PROJE FİKRİ:

Proje Adı: Hacker Avcısı

Proje Konsepti ve Amacı

Bu projeyi, siber güvenlik farkındalığını artırmayı amaçlayan eğitici ve interaktif bir oyun olarak tasarladım. Günümüzde bireyler ve kurumlar, hacker saldırılarına, kimlik avı (phishing) tehditlerine ve güvenlik açıklarına karşı savunmasız olabilmektedir. Bu oyunun temel amacı, oyunculara eğlenceli bir şekilde siber güvenlik bilinci kazandırmak ve onları çevrimiçi tehditlere karşı bilinçlendirmektir.

Hedef

- Kullanıcıların güvenli şifreler oluşturmayı öğrenmesi
- Kimlik avı (phishing) saldırılarını tanıma becerisinin geliştirilmesi
- Siber güvenlik açıklarını kapatma ve önlem alma bilincinin artırılması
- Gerçek hayattaki siber tehditleri deneyimleyerek öğretici bir süreç sunması

Hedef Kitle

Bu projeyi, geniş bir kullanıcı kitlesine hitap edecek şekilde tasarladım:

- Bilişim güvenliği konusunda temel bilgi edinmek isteyen öğrenciler
- Şirket çalışanları ve yöneticiler (Kurumsal güvenlik farkındalığını artırmak için)
- Genel internet kullanıcıları (Siber tehditlere karşı bilinçlenmek isteyen herkes)

Oyun Teması ve Hikayesi

Oyuncu, bir şirketin BT güvenlik uzmanı olarak işe başlar. Ancak şirket, hacker saldırılarının hedefi haline gelmiştir. Oyuncunun görevi, çalışanları bilinçlendirmek, güvenlik önlemlerini almak ve hacker saldırılarını durdurmaktır. Farklı seviyelerde oyuncuya gerçek dünya tehditlerini simüle eden senaryolar sunulur ve oyuncu doğru kararlar alarak şirketin güvenliğini sağlamaya çalışır.

Oyun Modları

- Senaryo Bazlı Görevler: Oyuncu belirli güvenlik senaryolarında doğru seçimler yaparak şirketi korur.
- Quiz ve Eğitici Mini Oyunlar: Kullanıcı, siber güvenlik bilgilerini test eden quiz'lere ve interaktif görevlerle öğrenme sürecine katılır.
- Gerçek Hayattan Örnekler: Oyunda kullanılan phishing saldırıları, şifre kırma teknikleri ve güvenlik açıkları, gerçek dünyada yaşanan siber saldırılardan ilham alarak tasarladım.

Bu projeyi, oyun tabanlı öğrenme (game-based learning) yaklaşımını benimseyerek, siber güvenlik eğitimlerini sıkıcı olmaktan çıkarıp eğlenceli ve etkileşimli hale getirdim. Oyunun sonunda kullanıcılar, siber tehditleri tanıma ve önlem alma konusunda bilinçlenmiş olacaklardır.

OYUN MEKANİĞİ VE ÖĞRENME SÜRECİ:

Oyun Mekaniği

Oyuncu, bir şirketin siber güvenlik uzmanı olarak göreve başlar ve şirketi hacker saldırılarına karşı korumak için çeşitli kararlar alır. Oyun, interaktif seçimler ve stratejik karar verme üzerine kuruludur. Oyuncular, şirketin güvenlik açıklarını belirleyip, bu tehditleri önlemek için uygun önlemleri almak zorundadır.

Temel Mekanikler:

- Seçim Tabanlı Oynanış: Oyuncuların güvenlik önlemlerini belirleyerek şirketin savunmasını güçlendirmesi gerekir.
- Risk Yönetimi: Oyuncular, şirketin güvenlik seviyesini artırmak için farklı stratejileri değerlendirmelidir.
- Zaman Yönetimi: Oyunda belirli tehditler zamana duyarlıdır ve oyuncuların hızlı karar vermesi gerekebilir.
- Geri Bildirim Mekanizması: Oyuncuların yaptığı seçimlere bağlı olarak pozitif veya negatif geri bildirimler verilir.

Öğrenme Süreci

Oyun, siber güvenlik farkındalığını artıran aşamalı bir öğrenme süreci sunar:

1. **Seviye 1: Şifre Analizi**
    - Oyuncuya çeşitli şifreler sunulur ve bunların güvenli olup olmadığını değerlendirmesi istenir.
    - Yanlış şifre seçimlerinde sistem saldırıya uğrar ve oyuncuya doğru şifre kriterleri öğretilir.
2. **Seviye 2: Şifre Oluşturma**
    - Oyuncu, güçlü bir şifre oluşturmalı ve sistemin değerlendirme kriterlerine uygun hale getirmelidir.
    - Doğru seçimlerle şifre kırılmaya karşı daha dayanıklı hale gelir.
3. **Seviye 3: Kimlik Avı (Phishing) Tespiti**
    - Oyuncuya sahte ve gerçek e-postalar gösterilir.
    - Oyuncunun sahte e-postaları tespit etmesi ve çalışanları bilinçlendirmesi beklenir.
4. **Final Seviye: Siber Savunma Planı Oluşturma**
    - Oyuncu, şirketin güvenliğini artırmak için stratejik kararlar alır.
    - Çalışanlara güvenlik eğitimi verir, güvenlik duvarı ayarlarını optimize eder ve sistem güncellemelerini yapar.
    - Oyuncunun seçimlerine bağlı olarak şirketin güvenlik seviyesi belirlenir ve oyunun sonucu şekillenir.

Oyun sonunda oyuncu, aldığı kararların sonuçlarını görerek siber güvenlik konularında bilinçlenmiş olur ve bu bilgileri gerçek hayatta nasıl uygulayabileceğini öğrenir.O seçimler üzerine kuruludur.

Temel Mekanikler:

- Seçim Tabanlı Oynanış: Oyuncuların doğru güvenlik önlemlerini alması gerekmektedir.
- Risk Analizi: Oyuncu, oyunun Mekaniği

  Oyuncu, bir şirketin siber güvenlik uzmanı olarak göreve başlar ve şirketi hacker saldırılarına karşı korumak için farklı seviyelerde kararlar alır. Oyun, interaktif kararlar ve stratejik olarak şirketin mevcut güvenlik açıklarını değerlendirir ve en iyi savunma yöntemini seçer.

- Zaman Yönetimi: Oyuncular belirli bir süre içinde kararlarını vererek saldırıları önlemeye çalışır.
- Geri Bildirim Mekanizması: Oyuncu yanlış veya eksik bir seçim yaptığında sistem ona uyarı verir ve doğru güvenlik protokollerini öğretir.

Öğrenme Süreci

Oyun, adım adım siber güvenlik farkındalığını artıran bir öğrenme süreci sunar.

1. Seviye 1: Şifre Analizi

- Oyuncu verilen şifrelerin güvenli olup olmadığını analiz eder.
- Yanlış seçim yaparsa, hacker sızdırma girişimi canlandırılır.
- Doğru şifre kriterleri hakkında geri bildirim verilir.

2. Seviye 2: Şifre Oluşturma

- Oyuncu, sistem tarafından verilen bir hesap için güvenli bir şifre oluşturur.
- Sistem, girilen şifrenin güvenlik seviyesini analiz eder ve geri bildirim verir.
- Oyuncu şifre güvenliğini artırmak için farklı öğeleri (büyük/küçük harf, özel karakterler, uzunluk) kullanmalıdır.

3. Seviye 3: Kimlik Avı (Phishing) Tespiti

- Oyuncuya sahte ve gerçek e-postalar gösterilir.
- Oyuncu, sahte e-postaları tespit ederek hacker saldırılarını önler.
- Gerçek dünyada phishing saldırılarının nasıl tespit edileceği hakkında bilgi verilir.

4. Final Seviye: Siber Savunma Planı Oluşturma

- Oyuncu, şirketin güvenliğini artırmak için stratejik kararlar alır.
- Çalışanlara zorunlu güvenlik eğitimleri düzenler.
- Güvenlik duvarı (firewall) ayarlarını optimize ederek saldırıları önler.
- Otomatik sistem güncellemelerini etkinleştirerek açıkları kapatır.
- Oyuncunun seçimlerine göre şirketin güvenlik seviyesi yükselir veya hacker saldırıları başarılı olur.

Kazanım: Oyuncu, oyunun sonunda siber güvenlik farkındalığı kazanmış olur ve gerçek dünyada siber tehditleri daha iyi anlayarak nasıl korunacağını öğrenir

KULLANICI DENEYİMİ VE BEKLENEN ETKİLER:

- Kullanıcılar, oyun sürecinde aktif kararlar alarak problem çözme becerilerini geliştirecek.
- Siber güvenlik konusunda bilgi sahibi olmayan kişiler, eğlenceli bir oyun deneyimiyle tehditleri tanımayı ve önlemeyi öğrenecek.
- Farklı senaryolar ve zorluk seviyeleri sunularak kullanıcıların tekrar oynamasını teşvik edeceğim.

TEKNİK GEREKSİNİMLER:

Geliştirme Ortamı ve Araçlar

- Oyun Motoru: Unity 6
- Programlama Dili: C# (Visual Studio Code 2022)
- Grafikler: Unity Asset Store veya özel UI tasarımları
- Animasyonlar: Basit UI animasyonları (hacker uyarıları vb.)
- Ses Efektleri: Uyarı ve hacker tehlike sesleri

Kodlama Gereksinimleri

- Unity UI Sistemi: Kullanıcının kararlarını verebileceği butonlar ve bildirim ekranları.
- Veritabanı Kullanımı: Oyuncuların en iyi skorlarını tutmak için SQLite veya Firebase.
- Zamanlayıcı Sistem: Oyun içinde belirli süre içinde eylemleri tamamlamazsa hacker sızdırması başarılı olur.

GİZEM AYDEMİR / 132330052