

Ders planı

2023-1-SK01-KA220-SCH-00015112



Başlık	Güvenlik ve teknoloji	
Blok adı	<i>Dünyanızı güvence altına alın – güvenli çevrimiçi davranış için bir uygulama</i>	
Yaş kategorisi	Süre	Ders saati sayısı
13 – 15	135 dakika	3
Öğrenci merkezli eğitim hedefleri (içerik ve performans standartları)		
İçerik standardı:		
Güvenli çevrimiçi davranışın ilkeleri.		
Kişisel verilerin korunmasının temelleri, dolandırıcılık, sahtekarlıklar.		
Performans standardı:		
Siber güvenlik konusunda eğitim veren bir uygulama tasarlayın.		
Tehditleri ve korunma yollarını belirleyin.		
Çözümün faydaları üzerinde işbirliği yapın ve düşünün.		
Derslerin bütünleştirilmesi:		
Bilişim,		
Vatandaşlık eğitimi,		
Slovak dili		
21. yüzyıl becerileri:		
Eleştirel düşünme,		

Dijital okuryazarlık,
İşbirliği

Didaktik araçlar ve öğretim teknikleri:

İnternet bağlantılı bilgisayarlar,
MIT uygulama mucidi,
Canva,
Cep telefonları

Referanslar / Kaynaklar (videolar, metodolojiler):

<https://appinventor.mit.edu>

Motivasyon aşaması:

Süre: 40 dakika

"Çevrimiçi güvenliği unutursak ne olabilir?"

Tanıtım videosu ve tartışmalar:

Öğretmen İnternet Güvenliği videosunu gösterecek

İzlemenin ardından en yaygın internet tehditleri hakkında moderatörlü bir tartışma yapılıyor; öğrenciler sahte profiller, sahte e-postalar veya güvenli olmayan web siteleri ile ilgili kişisel deneyimlerini paylaşıyorlar.

Öğretmen tahtaya anahtar kelimeleri yazar: şifre, kimlik avı, virüs, siber zorbalık, çerezler, dijital ayak izi.

Grup etkinliği – “Eğer...” olsaydı ne olurdu?

Gruplar, riskli durumları (örneğin şifreyi ifşa etmek, bilinmeyen bir bağlantıya tıklamak, kişisel verileri paylaşmak) anlatan kısa senaryolar oluşturacaklar.

Diğerleri karakterlerin hangi hataları yaptığını ve bunlardan nasıl kaçınabileceklerini tahmin etmeye çalışırlar.

Sorunun tanımı:

Öğrenciler birlikte şu soruyu formüle ederler: "Bir mobil uygulama insanların çevrimiçi ortamda daha güvenli davranmalarına nasıl yardımcı olabilir?"

Öğretmen, dersin amacının, internetin riskleri konusunda uyarıda bulunan ve doğru davranışları öğreten bir eğitim uygulaması tasarlamak ve oluşturmak olduğunu özetler.

Maruz kalma aşaması:

Süre: 50 dakika

Amaç:

Öğrenciler siber güvenliğin temel prensiplerini anlayacak ve kendi eğitim uygulamalarını tasarlarken bunları uygulayacaklardır.

Veri korumasına ilişkin teorik bilgiyi, internette riskli davranışları önlemeye yardımcı olacak dijital bir aracın pratikte oluşturulmasıyla birleştirme becerisini geliştirirler.

Bilim Entegrasyonu:

Öğrenciler, kimlik, güvenilirlik, manipülasyon ve çevrimiçi sorumluluk kavramlarını anlayarak vatandaşlık ve medya eğitiminden edindikleri bilgileri bir araya getiriyorlar.

Gerçek saldırı örneklerini (örneğin kimlik avı, sahte yarışmalar, viral aldatmacalar) analiz ederler.

Kullanıcıları korumak için teknolojilerin (örneğin iki faktörlü kimlik doğrulama, şifreleme) nasıl kullanıldığını tartışıyorlar.

Amaç, güvenlik prensiplerinin sadece teknik değil, aynı zamanda etik ve sosyal olduğunu göstermektir.

Bilişim entegrasyonu:

Öğrenciler MIT App Inventor aracında mobil uygulama geliştirmenin temel prensiplerini öğrenecekler:

rastgele verilerle (şifreler) çalışma,

bilgi bloklarının oluşturulması (güvenlik ipuçları, uyarılar),

etkileşimli öğelerin uygulanması (sınav, "Daha fazla bilgi edinin" düğmesi),

Kullanıcı yanıtlarına yanıt veren temel koşullu ifadeler (eğer – o zaman).

Bu şekilde dijital becerileri mantıksal düşünme ve kullanıcı arayüzü (UI/UX) prensipleriyle birleştiriyor.

Aktiviteler:

Gösterim ve analiz (10 dk)

Öğretmen MIT App Inventor'da basit bir şifre oluşturucunun oluşturulmasını gösterecek.

Güçlü bir parolanın neden büyük/küçük harfler, sayılar ve semboller içerdiğini açıklar.

Grup çalışması (30 dk)

Öğrenciler aşağıdaki unsurları içeren bir uygulama tasarlarlar:

güçlü şifre oluşturucu,

kısa güvenlik ipuçları,

Siber güvenlik üzerine mini sınav (3-5 soru).

Öğretmen blok mantığı ve test konusunda yardımcı olur.

Test ve ayarlamalar (10 dk)

Öğrenciler uygulamaları telefonlarda test ederek arayüzün işlevselliğini ve anlaşılabilirliğini doğruluyorlar.

Gruplar, uygulamalarının sınıf arkadaşlarına veya ebeveynlere nasıl yardımcı olabileceğini tartışırlar.

Fiksasyon aşaması (sabitleme ve derinleştirme):

Süre: 45 dakika

"Güvenlikten pratiğe"

Çıktıların sunumu:

Her grup uygulama prototipini sunacak, işlevlerini ve sıradan kullanıcılar için faydalarını açıklayacak.

Diğer öğrenciler geri bildirimde bulunurlar - uygulamayı neyin geliştirebileceği, neyin açık olduğu, neyin eksik olduğu.

Görsel özet:

Öğrenciler Canva'yı kullanarak "Daha Güvenli İnternet İçin 5 Kural" adlı bir infografik hazırlayacaklar ve bu infografik yazdırılabilecek veya okul web sitesinde yayınlanabilecek.

Refleksler:

Öğretmen tartışmayı başlatır:

Teknoloji çevrimiçi ortamda kendinizi korumanıza nasıl yardımcı olur?

Çevrimiçi davranışlarınız hakkında neler öğrendiniz?

Öğrenci değeriendirmesi:

Uygulamanın özgünlüğü ve işlevselliğı (%40)

Güvenlik prensiplerini anlamak (%30)

Takım çalışması ve sunum (%30)

Ekler: