GÜVENLİK TEDBİRLERİ	

Çalışma Yaprağı 3

MESAJLAŞMA UYGULAMALARI



UYGULAMALAR	
RİSKLER	
GÜVENLİK TEDBİRLERİ	

Çalışma Yapağı 4

DİZİ-FİLM



UYGULAMALAR	
RİSKLER	
GÜVENLİK TEDBİRLERİ	

Çalışma Yaprağı 5

VIDEO İZLEME UYGULAMALARI



UYGULAMALAR	
RİSKLER	
GÜVENLİK TEDBİRLERİ	

Çalışma Yapağı 6

SESLİ-YAZILI İLETİŞİM PROGRAMLARI



UYGULAMALAR	
RİSKLER	
GÜVENLİK TEDBİRLERİ	

Çalışma Yaprağı 7

YAZILIM



UYGULAMALAR	
RİSKLER	
GÜVENLİK TEDBİRLERİ	