Google | iKeepSafe™

# Akıllı
# Dikkatli
# Güçlü
# İyi
# Cesur

## İnternot Olmaya Var Mısın?

Dijital Vatandaşlık ve Güvenlik Ders Programı

# İnternot Olmaya Var Mısın?

Google ile internet Güvenlik Koalisyonu (iKeepSafe.org) arasında bir iş birliği çalışması olan İnternot Ders Programı'na hoş geldiniz. Bu kaynak, çocuklara internette güvenli ve akıllı davranmaları için gereken becerileri kazandırmak üzere tasarlanan çok yönlü bir program olan İnternot Olmaya Var Mısın? çalışmasının bir parçası.

İnternot Ders Programı, eğitimcilere sınıfta dijital güvenliğin temellerini öğretmek için gereken araçları ve yöntemleri sunmaktadır. En çok 3-5. sınıflara uygun olan bu ders planları en eleştirel öğrenimleri yüzeye çıkartmakta ve öğrencileri güvenli ve sorumlu dijital vatandaşlar haline getirmede eğitimcilere destek olmaktadır.

Dijital vatandaşlık ve güvenliğin beş temel konusu, İnternot Kodu şunlardır:

- **Düşünerek Paylaş**
- **Gerçek Olduğundan Emin Ol**
- **Sırların Sende Kalsın**
- **İyi Ol, Özel Ol**
- **Bir Sorun Olduğunda Konuş**

Bu dersler, dijital güvenliği öğrenme sürecini internetin kendisi kadar etkileşimli ve eğlenceli hale getiren tarayıcı tabanlı neşeli bir oyun olan Interland aracılığıyla sunulmaktadır. Eğitimciler, Interland ve tamamlayıcı ders programını kullanarak öğrencilerine en iyi uyan faaliyetleri seçebilir veya baştan sona tüm seri boyunca ilerleyebilirler.

Uluslararası Teknoloji Topluluğu, İnternot Olmaya Var Mısın? girişiminini öğrencileri 2016 ISTE Öğrenci Standartları'na hazırlayan bir kaynak olarak kabul etmiş ve Seal of Alignment for Readiness ile ödülüne layık bulmuştur.

İnternot Olmaya Var Mısın? ve Interland oyunu, aileler ve eğitimcileri güvenli internet kullanımı alışkanlıkları kazandırmaya teşvik eden pek çok kaynaktan iki tanesidir. Google'ın diğer kaynakları için **g.co/BeInternetAwesome** adresini ziyaret edin.

# İnternot Olmaya Var Mısın? Giriş mektubu/ e-posta şablonu

Anne babalara yeni eğitim araçlarının çocuklarının internette güvenlik ve davranış konusunda nasıl yardımcı olduğunu açıklamak üzere özelleştirebileceğiniz bir mektup şablonu (veya e-posta).

**Sevgili Anne Babalar,**

Çocuklarımız küçükken bir yandan onları online dünyanın risklerinden ve eksilerinden korumaya çalışırken bir yandan da internetten en iyi şekilde yararlanmaları için yardımcı olmaya çalışırız uğraşırız. Ama çocuklarımız ilk gençliğe adım attıklarında rolümüz dijital hayatlarında kendi güvenli ve etik kararlarını vermeyi öğrenmelerine yardım etmek olur.

[school name] okulunda bunun anlamı [grade]. sınıf öğrencilerimizi şunlara hazırlamaktır:
• **Eleştirel düşünmek** ve internet kaynaklarını değerlendirmek.
• **Kendilerini zorbalar ve sahtekarlar** gibi online tehditlerden korumak
• **Akıllıca paylaşımlar yapmak:** Ne, ne zaman ve kiminle.
• **Başkalarına karşı iyi olmak ve mahremiyetlerine** saygı göstermek
• **Zor durumlarda** bir anne babadan veya yetişkinden yardım istemek.

Bu yıl bu çabalar içerisinde, çocuklara internette güvenli ve akıllı davranmaları için gereken becerileri kazandırmak üzere tasarlanan çok yönlü bir program olan İnternot Olmaya Var Mısın? çalışması yer alacak. Kaynaklardan biri olan Interland, dijital güvenlik öğrenimini internetin kendisi gibi etkileşimli ve eğlenceli hale getiren tarayıcı tabanlı zevkli bir oyun. iKeepsafe.org'da Google tarafından eğitimciler ve internet güvenlik uzmanları tarafından geliştirilen İnternot Olmaya Var Mısın? girişimi, beş temel ders etrafında oluşturulan eğlenceli, yaşa uygun öğrenme imkanı sunuyor:
• **Düşünerek Paylaş**
• **Gerçek Olduğundan Emin Ol**
• **Sırların Sende Kalsın**
• **İyi Ol, Özel Ol**
• **Bir Sorun Olduğunda Konuş**

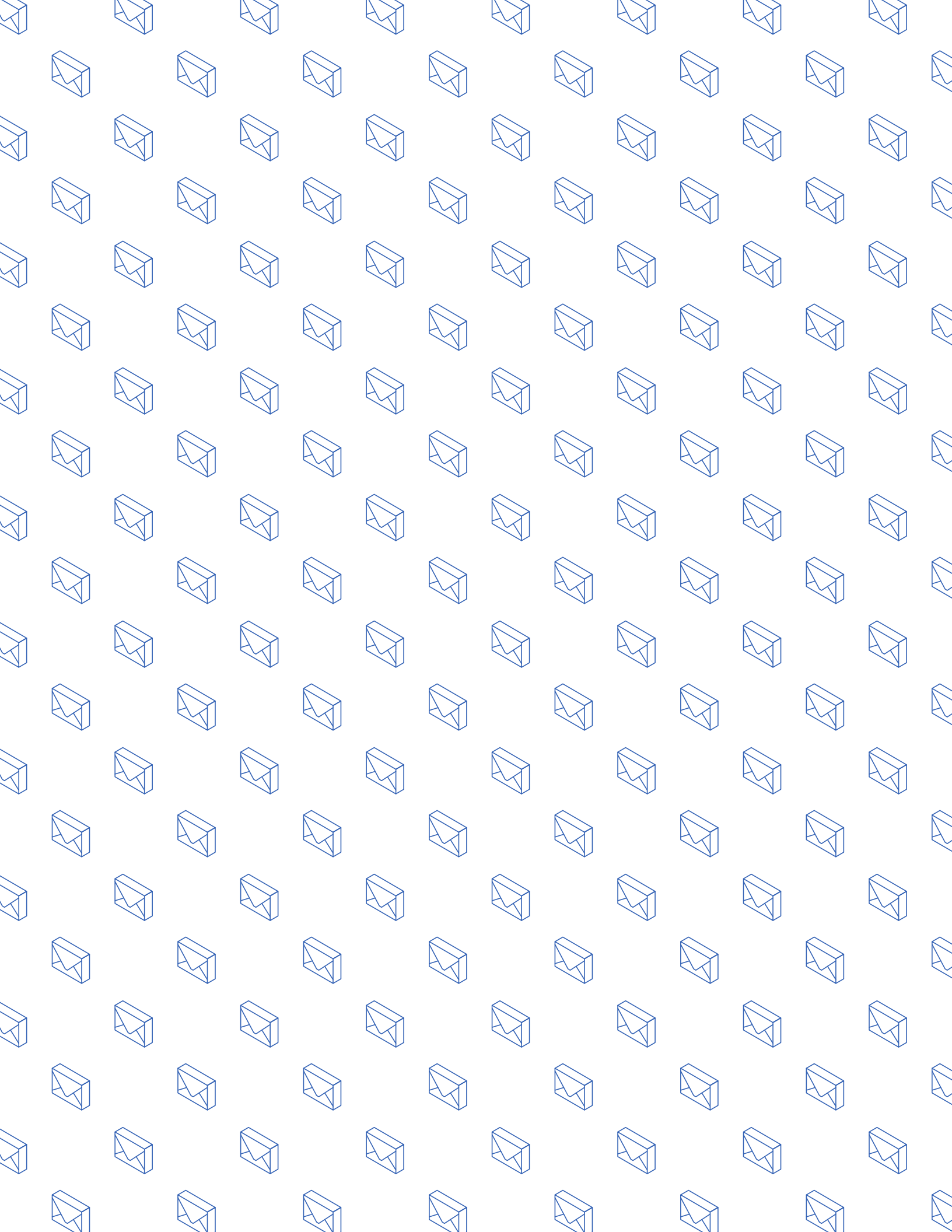
Akıllı ve güvenli teknoloji kullanımı öğrencilerin daha iyi öğrenmesine yardımcı olurken okullarımızın işlevini daha iyi yerine getirmesine destek olur. İnternot Olmaya Var Mısın? programı, [okul adı] okulumuzdaki tüm öğrencilerin internette öğrenmesini, keşfetmesini ve güvende kalmasını sağlamaya doğru attığımız önemli bir adım.

İlginizi çekiyorsa, çocuklarınızın evde kullanmaya başlayabileceği kaynaklardan bazılarına giriş de dahil olmak üzere bu yeni program ile ilgili daha fazla bilgiyi sizinle paylaşabiliriz. Çocuklarınıza sınıfta ne yaptığımızı sormanızı öneririz. Bakarsınız siz de gizlilik ve güvenlikle ilgili birkaç ipucu öğrenirsiniz!

Saygılarımızla,

[Siz]

# İçindekiler



1. Ders: Düşünerek Paylaş

# Düşünerek Paylaş

**İnternetteki itibarınızı koruma**

## Derse genel bakış

1. Etkinlik: **Sır tutabilir misin?**
2. Etkinlik: **Profil tahmin oyunu**
3. Etkinlik: **Başkaları bizi nasıl görüyor?**
4. Etkinlik: **Gizlilik alıştırması**
5. Etkinlik: **Interland: Mindful Mountain**

## Temalar

Öğretmenler ve anne babalar, erken yaşta yapılan dijital hataların kişinin itibarında kalıcı hasar yaratabileceğini biliyorlar. Ancak ergenlik öncesi gençleri bugün yapılan zararsız bir yayının gelecekte normalde hedeflemediğiniz bir kitle tarafından yanlış anlaşılabileceğine ikna etmek zor olabilir.

Bu etkinliklerde, öğrencilere gizliliklerini ve kişisel bilgilerini koruyarak internette nasıl olumlu bir şekilde itibara sahip olabileceklerini öğretmek için somut örnekler kullanılmaktadır.

## Hedefler

- ✓ **İnternette olumlu bir itibar** oluşturma ve yönetme.
- ✓ **Başkalarının sınırlarına** saygı gösterme.
- ✓ **Yanlış yönetilen dijital ayak izinin** potansiyel etkisini anlama.
- ✓ **Zor durumlarla başa çıkmak için** bir yetişkinden yardım alın.

## Üzerinde durulan standartlar

**Öğretmenler için ISTE Standartları:** 1a, 1b, 1d, 2a, 2c, 3b, 3d, 4a, 4b, 4c, 4d, 5b
**Öğrenciler için ISTE Standartları 2016:** 1d, 2a, 2b, 2d **AASL Öğrenim Standartları:** 1.1.1, 1.1.2, 1.1.8, 1.3.3, 1.3.5, 2.1.3, 2.1.4, 2.3.1, 2.3.3, 2.4.1, 3.1.2, 3.1.5, 3.1.6, 3.2.2, 3.3.3, 4.3.4, 4.4.4

# Düşünerek Paylaş
## Sözlük

### Dijital ayak izi
Dijital ayak iziniz internette size ait her şeydir! Fotoğraflar, ses, görüntü, metin, blog yayınları ve arkadaşlarınızın sayfalarına yazdığınız mesajlardır.

### Kişisel bilgiler
Belirli bir kişi ile ilgili bilgiler. Kişisel bilgileriniz, ne kadar hassas olduğuna bağlı olarak, farklı derecelerde herkese açık veya özel bilgiler olabilir.

### Ayarlar
Bir dijital üründe, uygulamada, web sitesinde ve benzeri bir ortamda ne paylaştığınızın ve hesabınızın nasıl yönetileceğini tanımladığınız veya ayarladığınız alan

### Sınır
İki şeyin nerede farklılaştığını veya yapılmaması gerekenler ile ilgili resmi olmayan kuralları belirten bir nokta veya limit. Sınırın bir tarafındaki davranış kabul edilebilirken diğer tarafındaki değildir.

## Düşünerek Paylaş: 1. Etkinlik

# Sır tutabilir misin?

Öğrenciler iki kişilik gruplar oluşturarak uydurdukları sırları karşılaştırır ve gizlilik alanları üzerine düşünmeye başlar.

## Hedefler

- ✓ **Ne tür kişisel bilgilerin** gizli kalması gerektiğini bilin.
- ✓ **Sırrının gizli kalmasını** istemek herkesin en doğal hakkıdır.
- ✓ **İnternette bulunabilecek** başka tür kişisel bilgileri belirtin.

## Haydi konuşalım

**İyilik neden önemli?**

Dijital ayak iziniz internette size ait olan her şeydir. Fotoğraflar, ses, görüntü, metin, blog yayınları ve arkadaşlarınızın sayfalarına yazdığınız mesajlardır. Siz yaş aldıkça güçlü bir online varlığınız olur ve size pek çok avantaj sağlayabilir. İnternet ailenizle, arkadaşlarınızla ve sizinle aynı zevklere sahip kişilerle iletişim kurmanızı kolaylaştırır. Bazen sosyal ağlarda pek fazla düşünmeden mesaj göndeririz, resim paylaşırız ve sohbetlere katılırız.

Ama bu online bağlantı, beraberinde riskler de getirebilir. Bir şey artık yayınlandığında bunun dönüşü yoktur. Bugün komik veya zararsız olduğunu düşündüğünüz bir şey, gelecekte bu yayınları görmesini istemeyeceğiniz kişiler tarafından görülüp yanlış anlaşılabilir. Unutmayın:

- İnternetteki diğer her şey gibi dijital ayak izinizi de dünyadaki herkes görebilir.
- Sizinle ilgili bir şey artık internetteyse artık hep internette kalabilir.

Gizliliğiniz işte bu yüzden önemlidir. Sadece paylaşma konusunda hiçbir şüphe duymadığınız şeyleri paylaşarak, diğer deyişle internette oluşturduğunuz kişilik konusunda dikkatli olarak gizliliğinizi koruyabilirsiniz. Ne zaman sessiz kalacağınızı bilmek, başkalarının gizliliğine saygı göstermek ve kendinizinkini korumak açısından önemlidir.

## Etkinlik

**1. Bir sır uydurun**

İlk olarak herkes bir sır düşünsün (gerçek olmasın).

**2. Ortağınıza söyleyin**

Tamam, sırlarınız hazır mı? Şimdi ikili gruplar oluşturalım, sırrınızı ortağınıza söyleyin ve şu iki soruyu tartışın:

- Bu sırrı kimseyle paylaşır mıydınız?
- Sırrınızı kiminle paylaşırdınız ve neden?

**3. Sınıfa söyleyin**

Son olarak, her öğrenci sınıfa sırrını ve paylaşıp paylaşmama konusunda neye karar verdiklerini söyleyecek.

Bir sonraki sayfada devam ediyor →

## Düşünerek Paylaş: 1. Etkinlik (devamı)

### Ana Fikir

Sırlar, gizli kalmasını isteyebileceğimiz ya da sadece güvendiğimiz ailemizle veya arkadaşlarımızla paylaşmak isteyeceğimiz kişisel bilgi türüdür. Başka hangi tür bilgilerin güvenliği konusunda dikkatli olmamız gerekir?

- Ev adresiniz ve telefon numaranız
- E-posta şifreniz ve diğer internet şifreleriniz
- Kullanıcı adlarınız
- Ödevleriniz veya oluşturduğunuz diğer dokümanlar
- Fotoğraflarınız, videolar, müzik dosyaları ve diğer içerikler

## Düşünerek Paylaş: 2. Etkinlik

# Profil tahmin etme oyunu

Öğrenciler, hayali bir karakterle ilgili kişisel bilgileri okur ve bu bilgiler ışığında bu kişiler hakkında çıkarımda bulunurlar.

## Hedefler

- ✓ **İnsanlarla** ilgili bilgilere online olarak ulaşmanın yollarını belirtin.
- ✓ **Kişisel verilerine dayanarak** birisi hakkında ne biliyor olacağınıza karar verin.
- ✓ **Tüm bu çıkarımların** bir kişi ile ilgili tam doğru bilgileri yansıtmadığının farkına varın.

## Haydi konuşalım

**Ne bildiğimizi nereden biliyoruz?**

İnternette çok fazla kişisel bilgi var. Bu bilgilerden bazıları insanlar hakkında doğru olmayan çıkarımlarda bulunmamıza neden olabilir. İşte yanıtlarını keşfedeceğimiz sorulardan bazıları:

- Kişisel bilgilerinden kişi hakkında neler öğrenebiliriz?
- Emin olmasak bile kişisel bilgilerden neleri tahmin edebiliriz?
- Bu bilgilerin nasıl elde edildiğini biliyor muyuz?

## Etkinlik

**Gereken malzemeler:**

- Çeşitli hayali kişisel veri kaynakları. Bir sonraki sayfadaki broşürü kullanabilir veya şu fikirlerden yola çıkarak kendiniz bir tane oluşturabilirsiniz:
  - Yaşları uygunsa sosyal medya hesapları
  - Tarayıcı geçmişi günlüklerinin çıktısı
  - "Check in" yaptıkları yerlerin (restoran, kafe, kablosuz bağlantı noktası) çıktısı
  - Kısa bir yazı ödevi için defter veya cihaz

**1. Kişiye yakından bakın**

İlk önce herkes karakterimizin dijital ayak izinin bir kopyasını alıp okusun.

**2. Bir açıklama yazın**

Sonra gruplara ayrılacağız ve her grup bu kişi hakkında kısa bir açıklama yazacak. Sizce kim bunlar?

**3. Gerçeği açığa çıkartın**

Evet, şimdi karakterlerimiz hakkındaki gerçekler:

- **Ceren** lise son sınıf öğrencisi. Seneye üniversiteye gidecek ve işletme okuyup ileride kendi moda markasını yaratmak istiyor. Onun için en önemli şeyler: aile, gönüllü işler, pop kültürü ve moda.
- **Tolga**, lise basketbol takımında oyun kurucu. 16 yaşında ve İstanbul'da oturuyor. 8 yaşında bir kız kardeşi var. En önem verdiği şeyler: basketbol, sanat, gitar çalmak ve arkadaşları.
- **Lara** 17 yaşında. Voleybol takımına yeni katıldı ve iki kedisi var. Mühendislik işlerinde ok iyi ve hafta sonları robot yapmayı seviyor. En önem verdiği şeyler: teknoloji, voleybol takımı, hayvanlar ve hayvan hakları.

Şimdi hangi tahminlerimiz doğru çıktı, hangileri çıkmadı?

Bir sonraki sayfada devam ediyor →

## Düşünerek Paylaş: 2. Etkinlik (devamı)

### Ana Fikir

İnsanlar hakkındaki yargılarımız her zaman doğru değildir. Ama sık sık bu yanlış çıkarımlardan yola çıkarak karar verir veya yargılarız. Her zaman için tanıdığını düşündüğün kişilerle ilgili şeyleri gerçekten doğru bildiğinden emin ol.

Aşağıda her kişinin online etkinliği ile ilgili açıklamayı oku. Her örnekten sonra, bu kişinin kim olduğu ile ilgili kısa bir açıklama yaz. Nelerden hoşlanır, nelerden hoşlanmaz, neye önem verir?

## Ceren

- Danstan deniz altı fotoğrafları! Hepiniz harika görünüyorsunuz!
- En iyi Akne İlaçları
- Kardeşim Ali çok sinir. Belki de uzaylıdır
- Arena Merkezi, Cumhuriyet Cad.
- Genç Tasarımcılar Konferansı - İzmit Üniversitesi
- EN SONUNDA YENİ CASUS SAVAŞLARI FİLMİNİ GÖRDÜM. Aman tanrım taktım buna!

## Tolga

- Oyunu kazandım! Şampiyonluk öncesi bir oyun daha. Kale atışlarına daha çok çalışmam lazım.
- Okul danslarından nefret ediyorum. #gitmiyorum
- Ankara Fen Lisesi
- Anne Babanızın Hayatınızı Mahvetmeye Çalıştığını Gösteren 10 İşaret
- Bu cumartesi babamla Sapanca gölüne gidiyorum! Mükemmel olacak
- Şehir Merkezinde La La Luna

## Lara

- Elit Burger
- Kazanamadık. Çok sinir. Ama en azından berabere kaldık.
- 25 Köpek Yavrusu Fotoğrafı
- Atatürk Ortaokulu Mezuniyeti
- Arkadaşımın web sitesine bir göz atın! Kodunu ben yazdım.
- Yüksek puan aldım!! Eveeet. Gem Jam'e bayılıyorum!!

## Düşünerek Paylaş: 3. Etkinlik

# Başkaları bizi nasıl görüyor?

Öğrenciler, önceki etkinlikte anne babalar, işverenler, arkadaşlar, polis gibi farklı kişilerin karakteri nasıl göreceğini keşfeder.

## Hedefler

- ✓ **Bir bilgiyi** online paylaşıp paylaşmamaya karar verirken kendiniz dışında başkalarının bakış açılarını da göz önünde bulundurun.
- ✓ **Kişisel bilgileri** herkese açıklamanın sonuçlarını düşünün: Paylaştıklarınız toplumda gördüğünüz saygının parçası olur ki bu da kalıcı olabilir.

## Haydi konuşalım

**Yeni bir bakış açısı**

Dijital ayak izinizdeki bilgiler insanlara hakkınızda bilmelerini istediğinizden daha fazlasını söyleyebilir ve bu durumun önemli sonuçları olabilir.

Şimdi karakterimizin bakış açısından profile tekrar bakalım.

- Sizce başkalarının tüm bu kişisel bilgilere sahip olmasını ister mi?
- Bu bilgi başkaları tarafından nasıl kullanabilir?

Farklı durumlar farklı gizlilik seviyeleri gerektirir. Dünyayı başkasının bakış açısından görmek gizlilik hakkını anlamada temel öneme sahiptir.

## Etkinlik

**Gereken malzemeler:**

- 2. Etkinlikteki hayali profili canlandıran her öğrenci için bir kopya

**1. Yeni bir bakış açısıdan bakın**

Şimdi gruplara ayrılacağız ve her grup karakterimize şu insanların bakış açısından yaklaşacak:

- Anne baba
- Antrenör
- İşveren
- Arkadaş
- Polis
- Reklamcı
- 10 yıl sonra siz

Bu kategorideki kişiler için ne önemli? Bu profil hakkında hangi sonuçlara varırlardı? Karakterimizin, grubunuzun görmesini istemeyeceği veya açıklamalarının akıllıca olmayacağını düşündüğünüz bilgilerin üzerini çizin.

**2. Sonuçları sunun**

Son olarak, her grup sonuçlarını sunar ve gizlilik tercihlerini açıklar.

## Ana Fikir

Farklı kişiler aynı bilgiyi görüp farklı sonuçlar çıkarabilir. Online ortamda başkalarının sizi sizin düşündüğünüz gibi göreceklerini varsaymayın.

## Düşünerek Paylaş: 4. Etkinlik

# Pratikte gizlilik

Sınıf, yazılı üç senaryoyu gözden geçirir ve her biri için en iyi gizlilik çözümünün ne olduğunu tartışır.

## Hedefler

- ✓ **Gizlilik ile ilgili endişelere** farklı kişilerin bakış açısından bakmaya çalışın.
- ✓ **Farklı senaryoların** nasıl farklı gizlilik seviyeleri gerektirdiğini anlayın.

## Haydi konuşalım

**Gizlilik senaryoları: Ne yapmanız gerekir?**

**1. Örnek:** Okuldan tanıdığınız bir çocuğu karnında renkli, çirkin bir kızarıklığa neden olan garip bir böcek ısırdı. Bunu başkalarının bilmesini istemiyor.
- Başkalarının bilmeye hakkı var mı?
- Onlara söylemeli misin?

**2. Örnek:** Birisi günlüğüne bir şeyler yazdı. Bir başkası yazdıklarını kopyaladı ve online ortamda paylaştı.
- Diğer kişi günlüğü paylaşarak yanlış bir şey mi yapmış oldu?
- Birisi sizin günlüğünüzü paylaşsa ne hissederdiniz?

**3. Örnek:** Birisi arkadaşının sosyal medya sayfasına "İyi tatiller!" yazıyor.
- Bu kişi arkadaşının bir yerlere gittiğini herkese duyurmuş mu oluyor?
- Bu dileği iletmenin daha gizli yolları yok mu? Örneğin özel mesaj veya kısa mesaj gönderse daha mı iyi olurdu?

## Etkinlik

Üç senaryoyu gözden geçirip her birinin nasıl farklı bir gizlilik çözümü olabileceği üzerine konuşacağız.

## Ana Fikir

Farklı durumlar farklı yanıtlar gerektirir. Normalde sizin yapacağınız tercihler olmasa bile başkalarının gizlilik tercihlerine saygı göstermek her zaman önemlidir.

## Düşünerek Paylaş: 5. Etkinlik

# Interland: Mindful Mountain

Interland'ın dağlık şehir merkezi herkesin karşılaştığı ve kaynaştığı bir yer. Ama kiminle ne paylaştığına dikkat etmen gerekiyor. Bilgi ışık hızında seyahat ediyor ve tanıdığın İnternot'lar arasında çenesi biraz düşük olanlar var.

Masaüstü veya mobil cihazda (ör. tablet) bir web tarayıcısını aç, **g.co/Interland** adresine git ve Mindful Mountain oyun seçeneğine gir.

## Tartışma Konuları

Oyunu sınıfınızla oynayın ve aşağıdaki sorulardan yararlanarak oyunda öğrendikleri dersleri daha detaylı tartışın.

- Oyunda paylaştığınız tüm yayınlardan hangisini gerçek hayatta en fazla paylaşırdınız? Ve neden?
- Yapmamanız gerektiği halde yanlışlıkla bir şeyi paylaştığınız bir anınızı anlatın.
- Sizce Mindful Mountain'daki karaktere neden çenesi düşük deniyor?
- Çenesi düşük karakter hakkında bilgi verin ve hareketlerinin oyunu nasıl etkilediğini belirtin.
- Mindful Mountain oynamak gelecekte başkalarıyla online paylaşacaklarınız konusunda düşüncelerinizi değiştirdi mi?
- Bu derslere katıldıktan ve oyunu oynadıktan sonra daha önce yaptığınız neyi farklı yaparsınız?
- Bir şeyi sadece arkadaşlarınız yerine herkesle paylaşmanın yaratabileceği olumsuz sonuçlara bir örnek verebilir misiniz?
- Kişisel bir şeyi yanlışlıkla paylaşırsanız ne gibi adımlar atabilirsiniz?

2. Ders: Gerçek Olduğundan Emin Ol

# Gerçek Olduğundan Emin Ol

**Kimlik avından ve sahtekarlıklardan uzak durma**

## Derse genel bakış

1. Etkinlik: **Bu kimlik avı tezgahına aldanmayın!**
2. Etkinlik: **Gerçekten kimsin?**
3. Etkinlik: **Interland: Reality River**

## Temalar

Çocukların, internette buldukları içeriğin doğru ve güvenilir olmayabileceğini bilmeleri önemlidir. Bazen bu bilgileri çalmak için kötü niyetli çaba gösterilebilir. Kimlik avı ve diğer online sahtekarlıklar, her yaştan internet kullanıcısını tanımadıkları veya tanıdıkları birinin kimliğine bürünmüş kişilerden gelen gizemli mesajlara yanıt vermeye teşvik edebilir.

## Hedefler

- ✓ **Bir şeyin** internette olmasının o şeyin doğru olduğu anlamına gelmediğini unutmayın.
- ✓ **Kimlik avının** işleme mekanizmasını ve neden bir tehdit oluşturduğunu öğrenin.
- ✓ **Sahte teklifleri**, ödülleri ve diğer online sahtekarlıkları fark edin.

## Üzerinde durulan standartlar

**Öğretmenler için ISTE Standartları:** 1a, 1b, 2a, 3d, 4a, 4b, 4c, 4d **Öğrenciler için ISTE Standartları 2016:** 1d, 2a, 2b, 2c, 2d, 3a, 3b **AASL Öğrenim Standartları:** 1.1.1, 1.1.5, 1.1.6, 1.1.8, 1.2.4, 1.2.6, 1.3.3, 1.3.5, 2.1.1, 2.1.4, 2.3.1, 2.3.3, 2.4.1, 3.1.2, 3.1.5, 3.1.6, 3.2.2, 4.1.7, 4.3.2, 4.3.4, 4.4.4 **C3:** II:A, II:B, II:C, III:A, III:B,III:C, III:D

# Gerçek Olduğundan Emin Ol
## Sözlük

### Kimlik Avı
Kimlik avı saldırısı, birisi sizi kişisel bilgilerinizi internette paylaşmanız için kandırdığında olur. Kimlik avı çoğunlukla e-posta, reklam veya kullanıyor olduğunuz sitelere benzer siteler aracılığıyla yapılır.

### Hedef Odaklı Kimlik Avı
Bu kimlik avı türü, saldırganın kişisel bilgilerinizi kullanarak daha hedef odaklı bir şekilde dolandırmaya çalışmasıdır.

### Sahtekarlık
İnsanları kandırarak para kazanma veya değerli bir şeyi elde etmek amaçlı dürüst olmayan bir girişimdir.

### Güvenilir
Doğru olan veya gerekli bir şeyi yapma konusunda güvenebilecek olan

### Özgün
Gerçek, asıl, doğru veya kesin; sahte ya da kopya olmayan

### Doğrulanabilir
Kanıtlanabilir veya doğru ya da gerçek olduğu gösterilebilir olan

### Aldatıcı
Birisini doğru olmayan bir şeye inandırmak niyetiyle yapılır

### Hileli
Birisinden değerli bir şeyi almak için kandırmak amacıyla yapılır

### Güvenlik Duvarı
Bilgisayarınızı sahtekarlık ve hileli durumlara karşı koruyan program

# Bu kimlik avı tezgahına aldanmayın!

Öğrencilerin çeşitli e-posta ve kısa mesajlara göz atıp hangi mesajların yasal, hangilerinin kimlik avı sahtekarlığı olduğuna karar vermeye çalıştıkları bir oyun.

## Hedefler

- ✓ **Kişilerin kimlik çalmak için** kullandıkları teknikleri öğrenin.
- ✓ **Kimlik hırsızlığını** engellemenin yollarına göz atın.
- ✓ **Kimlik hırsızlığına** uğradıklarını düşünüyorlarsa güvendikleri bir yetişkinle konuşmalarını söyleyin.
- ✓ **Kimlik avı denemesinin** işaretlerini bilin.
- ✓ **Kişisel bilgilerini** nasıl ve kimlerle paylaştıkları konusunda dikkatli olun.

## Haydi konuşalım

**Bu kimlik avı denilen şey nedir?**

Kimlik avı, birisinin güvendiğiniz bir kişi gibi davranarak e-posta, kısa mesaj ya da başka bir online iletişimde oturum veya hesap bilgileriniz gibi verilerinizi çalmaya çalışmasıdır. Kimlik avı e-postaları—Sizi göndermek istedikleri güvenli olmayan siteler veya indirip açmanız için sizi kandırmaya çalıştıkları dosyalar ve ekler bilgisayarınıza virüs bulaşmasına neden olabilir. Bu virüsler, daha fazla kimlik avı e-postası göndermek üzere kişi listenizdeki arkadaşlarınızı ve ailenizi hedef alabilir. Başka dolandırıcılık türleri de, cihazınızda bir sorun olduğu söylenerek kötü amaçlı veya istenmeyen yazılım indirmeniz için sizi kandırabilir. Unutmayın: Bir web sitesi veya reklam, makinenizde bir sorun olup olmadığını bilemez!

Bazı kimlik avı saldırıları açık olarak sahtedir. Ancak bazıları iyi düşünülmüş ve ikna edici olabilir. Örneğin, bir sahtekar size bazı kişisel bilgilerinizi içeren bir mesaj gönderirse buna hedef odaklı kimlik avı denir ve çok etkili olabilir.

E-posta ve kısa mesajlardaki gariplik veya olağan olmayan durumları şüpheli bağlantıları tıklamadan ya da riskli web sitelerine şifrenizi girmeden, bir an önce fark etmek önemlidir.

İşte bir mesajı veya siteyi değerlendirirken sormanız gereken bazı sorular:

- Rozet gibi güvenilir bir siteye ait göstergeler içeriyor mu?
- Bir sitenin URL'si aradığınız adla ve başlıkla aynı mı?
- Pop-up pencereler çıkıyor mu? (Bu pencereler genellikle kötü haber içerir.)
- URL, önünde yeşil bir kilit olan https:// ile mi başlıyor? (Bu bağlantının şifreli ve güvenli olduğunu gösterir.)
- Küçük dip not metninde ne yazıyor? (Sinsi içeriği bu bölüme koyarlar.)

Peki kandırılırsanız ne olur? Öncelikle panik olmayın!

- Anne babanıza, öğretmeninize veya güvendiğiniz bir yetişkine hemen söyleyin. Ne kadar uzun beklerseniz işler o kadar kötüleşir.
- İnternet hesaplarının şifrelerini değiştirin.
- Kimlik avı denemesine veya sahtekarlığına uğrarsanız bundan etkilenebilecek arkadaşlarınıza haber verin.
- Mümkünse mesajı spam olarak bildirme ayarlarını kullanın.

Bir sonraki sayfada devam ediyor →

# Gerçek Olduğundan Emin Ol: 1. Etkinlik (devamı)

## Etkinlik

**Gereken malzemeler:**

- Öğrenciler için broşür: Kimlik avı örnekleri

**Öğrenciler için broşür: Kimlik avı örnekleri**

1. **Gerçek.** E-postada, zararlı olabilecek bir bağlantı sağlamak yerine, kullanıcıdan kendi hesaplarında oturum açmaları istenmektedir.
2. **Sahte.** Şüpheli ve güvenli olmayan URL
3. **Gerçek.** URL'deki https:// adresine dikkat edin
4. **Sahte.** Banka bilgileri karşılığında şüpheli teklif
5. **Sahte.** Güvenli olmayan ve şüpheli URL

**1. Gruplar örnekler üzerinde çalışıyor**
Şimdi gruplara ayrılalım ve her grup mesaj ve web sitesi örnekleri üzerinde çalışsın.

**2. Kişiler tercihlerini belirtiyor**
Her örneğin "gerçek" mi veya "sahte" mi olduğuna karar verin ve nedenlerini aşağıda sıralayın.

**3. Gruplar seçenekleri tartışıyor**
Hangi örnekler güvenilir, hangileri şüpheli göründü? Cevaplardan sizi şaşırtan oldu mu?

**4. Daha Detaylı Tartışma**
İşte online karşınıza çıkan mesaj ve siteleri değerlendirirken kendinize sorabileceğiniz başka sorular:

**• Bu mesaj gerçek görünüyor mu?**
İlk izleniminiz ne? Güvenilir gelmeyen herhangi bir şey fark ettiniz mi?

**• E-postada size bedava bir şey sunuluyor mu?**
Ücretsiz teklifler genellikle ücretsiz değildir.

**• Sizden kişisel bilgi isteniyor mu?**
Bazı web sitelerinde size daha fazla sahte mesaj gönderebilmeleri için kişisel bilgilerinizi girmeniz istenir. Mesela "kişilik testleri", şifrenizi tahmin etmeyi kolaylaştırmak veya başka gizli bilgiler almak için bilgi almaya çalışır. Gerçek işletmeler ise sizden e-postayla kişisel bilgi almaya çalışmayacaktır.

**• Zincir e-posta mı sosyal yayın mı?**
E-postayı tanıdığınız herkese iletmenizi isteyen e-posta ve yayınlar sizi ve başkalarını riske atabilir. Kaynağından ve mesajı iletmenin güvenli olduğundan emin değilseniz iletmeyin.

**• Metinde dipnot var mı?**
Çoğu dokümanın en altında "dipnot" vardır. Bu metin çok küçüktür ve görmemeniz gereken bilgiler yazar. Mesela yukarıda bedava telefon kazandığınız yazmaktadır, ama küçücük puntoyla bu firmaya ayda 200 ABD doları ödemeniz gerektiği yazar.

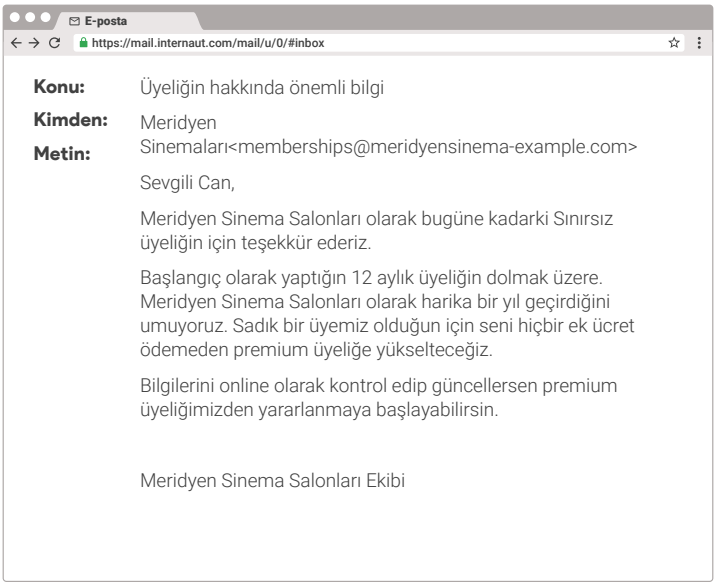
**Not:**
Bu alıştırmada İnternot Posta'nun gerçek, güvenilir bir hizmet olduğunu varsayın.

## Ana Fikir

Online ortamda e-posta, kısa mesaj ve yayınlanan mesajlarda her zaman kimlik avı saldırılarına karşı dikkatli olun. Birisi sizi kandırırsa mutlaka doğru kişiye bu durumu haber verin.

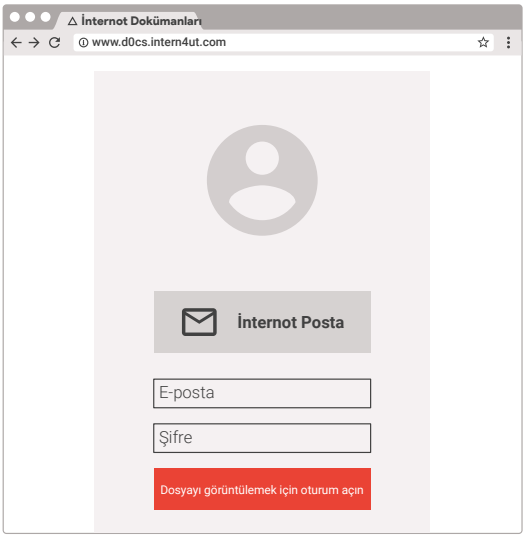
## Çalışma Sayfası: 1. Etkinlik

# Kimlik avı örnekleri



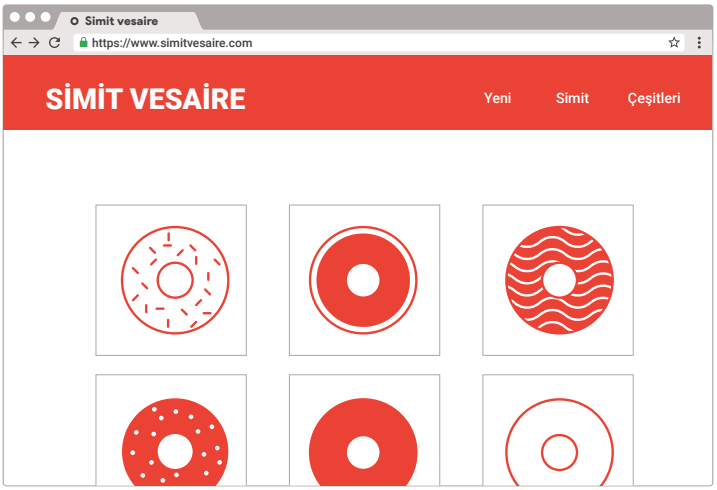

### 1. Gerçek mi sahte mi?

Gerçek _____ Sahte _____




### 2. Gerçek mi sahte mi?

Gerçek _____ Sahte _____

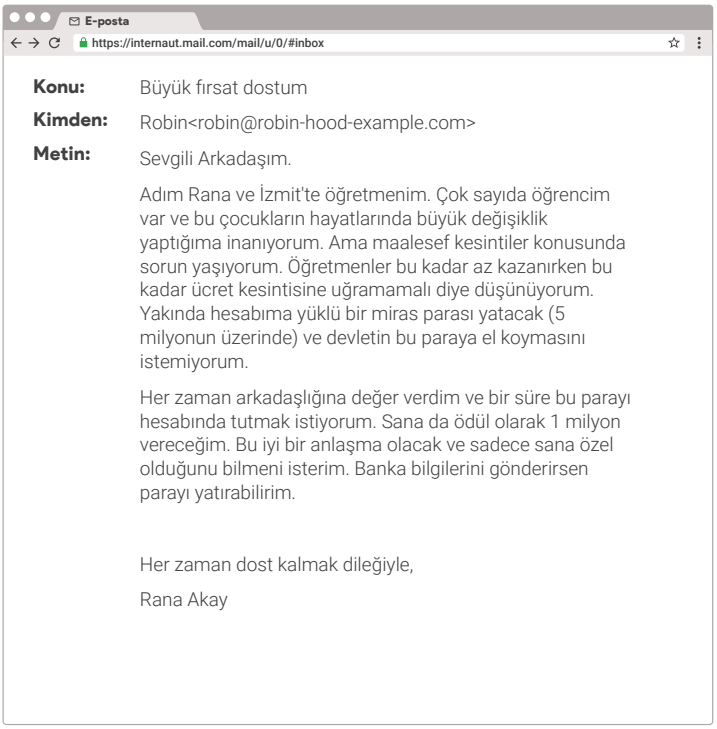



### 3. Gerçek mi sahte mi?

Gerçek _____ Sahte _____

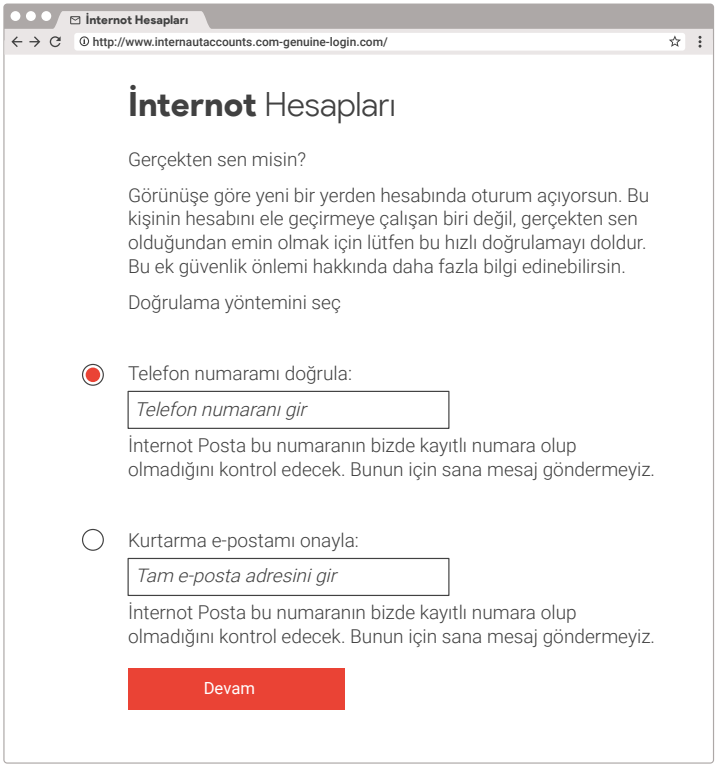
Bir sonraki sayfada devam ediyor →

# Çalışma Sayfası: 1. Etkinlik (devamı)




## 4. Gerçek mi sahte mi?

Gerçek _____ Sahte _____




## 5. Gerçek mi sahte mi?

Gerçek _____ Sahte _____

# Pardon kimsiniz?

Öğrenciler şüpheli online metinlere, yayınlara, resimlere ve e-postalara verilebilecek cevapları canlandırarak ve tartışarak kimlik avına karşı yapabileceklerinin pratiğini yaparlar.

## Hedefler

- ✓ **Online kitlelerinin** düşündüklerinden daha büyük olabileceğini hesaba katın.
- ✓ **Online ortamda** konuştukları kişilerin kimliklerini gerçekten bildiklerinden emin olun.
- ✓ **Birileriyle** online ortamda "arkadaş" olmadan veya bağlantı kurmadan önce durup düşünün.
- ✓ **Kişisel bilgilerini** verdikleri kişiler ve ne tür bilgiler paylaşabilecekleri konusunda dikkatli olun.
- ✓ **Emin değillerse** sorular sorabilir ve/veya bir yetişkinden yardım isteyebilirler.
- ✓ **Online ortamda** birisi kendilerini rahatsız eden bir konuyu tartışmak isterse bir yetişkine söylesinler.
- ✓ **Tüm online** işlemlerinde dürüst davransınlar.

## Haydi konuşalım

**Gerçekten o kişi olduklarını nasıl anlarsın?**
Bir arkadaşınızla telefonda konuşurken yüzünü göremeseniz de o olduğunu nasıl anlarsınız? Bazen insanlar dalga geçmek için online ortamda başka biri gibi davranabilirler. Bazen de kişisel bilgileri çalmak için başkalarının kimliğine bürünürler. İnternetteyken yabancılar sizinle bağlantı kurmak isteyebilirler. Bu kişiyle bağlantı kurmak isteyip istemeyeceğiniz ve nasıl cevap vereceğiniz size bağlıdır.

Neyse ki kişilerin kimliğini doğrulayabilir ve sahtekarları tespit edebilirsiniz. İşte size birkaç fikir.

**• Profil resimleri şüpheli mi görünüyor?**
Profil resimleri soluk veya zor seçilir durumda mı? Öyleyse dikkatli olun; net olmayan bir fotoğrafın arkasında gizlenmek daha kolaydır. Ayrıca dolandırıcıların sahte bir profil oluşturmak için gerçek kişilerin fotoğrafları çalmaları da sık karşılaşılan bir durumdur.

**• Görünen ad kullanıcı adlarıyla aynı mı?**
Mesela sosyal medyada profil URL'leri verdikleri adla aynı mı? (Örneğin, SocialMedia.com/jane.doe gibi bir adrese sahip sahte bir isim)

**• Kişisel özgeçmişleri var mı?**
Öyleyse gerçek bir kişi tarafından yazılmış gibi mi duruyor? Sahte hesaplarda "Hakkımda" bölümünde pek bilgi bulunmaz veya kişi sahte bir profil oluşturmak için bazı bilgileri bir araya getirmiş olabilir.

**• Hesap ne kadar zamandır etkin?**
Profil yeni mi veya çok sayıda anormal etkinliği mi var? Sahte hesapların genellikle geçmiş yayın veya sosyal etkileşimi yoktur.

Bir sonraki sayfada devam ediyor →

# Gerçek Olduğundan Emin Ol: 2. Etkinlik (devamı)

## Etkinlik

**Gereken malzemeler:**

- "Gerçekten kimsin?" çalışma sayfasının şeritler halinde kesilmiş bir kopyası. Her bir şeritte bir senaryo bulunuyor.
- Öğrencilerin içinden bir şerit seçebilecekleri kap veya kutu
- 25 ve 26. sayfalar için kopya sayfası

**1. Grup inceleme senaryoları**

Tamam, şimdi gruplara ayrılacağız. Her grup bu kutudan bir senaryo seçecek ve böylesi bir durumda nasıl cevap vermesi gerektiğini konuşacak.

**2. Grup eylem senaryoları**

Şimdi her grup senaryosunu canlandıracak. Bir öğrenci okuyacak, diğer bir öğrenci "mesajı" canlandıracak, üçüncüsü yanıt verecek ve belki bir dördüncüsü mantığını açıklayacak.

**3. Sınıf, grupların tercihlerini tartışacak**

Son olarak, her grubun tercihlerini tartışmak için bu kopya kağıdını kullanalım.

## Ana Fikir

Online ortamda kimlerle konuşacağını sen belirlersin. Bağlantı kurduğun kişilerin söyledikleri kişi olduklarından emin ol!

Çalışma Sayfası: 2. Etkinlik

# Pardon kimsiniz?

| | |
|---|---|
| **Senaryo 1** | Bir yabancıdan internette mesaj isteği aldınız. "Selam! Eğlenceli birisine benziyorsun. Bir ara takılmaya ne dersin? Beni arkadaş listene ekler misin? –Can” |
| **2. Senaryo** | Cep telefonunuza tanımadığınız birisinden kısa mesaj geldi. "Selam, ben Özlem! Geçen yaz tanışmıştık, hatırladın mı?" |
| **3. Senaryo** | Zeynep Hanım ile matematik dersinden sonra cep telefonuna şöyle bir mesaj geliyor. "Zeynep Hanım'ın matematik sınıfından Berk ben. Ödevi anladın mı?" |
| **4. Senaryo** | Takip etmediğiniz birinden mesaj aldınız. "Selam! Yazdıkların çok hoşuma gidiyor. ÇOK komik! Bana telefon numaranı yazsana, daha çok konuşuruz böylece!" |
| **5. Senaryo** | Bilmediğiniz birisinden sohbet mesajı aldınız. "Bugün seni Matematik sınıfında gördüm. Çok tatlısın! Adresini öğrenebilir miyim? Birlikte takılabiliriz." |
| **6. Senaryo** | Online bir mesaj geldi. “Selam, biraz önce arkadaşın Selim ile tanıştım! Bana senden bahsetti, seninle de tanışmak isterim. Bana adresini yazar mısın? |

# Pardon kimsiniz?

## Senaryo 1

Tanımadığın birinden şöyle bir mesaj aldın: "Selam! Eğlenceli birisine benziyorsun. Bir ara takılmaya ne dersin? Beni arkadaş listene ekler misin? -Can"

- **Can'ı dikkate alma.** Tanımıyorsan konuşmamayı tercih edebilirsin. Bu kadar basit.
- **"Can merhaba. Tanışıyor muyuz?"** Emin değilsen önce sor.
- **Can'ı engelle.** Kim olduğunu kontrol edip engellemeye karar verirsen bu kişiden başka mesaj almazsın.
- **Can'ı arkadaş listene ekle.** Kim olduğundan emin olmadıkça önerilmez.
- **Can'ın profilini kontrol et.** Uygun görünüyorsa arkadaş listene ekleyebilirsin. Ama dikkatli ol. Profil kolayca oluşturulabilen bir şey! Kimlerle bağlantıda olduğunu görmek için bu kişinin arkadaş listesine bak. Arkadaş grubu gerçek olup olmadığını anlamanın bir yollarından birisidir.
- **Bu kişiye kişisel bilgi ver.** "Mahallede yeni birileriyle tanışmak harika!" gibi bir mesaja yanıt vermeli misin? Buraya yeni taşındım. Okuldan sonra buluşmaya ne dersin (Atatürk Ortaokuluna gidiyorum)"? Kesinlikle olmaz! Tanımadığın birine kişisel bilgilerini vermek hiç doğru değil. Özellikle de online ortamda.

## Senaryo 2

Cep telefonunuza tanımadığınız birisinden kısa mesaj geldi. "Selam, ben Özlem! Geçen yaz tanışmıştık, hatırladın mı?"

- **Özlem'i engelle.** Gerçekten tanıdığın biriyse engellemek kabalık olabilir. Bu seçeneği, o kişiyi gerçekten tanıyor ama sana artık mesaj göndermesini istemiyorsan ya da geçen yaz Özlem diye birisiyle tanışmadıysan tercih edebilirsin.
- **Özlem'i dikkate alma.** Yukarıda da belirttiğimiz gibi bu kişiyi tanımıyorsan konuşmasan iyi olur. Doğrusu bu.
- **"Merhaba Özlem. Tanışıyor muyuz?"** Ne yapacağından emin değilsen doğru davranış bu olacaktır.
- **"Selam! Ne var ne yok? Yeniden haberleşmek güzel."** Bu kişiyi geçen yazdan hatırlıyorsan böyle yazmanda bir sakınca yok.
- **"Saçların kızıldı, değil mi?"** Bu kişiyi tanıdığından emin değilsen hatırlamana yardımcı olacak birkaç bilgi almaya çalışabilirsin.
- **"Seni hatırlamıyorum, ama yine de bir ara buluşabiliriz."** Bu hiç iyi bir fikir değil. Tanımadığın birine buluşmayı teklif etmemelisin.

Bir sonraki sayfada devam ediyor →

## Kimlik avı kopya kağıdı: 2. Etkinlik (devamı)

### Senaryo 3

Zeynep Hanım ile matematik dersinden sonra cep telefonuna şöyle bir mesaj geliyor. "Zeynep Hanım'ın matematik sınıfından Berk ben. Ödevi anladın mı?"

- **Berk'i dikkate alma.** Her zaman olduğu gibi bu kişiyi tanımıyorsan cevap vermek zorunda değilsin.
- **Berk'i engelle.** Zeynep Hanım'ın matematik sınıfında Berk adında biri olmadığından eminsen doğrusu bu olacaktır.
- **"Selam Berk. Derste arkamda mı oturuyordun?"** Emin değilsen şöyle sorabilirsin.
- **"Evet. Okuldan sonra anlatırım."** Sadece bu kişinin kim olduğundan eminsen böyle yazmak doğru olacaktır.
- **"Matematik öğretmenim Zeynep Hanım değil.Ali Bey."** Söyledikleri yüzünden bu kişiye güvenmiyorsan en iyisi mesajı dikkate almamaktır. Matematik öğretmeninin adı gibi kişisel bilgileri vermemen gerekir.
- **"Numaram (532) 555 3444."** İyi bir fikir değil. Bu kişiyi tanıdığından emin değilsen kişisel bilgilerini paylaşmak doğru olmaz.

### Senaryo 4

Takip etmediğin birinden bir mesaj aldın. "Selam! Yazdıklarına bayılıyorum, ÇOK komiksin! Bana telefon numaranı yazsana, daha çok konuşuruz böylece!"

- **soccergirl12'yi dikkate alma.** İstemezsen cevap vermek zorunda değilsin.
- **soccergirl12 kullanıcısını engelle.** Bu kişinin şüpheli olduğunu düşür ve engellersen bir daha seninle iletişim kuramaz.
- **"Merhaba, tanışıyor muyuz?"** Emin değilsen kişisel bilgilerini vermeden önce sorular sorabilirsin.
- **"Olur, numaram..."** Bu yanlış! Bu kişinin kim olduğunu doğrulasan bile sosyal medyada kişisel bilgilerini vermek iyi bir fikir değil. İletişim kurmak için başka bir yol düşün. Bu anne baban, öğretmenlerin veya güvendiğin birisi üzerinden olabilir.

### Senaryo 5

Tanımadığın biri sohbet mesajı gönderdi. "Bugün seni Matematik sınıfında gördüm. Çok tatlısın! Adresini öğrenebilir miyim? Birlikte takılabiliriz."

- **Bu mesajı dikkate alma.** Doğru bir seçenek.
- **Bu kişiyi engelle.** Birisi hakkında hoşuna gitmeyen bir şeyler varsa tereddüt etme.
- **"Kimsiniz?"** Pek doğru bir adım değil. Mesaj şüpheli geliyorsa cevap vermemek veya engellemek daha iyi olacaktır.
- **"Elif sen misin? Sen de hoşsun! Uzay Apt. No: 34'te oturuyoruz."** Kim olduğunu bilsen bile bu pek de iyi bir fikir değil. Yeni birisine adresini veya başka kişisel bilgilerini vermeden önce tanıdığını düşünsen bile önce kontrol edip emin ol.

### Senaryo 6

Şöyle bir mesaj aldın: "Selam, arkadaşın Selim ile tanıştım! Bana senden bahsetti, seninle de tanışmak isterim. Bana adresini yazar mısın?

- **Bu mesajı dikkate alma.** Bu kişiyi tanımıyorsan, ama Selim adında bir arkadaşın varsa en güvenlisi yanıt vermeden önce Selim'e sormak olacaktır.
- **Engelle.** Bu kişiyi tanımıyorsan ve Selim adında bir arkadaşın da yoksa en doğru seçenek ileride seninle iletişim kuramaması için bu kişiyi engellemektir.
- **"Kimsiniz?"** Bu kişiyi tanımıyorsan bunu sormak pek de iyi bir fikir değildir. Selim cevap verene kadar bir şey yazmamak daha doğru olacaktır.

## Gerçek Olduğundan Emin Ol: 3. Etkinlik

# Interland: Reality River

Interland'dan geçen nehir gerçekler ve kurgular üzerinde akıyor. Ama bazen bir şey göründüğü gibi olmayabilir. Suyun en hızlı aktığı yerden karşıya geçmek için aklınızı kullanın ve kimlik avcısının oyununa gelmeyin.

Masaüstünüzde veya mobil cihazda (ör. tablet) bir web tarayıcısını açın, **g.co/Interland** adresine gidin ve Reality River oyun seçeneğine girin.

## Tartışma Konuları

Reality River öğrencilerin düşünme şeklini geliştirir. Oyundan sonra bu sorular, oyunun temalarını tartışma sürecine destek olur.

- Online bir şeyin gerçek mi sahte mi olduğuna karar vermenin gerektiği bir zamanı bizimle paylaş. Ne gibi işaretler dikkatini çekti?
- Karşındaki kimlik avcısı mıydı? Davranışlarından ve oyunu nasıl etkilediğinden bahset.
- Reality River oynamak, ileride online ortamda işaretleri ve kişileri nasıl değerlendireceğini değiştirdi mi?
- Bu derslere katıldıktan ve oyunu oynadıktan sonra sence neyi farklı yaparsın?
- Belirli bir online durum ile ilgili olarak "sorunlu" bir şeyler olduğunu gösteren işaretler ne olabilir?
- Online ortamda bir şeyler şüpheli olduğunda nasıl hissedersin?
- Bir şeyin gerçek olup olmadığı konusunda şüphelerin varsa ne yapman gerekir?

# Sırların Sende Kalsın

## Gizlilik ve güvenlik konusunda gerçekçi olma

### Derse genel bakış

1. Etkinlik: **Mükemmel bir şifre nasıl oluşturulur?**
2. Etkinlik: **Şifrenizi kendize saklayın**
3. Etkinlik: **Interland: Tower of Treasure**

### Temalar

İnternet gizlilik ve güvenlik sorunlarının her zaman için net bir doğru ve yanlış çözümleri yoktur. Sizi siz yapan kişisel ve gizli bilgilerinizi korumak doğru soruları sormak ve kendi cevaplarınızı bulmak demektir.

### Hedefler

- ✓ **Gizliliğin** neden önemli olduğunu ve internet güvenliği ile neden ilgili olduğunu öğrenin.
- ✓ **Güçlü şifre oluşturma** alıştırması yapın.
- ✓ **Korsanlara ve diğer tehditlere** karşı koruma sağlayan araçları ve ayarları gözden geçirin.

### Üzerinde durulan standartlar

**Öğretmenler için ISTE Standartları:** 1a, 1b, 2a, 3b, 4a, 4b, 4c, 4d, 5a **Öğrenciler için ISTE Standartları 2016:** 1d, 2a, 2d **AASL Öğrenim Standartları:** 1.1.8, 1.3.5, 2.1.3, 2.3.1, 2.3.3, 3.1.2, 3.1.5, 3.1.6, 3.2.2, 3.3.3, 4.3.4, 4.4.4 **C3:** II:A, II:B, II:C, III:A, III:B

# Sırların Sende Kalsın
## Sözlük

**Gizlilik**
Kendinizin ve başkalarının kişisel bilgilerini koruma

**Güvenlik**
Donanım ve yazılımın güvenliğini sağlamak için iyi alışkanlıklardan yararlanma

**İki adımlı doğrulama**
Bir hizmette oturum açılabilmesi için iki adım gereken bir güvenlik süreci. Örneğin şifrenizi ve mesaj olarak telefonunuza gönderilen bir kodu girmeniz gerekebilir.

**Güvenlik jetonu**
Erişim yetkisi vermek için yanınızda taşıdığınız bir anahtarlık veya küçük donanım cihazı

**Şifre**
Bir şeye erişmek için kullanılan gizli bir kombinasyon

## Sırların Sende Kalsın: 1. Etkinlik

# İyi bir şifre nasıl oluşturulur?

Öğrenciler nasıl güçlü şifre oluşturacaklarını öğrenirler ve oluşturduktan sonra gizli kalmasını sağlarlar.

## Hedefler

- ✓ **Şifrelerini sadece** anne babaları veya yasal vasileri ile paylaşmalarının önemine dikkat çekin.
- ✓ **Cihazlarını koruma altına alan** şifreler hakkında bilgi alın.
- ✓ **Tahmin edilmesi zor ve hatırlanması kolay** şifrelerin nasıl oluşturulacağını öğrenin.
- ✓ **Oturum açma ayarları için** iki adımlı doğrulama da dahil olmak üzere doğru güvenliği seçin.

## Haydi konuşalım

**Pişman olmaktansa tedbirli olmak en iyisidir**

Dijital teknoloji sınıftaki ve dışarıdaki arkadaşlarla, öğretmenlerle ve daha pek kişiyle iletişim kurmayı kolaylaştırıyor. Dünyayla türlü şekillerde iletişim kurabiliriz. E-posta, kısa mesaj ve anında mesajla. Kelimelerle, resimlerle ve videolarla, telefon yoluyla, tabletlerle ve dizüstü bilgisayarlarla. (Arkadaşlarınla nasıl bağlantı kuruyorsun?)

Bilgiyi paylaşmamızı kolaylaştıran araçlar aynı zamanda korsanların ve sahtekarların da bu bilgileri çalmasını ve cihazlarımıza, ilişkilerimize ve itibarımıza zarar vermek için kullanmalarını kolaylaştırıyor.

İnternetteki itibarımızı oluşturmaya yarayan tüm bilgileri koruma altına almak basit, ama akıllıca yollarla mümkün. Örneğin, cihazlarımızda ekran kilitleri kullanmak, çalınabilecek veya kaybolabilecek cihazlarda kişisel bilgilerimizi bulundurma konusunda dikkatli olmak ve hepsinden önemlisi iyi şifreler seçmek bunlardan bazıları.

• En sık kullanılan iki şifre hangisi tahmin edin. (Yanıt: “1 2 3 4 5 6” ve “sifre”)
• Şimdi de bazı kötü şifre örneklerine bakalım.(Örnek: adınız, telefon numaranız, “çukulata”)

Kimler bu şifrelerin iyi olduğunu düşünüyor?

Bir sonraki sayfada devam ediyor →

## Sırların Sende Kalsın: 1. Etkinlik (devamı)

### Etkinlik

**Gereken malzemeler:**

- Öğrenciler veya gruplar ya da öğrenciler için internete bağlı cihazlar
- Tebeşir/beyaz tahta veya projeksiyon ekranı
- Öğrenciler için broşür: Güçlü şifre oluşturma yönergeleri

Şimdi bulmaca oyunu oynayarak yeni öğrendiklerimizi pekiştirelim.

**1. Şifre oluşturun**
Hepimiz iki kişilik gruplara ayrılacağız. Her grup 60 saniye içinde bir şifre oluşturacak.

**2. Şifreleri karşılaştırın**
İki takım birden şifrelerini tahtaya yazacak.

**3. Oylayın!**
Her şifre grubu için oy verecek, hangi şifrenin daha güçlü olduğunu tartışacağız.

### Ana Fikir

İşte ekstra güvenli bir şifre oluşturma fikirleri.

Unutmayacağınız eğlenceli bir ifade düşünün. Sevdiğiniz bir şarkı sözü, kitap adı, bir filmden replik ve benzer şeyler olabilir.

- İfadedeki her kelimenin ilk harfini veya ilk iki harfini seçin.
- Bazı harfler yerine sembol kullanın.
- Bazı harfleri büyük, bazılarını küçük harf yapın.

### Güçlü şifre oluşturma yönergeleri

İşte sırlarının güvende kalması için nasıl şifre oluşturacağınla ilgili bazı ipuçları.

**Güçlü şifreler,** kolayca hatırlayabileceğin, ama başkasının kolayca tahmin edemeyeceği açıklayıcı bir cümleye dayalıdır.

**Orta düzeyde güçlü şifreler,** güçlü olan, kötü yazılımlar tarafından kolayca tahmin edilemeyen, ancak seni tanıyan birisi tarafından tahmin edilebilecek şifrelerdir.

**Zayıf şifreler**, genellikle kişisel bilgilerin kullanıldığı, kırılması kolay ve seni tanıyan birisi tarafından tahmin edilebilecek şifrelerdir.

### YAPILACAKLAR

- Önemli hesaplarınızın her biri için benzersiz bir şifre kullanın.
- En az sekiz karakter kullanın
- Harf (büyük/küçük harf), sayı ve sembolleri bir arada kullanın.

### YAPILMAYACAKLAR

- Şifrenizde kişisel bilgi (ad, adres, e-posta, telefon numarası, Sosyal Güvence numarası, annenizin kızlık soyadı, doğum tarihi vb.) veya sık kullanılan kelimelere yer vermeyin.
- Takma adınız, okulunuzun adı, favori beyzbol takımınız gibi tahmin edilmesi kolay şifreler kullanmayın.
- Anne babanız veya yasal vasiniz dışında kimseyle şifrenizi paylaşmayın.

# Kendine sakla

Öğretmen, gizlilik ayarlarını özelleştirirken nereye bakılacağını ve ne aranacağını okul cihazını kullanarak gösterir.

## Hedefler

- ✓ **Kullandıkları online hizmetler için** gizlilik ayarlarını özelleştirme.
- ✓ **Kullandıkları siteler** ve hizmetlerde bilgi paylaşımı ile ilgili karar verme.
- ✓ **İki faktörlü** ve iki adımlı doğrulamanın ne olduğunu ve ne zaman kullanılacağını anlama.

## Haydi konuşalım

### Gizlilik eşittir güvenlik

Online gizlilik ve online güvenlik birbirleri ile yakından ilgilidir. Çoğu uygulama ve yazılım, ne tür bilgileri ve nasıl paylaştığımızı kotrol etmenin yollarını sunar.

Bir uygulama veya web sitesini kullandığında "Hesabım" ya da "Ayarlar" gibi seçenekleri ara. Burada şunlara karar verebilmeni sağlayan gizlilik ve güvenlik ayarlarını bulabilirsin:

- Profilinde hangi bilgiler görünür durumda
- Yayınladıklarını, fotoğraflarını, videolarını veya paylaştığın diğer içerikleri kimler görebilir?

Gizliliğini korumak üzere bu ayarları nasıl kullanacağını öğrenmek ve bu ayarları güncel tutmak, mümkün olduğu kadar güvende olmana yardımcı olur.

## Etkinlik

**Gereken malzemeler:**

- Projeksiyona bağlı ve sınıfta gösterim için uygun bir örnek hesabı gösterebilen (ör. geçici bir e-posta veya web sitesi hesabı) bir okul cihazı

### 1. Seçenekleri gözden geçirme

Okul cihazım projeksiyon ekranına bağlı. Şimdi bu uygulamanın ayarlar sayfasına gidelim. Seçeneklerimiz arasında şunların yer aldığını görebiliriz:

- Şifreyi değiştirme
- Bilinmeyen bir cihazdan birisi hesabında oturum açmaya çalıştığında uyarı alma
- Fotoğraflar ve videolar da dahil olmak üzere online profilini sadece seçtiğin aile ve arkadaşlar grubunun görebilmesini sağlama
- İki faktörlü veya iki adımlı doğrulamayı etkinleştirme

### 2. Ek doğrulama seçenekleri

Şimdi iki adımlı ve iki faktörlü doğrulamaları konuşalım.

- İki adımlı doğrulama: Hesabında oturum açtığında iki adımın tamamlanması gerekir. Örneğin, şifreni girmen istenebilir VE size kısa mesajla 10 dakika içinde kullanım süresi dolan bir kod gönderilir.
- İki faktörlü doğrulama: Sistem oturum açabilmen için senden iki tür bilgi ister. Örneğin, normal şifreni VE parmak izini isteyebilir.

Bir sonraki sayfada devam ediyor →

## Sırların Sende Kalsın: 2. Etkinlik (devamı)

Hangi gizlilik ve güvenlik ayarları senin için doğru? Bunu anne babanla veya velinle tartışman gerekir. Ama unutma, en önemli güvenlik ayarı senin aklında. Kişisel bilgilerinin ne kadarını, ne zaman ve kiminle paylaşacağına sen karar verirsin.

### Ana Fikir

Önemli hesaplarınız için güçlü ve benzersiz bir şifre seçmek ilk iyi adımdır. Şifrelerinizi unutmamanız ve güvenli kalmasını sağlamanız gerekir.

Şifrelerinizi bir yere yazmak tam olarak yanlıştır diyemeyiz. Ancak bu durumda şifrelerinizi hemen göze çarpacak şekilde bilgisayarınızın üzerinde veya masanızda bırakmayın. Listenizi kolayca görülmeyecek bir yerde güvenli bir şekilde saklayın ve kendinizi koruyun.

## Sırların Sende Kalsın: 3. Etkinlik

# Interland: Tower of Treasure

Tehlike! Kule kilitli değil. İnternot'ların kişisel bilgi ve şifre gibi değerli bilgileri yüksek risk altında. Korsandan daha hızlı düşün ve sırlarını ilk ve son olarak güvence altına almak için hiçbir adımda kırılamaz bir şifre oluştur.

Masaüstü veya mobil cihazda (ör. tablet) bir web tarayıcısını açın, **g.co/Interland** adresine gidin ve Tower of Treasure oyun seçeneğine girin.

## Tartışma Konuları

Tower of Treasure öğrencilerin düşünmesini sağlayacak. Oyundan sonra, oyunun temaları ile ilgili tartışma başlatmak için şu sorulardan yararlanabilirsin.

- Süper güçlü bir şifrenin özellikleri nelerdir?
- Gerçek hayatta güçlü şifre oluşturmak ne zaman önemlidir? Bunu nasıl yapacağınla ilgili ne tür ipuçları öğrendin?
- Korsan ne demektir? Bu karakterin davranışlarını ve oyunu nasıl etkilediklerini açıkla.
- Tower of Treasure, bilgilerini gelecekte nasıl koruyacağınla ilgili planlarını değiştirdi mi?
- Bu derslere katıldıktan ve oyunu oynadıktan sonra daha önce yaptığın neyi farklı yaparsın?
- "Süper güçlü" testini geçecek üç şifre oluştur.
- Korunması gereken hassas bilgilere ne gibi örnekler verebilirsin?

4. Ders: İyi Ol, Özel Ol

# İyi Ol, Özel Ol

## İnternette olumlu davranışın gücü

### Derse genel bakış

1. Etkinlik: **Olumsuz davranışa nasıl karşı çıkabilirim?**
2. Etkinlik: **...ama kibarca söyleyin!**
3. Etkinlik: **Söyleme tarzınıza dikkat edin**
4. Etkinlik: **Harekete geçme**
5. Etkinlik: **Interland: Kind Kingdom**

### Temalar

Dijital dünya, çocuklar için bazı zorlukları beraberinde getiriyor. İnternette sosyal işaretleri okumak zor olabilir. Gerçek ismini kullanmıyor olmak olumsuz davranışları teşvik edebilir ve online ortamda zorbalık kolayca tekrarlanır ve dijital ayak izi bırakır.

Ancak internet, olumsuzluğun yanı sıra iyiliğin çoğalmasını da sağlayabilir. İyiliği, empatiyi yaymayı ve olumsuzluğa ve tacize nasıl yanıt verileceğini öğrenmek sağlıklı ilişkiler oluşturmanın temelidir ve bazen zorbalığa, depresyona, akademik engellere ve diğer sorunlara neden olan yalıtılmışlık duygusunu azaltır.

Yapılan bir araştırmaya göre, çocuklara internette olumsuz davranma demek yerine etkili bir güvenlik eğitimi vermek, olumsuz davranışların nedenlerini ortadan kaldırmada daha fazla işe yaramaktadır. Bu etkinlikler öğrencileri en başından itibaren olumlu iletişim kurmaya teşvik etmekte ve karşılaştıklarında olumsuz davranışlarla nasıl baş edeceklerini öğretmektedir.

### Hedefler

- ✓ **İnternette** olumlu davranmanın nasıl bir şey olduğunu tanımlayın.
- ✓ **İnternette veya çevrimdışıyken** olumlu davranmak ne demek tanımlayın.
- ✓ **Online ortamda** iletişim kurarken olumlu davranarak örnek olun.

### Üzerinde durulan standartlar

**Öğretmenler için ISTE Standartları:** 1b, 1d, 2a, 3b, 4a, 4b, 4c, 5a **Öğrenciler için ISTE Standartları 2016:** 2a, 2b **AASL Öğrenim Standartları:** 1.1.5, 1.3.3, 1.3.5, 2.1.3, 2.3.1, 2.3.2, 2.3.3, 2.4.1, 2.4.3, 3.1.2, 3.1.5, 3.1.6, 3.2.2, 3.3.2, 3.3.3, 3.3.6, 4.1.7, 4.2.3, 4.3.4, 4.4.4 **C3:** I:B, I:D, I:E, I:F, I:H, II:C

# İyi Ol, Özel Ol
## Sözlük

**Zorbalık**
Zaman içinde tekrarlanan (veya tekrarlanma ihtimali olan) istenmeyen, agresif davranışlar

**Seyirci Kalan**
Kötü bir davranışta araya girme veya bildirme gücü olan,ancak bu davranışı durdurmak için bir şey yapmayan kişi

**Müdahale Eden**
Uygunsuz davranışı durduran ve/veya bildiren kişi

**Taciz**
Davetsiz ve hoş karşılanmayan sözlü ya da fiziksel bir davranış nedeniyle istenmeyen veya düşmanca bir durum oluşturmak

**Şiddetlendirme**
Bir şeyi daha sesli ve güçlü hale getirmek

**Engelleme**
Birisinin profilinize ulaşmasını, size mesaj göndermesini ve başka şeyler yapmasını engellemek

İyi Ol, Özel Ol: 1. Etkinlik

# Müdahale eden kişi nasıl olurum?

Öğrenciler bir zorbalık durumunda taraf olan üç rolü belirleme (zorbanın kendisi, hedef olan kişi ve seyirci kalan kişi) görgü tanığı veya hedef olmaları durumunda ne yapmaları gerektiğinin alıştırmasını yaparlar.

## Hedefler

- ✓ **Seyirci kalan veya müdahale eden taraf** ne demek değerlendirin.
- ✓ **Karşılaştığınızda** zorbalığa hangi şekillerde cevap verebileceğinizi öğrenin.
- ✓ **Tacizle karşılaştığınızda** nasıl davranacağınızı bilin.

## Haydi konuşalım

**İyilik neden önemli?**

Bazen kendimize her kullanıcı adının ve avatarın arkasında duyguları olan gerçek bir insan olduğunu ve ona göre davranmamız gerektiğini hatırlatmamız gerekir. Zorbalık veya başka uygunsuz bir davranış yaşandığında, çoğunlukla üç taraf yer alır.

- Bir veya birden fazla **zorba**.
- Zorbalığa uğrayan kişi, yani **hedef** veya **kurban.**
- ve **seyirci dediğimiz bir veya daha fazla kişi.**

Seyirci, uygunsuz bir davranışta araya girme veya bildirme gücü olan, ancak bu davranışı durdurmak için bir şey yapmayan kişidir. Amacınız kötü davranışla mücadele eden ve iyiliği, olumlu davranış için kötüye karşı çıkan, müdahale eden kişi olmaktır. Küçük bir olumlu davranış internet ortamında çok işe yarayabilir. Ama bunun tersi de doğrudur: Küçük bir olumsuzluk büyük ve çirkin bir şeye dönüşebilir.

İşte müdahale eden kişilerin, internette zorbalığı ve olumsuz mesajları durdurmaya nasıl yardımcı olabileceği ile ilgili birkaç örnek:

- **İyi örnek olun.**
  Arkadaşlarınız arasında olumlu davranış diğerlerini de olumlu davranmaya teşvik eder.

- **Dost olun.**
  Hem internette hem fiziksel dünyada dostça davranmak sınıf arkadaşlarınıza yalnız olmadıklarını gösterir. Bu da zorbalığa uğrayan veya kendisini iyi hissetmeyen arkadaşlarınıza yardımcı olur.

- **Kötü davranışın seyirci bulmasına izin vermeyin.**
  Kırıcı yorumları ya da yayınları "beğenmeyin" veya yanıtlamayın. Bazen zorbalar dikkat çekmek için agresif davranırlar ve siz ve arkadaşlarınız onları cesaretlendirmezseniz bir daha yapmayabilirler.

- **Kırıcı mesajları devam ettirmeyin.**
  Bunun yerine mesajı gönderen kişiye mesajın komik veya kabul edilebilir olmadığını söyleyin ve destek olmak, gerekirse yardım almasına yardımcı olmak için hedef olan kişiyle iletişim kurun.

- **Kötü niyetli, zorbalık içeren davranışı bildirin.**
  Anne babanıza, öğretmeninize, arkadaşınıza veya kardeşinize söylemek için online raporlama araçlarından yararlanın.

Bir sonraki sayfada devam ediyor →

## İyi Ol, Özel Ol: 1. Etkinlik (devamı)

### Etkinlik

**Grup olarak pratik yapın**

Online ortamda zorbalığa veya başka kötü bir davranışa maruz kalırsanız işte yapabilecekleriniz.

**Hedef bensem...**

- Cevap vermeyebilirim
- Engelleyebilirim
- Anne babama, öğretmenime, kardeşime veya arkadaşıma söyleyebilirim.

Peki kötü bir şeye tanık olursanız ne yapabilirsiniz?

**Kötü bir olaya tanık olduysam...**

- İyi olmaya çalışırım
- Engelleme
- Anne babama, öğretmenime, yani yardımcı olabilecek birine söyleyebilirim.

Tanık olarak harekete geçerseniz seyirci kalan yerine müdahale eden olursunuz.

### Ana Fikir

Başkalarını savunmak, kırıcı davranışları bildirmek veya daha kötü sonuçlar doğurmasını engellemek üzere için bir şeyi göz ardı etmek gibi farklı stratejiler arasından seçim yapabilirsiniz. Online ortamın güzel ve kaliteli olmasından herkes sorumludur.

# ...ama kibarca söyleyin!

Bu etkinlikte, olumsuz etkileşimleri olumluya çevirmeyi öğrenmek için öğrenciler birlikte çalışacak ve olumsuz yorumlara farklı bir açıdan bakacaklar.

## Hedefler

- ✓ Duygularınızı ve düşüncelerinizi olumlu şekilde ifade edin.
- ✓ Olumsuzluğa yapıcı ve medeni şekilde yanıt verin.

## Haydi konuşalım

**Olumsuzu olumluya dönüştürme**

Sizin yaşınızdaki çocuklar pek çok farklı çeşitte içerik üretebilirler. Bunlar da kötü davranışların artmasına neden olacak olumsuz mesajlar içerebilir.

- Siz (veya tanıdığınız birisi) web'de hiç iyi niyetli bir davranışla karşılaştınız mı? Bu nasıl hissetmenize sebep oldu?
- Siz (veya tanıdığınız birisi) web'de olumsuz tavır gösteren birisi ile karşılaştınız mı? Kendinizi nasıl hissettiniz?
- Olumsuz etkileşimleri olumluya dönüştürmek için ne tür basit adımlar atabiliriz?

Dostça olmayan yorumları başka şekilde ifade ederek ve online ortamda kurduğumuz iletişimde kullandığımız tona dikkat ederek olumsuz duygulara yapıcı şekilde yanıt verebiliriz.

## Etkinlik

**Gereken malzemeler:**

- Tebeşir/beyaz tahta veya projeksiyon ekranı
- Öğrenciler için broşür: ...ama kibarca söyleyin!
- Yapışkan not kağıtları ve öğrenciler için cihazlar

**1. Yorumları okuyun**

Hepimiz olumsuz yorumlara bakıyoruz

**2. Yorumları düzelterek yazın**

Şimdi üç kişilik gruplara ayrılalım ve bu yorumlara iki farklı türde yanıt vermeye çalışalım:

- Aynı veya benzer noktalara olumlu ve yapıcı bir şekilde nasıl değinebilirdin?
- Sınıf arkadaşlarından biri bu tarz yorumlar yapsaydı sohbeti daha olumlu yönlendirmek için nasıl yanıt verebilirdin?

**3. Yanıtları sunun**

Şimdi her grup iki durum için de yanıtlarını paylaşsın.

## Ana Fikir

Olumsuz bir şeye olumlu bir davranışla cevap vermek daha eğlenceli ve ilginç bir sohbetle sonuçlanabilir. Bu tür bir adım, kibar olmayan bir yorumun neden olacağı tatsızlığı gidermekten çok daha iyidir.

## Çalışma Sayfası: 2. Etkinlik

# ...ama kibarca söyleyin!

Aşağıdaki yorumları okuyun. Her yorumdan sonra şunları tartışın:

**1. Aynı veya benzer noktalara olumlu ve yapıcı bir şekilde nasıl değinebilirdin?**

**2. Sınıf arkadaşlarından biri bu tarz yorumlar yapsaydı sohbeti daha olumlu yönlendirmek için nasıl yanıt verebilirdin?**

Düşüncelerinizi yazmak için her yorumun altındaki boş bölümü kullanın.

“Leyla sınıfta bu hafta sonu kamp gezisine gitmeyen tek öğrenci.”

"Herkes yarın mor bir şeyler giysin, ama Leyla'ya söylemeyin."

"Maalesef partime gelemezsin. Çok pahalı."

"Alınma ama yazın çok feci. Bu projede başka gruba geçsen iyi olacak."

"Ben utandım onun yerine. Şarkı söyleyebildiğini mi sanıyor??"

"Hesabının şifresini vermen şartıyla grubumuza katılabilirsin."

“Selma'yı şirinlere benzeten bir ben miyim?”

“👎👎👎”

İyi Ol, Özel Ol: 3. Etkinlik

# Söyleme tarzınıza dikkat edin

Öğrenciler kritik düşünebilme ve online bir şeyler gönderip aldıklarında yanlış anlamaları ve çatışmaları engelleme pratiği yapmak için kısa mesajların arkasındaki duyguları yorumlar.

## Hedefler

- ✓ **Neyi nasıl ifade edeceğinizi** seçerken akıllıca karar verin.
- ✓ **Bir arkadaşınızla** yüz yüze iletişim kurmayı kısa mesaj göndermeye veya mesajlaşmaya tercih edeceğiniz durumları belirleyin.

## Haydi konuşalım

**Yanlış anlamak kolay**

Gençler değişik zamanlarda farklı iletişim türlerini kullanır, ancak sohbet ve kısa mesaj ile gönderilen mesajlar yüz yüzeyken veya telefonda söylenenden farklı anlaşılabilir.

- Hiç gönderdiğiniz kısa mesajın yanlış anlaşıldığı oldu mu? Mesela kısa mesajda yazdığınız bir şakayı arkadaşınızın ciddiye aldığı oldu mu?
- Hiç kısa mesaj veya sohbet sırasında başkasını yanlış anladığınız oldu mu? Durumun açıklığa kavuşması için ne yaptınız? Neyi farklı yapabilirdiniz?

## Etkinlik

**Gereken malzemeler:**

- Tahtaya yazılan veya yansıtılan örnek kısa mesajlar

**1. Mesajları gözden geçir**

Şimdi tahtadaki örnek kısa mesajlara bakalım:

- "Bu harika"
- "Her neyse"
- "Sana çok kızgınım"

**2. Mesajları sesli oku**

Her bir mesajı birisinin belirli bir ses tonunda (ör. sinirli, alaycı, samimi) sesli okumasını isteyeceğiz.

Ne fark ettin? Bunun için başkaları ne düşünür? "Mesajı gönderen" gerçekte ne demek istediğini daha iyi nasıl ifade edebilir?

## Ana Fikir

Birisinin sana yazdıklarını veya mesajlarını okurken gerçekte nasıl hissettiklerini anlamak zor olabilir. Bir sonraki iletişiminde doğru modu seçtiğinden emin ol ve insanların online ortamda söylediklerinden çok anlam çıkarmamaya çalış.

# Harekete geçme

Çocukların aynı zamanda yetişkinlere davranış modeli sergilemesi konusunda basit bir sınıf tartışması

## Hedefler

- ✓ **Yetişkinlerin** online davranışını yansıtır.
- ✓ **Yetişkinlerin** davranış şeklinin daha genç nesillere nasıl örnek olabileceğini düşün.

## Haydi konuşalım

**Yetişkinler çocuklara ne öğretebilir?**
İyi olmayı öğretmek önemlidir. Aynı zamanda verdiğimiz iyilik dersleri konusunda örnek olmak da önemlidir. Zorbalık ve tacizin sadece çocukların başına gelmediğini gösteren pek çok örnek bulunmaktadır. Yetişkinlerin birbirlerine online ortamda veya trafikte nasıl davrandığına bir bakın.

Sınıf arkadaşlarına ve diğer arkadaşlarına online veya değilken iyi davranmanın ne kadar önemli olduğunu konuşuyorduk. Peki yetişkinlerin birbirilerine negatif davrandıklarına şahit oldun mu? Yetişkinlerin birbirilerine zorbalık yaptığını gördün mü? (İsim vermemiz gerekmediğini hatırlatırım. Sadece nasıl davrandıklarından bahsedelim.)

Sence bazı çocuklar etraflarındaki büyüklerden görüp zorbalık yapıyor ya da iyi olmayan davranışlarda bulunuyor olabilir mi?

## Ana Fikir

Arkadaşlarınla birbirinize online ortamda nasıl davranacağın, neslinizin oluşturacağı dijital dünyayı önemli oranda etkileyecektir. Neslinizin bazı yetişkinlerin kendileri için oluşturduğundan daha iyi ve daha olumlu bir internet oluşturabileceğini düşünüyor musun?

Pek çok yetişkin bu konuda da iyi olacağınızı düşünüyordur...

# Interland: Kind Kingdom

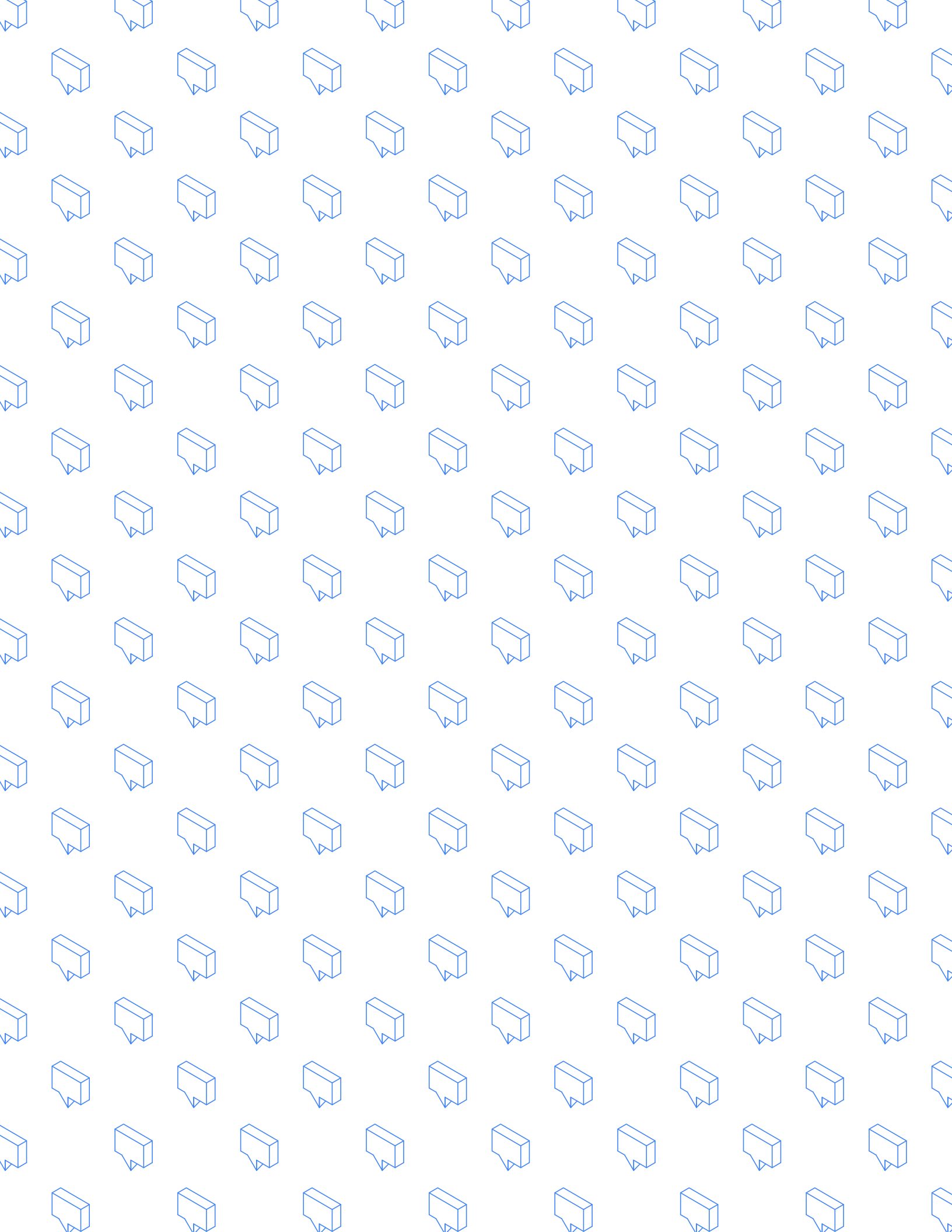
İster iyi ister kötü olsun tüm davranışlar bulaşıcıdır. Şehrin en popüler meydanında siber zorbalar sağa sola saldırıyor, her yere negatif enerjilerini yayıyorlar. Bu duruma bir son vermek için zorbaları durdurun ve bu kişileri gereken yerlere bildirin. Bu topraklara tekrar barış havası getirmek için diğer İnternotlara iyi davranın.

Masaüstü bilgisayarınızda veya mobil cihazınızda (ör. tablet) bir web tarayıcısı açın, **g.co/Interland** adresini ziyaret edin ve Kind Kingdom oyun seçeneğine gidin.

## Tartışma Konuları

Kind Kingdom oynamak öğrencileri düşünmeye teşvik edecek. Sonrasında, oyunun temaları ile ilgili tartışma başlatmak için şu sorulardan yararlanabilirsiniz.

- Kind Kingdom'da en çok hangi senaryo sana hitap ediyor ve neden?
- Bizimle internette başkalarını iyi olmaya yöneltmek için harekete geçtiğin bir zamanı paylaş.
- Hangi durumda birisini internette engellemek uygun olacaktır?
- Hangi durumda birisinin davranışını gerekli yerlere bildirmek uygun olacaktır?
- Sence neden Kind Kingdom'daki karaktere siber zorba deniyor? Bu karakterin özelliklerinden bahset ve sence bu karakterin davranışları oyunu nasıl etkiliyor?
- Bu oyun başkalarına davranış şeklini değiştiriyor mu?



5. Ders: Cesur Ol

# Bir Sorun Olduğunda Konuş

**İnternette Cesur davranmayı teşvik eden özet bir rehber**

## Genel Bakış

Bu derslerde sık sık yer verilen bir tavsiye, tüm internet faaliyetleri için geçerlidir. Şüpheli bir şey ile karşılaştığınızda bu konu ile ilgili olarak güvendiğiniz bir yetişkinle konuşun. Öğrenciler tüm derslerden bu bilgiyi almaktadır, ancak aşağıdaki durumlarda, hızlı bir başvuru kaynağı olarak "Bir sorun olduğunda konuş" ilkesi öğrencileriniz için en faydalı bilgi olarak değerlendirilebilir.

Öğrenciler her ihtiyaç duyduklarında güvendikleri yetişkinle "konuşabilirler." Sık karşılaşılan durumlardan bazıları şunlardır:

- Hesaplarının ele geçirilmiş olduğunda şüpheleniyorlar. (Tartışma fırsatı: Hesabınızın güvenliğini daha güçlü hale getirmek için ne yapabilirsiniz? Bkz. sayfa 31.)
- Şifreyi hatırlayan güvenilir bir yetişkinden yardım istemeleri gerekir.
- Bir şeyin sahte olup olmadığından emin değiller veya aldatılmış olabileceklerinden şüpheleniyorlar. (Tartışma fırsatı: Tehlike işaretleri neler? Bkz. sayfa 18.)
- İnternette birisi kendilerini rahatsız eden bir şeyi tartışmaya çalışıyor.
- Bir yabancı şüpheli bir şekilde iletişim kurmaya çalışıyor.
- İnternette iyi ve *kötü* davranışları tartışmak istiyorlar.
- Online ortamda paylaşmamaları gereken bir şeyi paylaşmış olabileceklerinden endişe ediyorlar.

Sınıfınızda açık iletişimin önemini vurgulayın ve ihtiyaç duyduklarında destek için yanlarında olduğunuzu hatırlatın. Bir öğrenci paneli veya çalışma grubu (özellikle yaşça daha büyük öğrencilerle) bu konu başlığına öğrenci temsilciliği oluşturmada etkilidir.