ESCUELA POLITÉCNICA NACIONAL

ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

JUEGOS INTERACTIVOS

Documentos iPlus EXAMEN 02
“CYBERSECURE: PHISING”

Autor:

- Santiago León

PERIODO: 2024 A

Índice

A. Documento de Requisitos

1. Introducción

- **Propósito:** Este documento detalla los requisitos para el desarrollo del juego "CyberSecure: Defend the Network", un juego serio destinado a enseñar conceptos de ciberseguridad, específicamente la prevención del phishing.
- **Alcance:** El juego será una aplicación de estrategia en tiempo real para PC, dirigida a estudiantes y profesionales de TI.

2. Requisitos Funcionales

- **RF1:** El juego debe permitir a los jugadores construir y mejorar defensas como firewalls y sistemas antivirus.
- **RF2:** Los jugadores deben gestionar recursos como ancho de banda y potencia de procesamiento.
- **RF3:** El juego debe incluir escenarios que presenten amenazas de phishing y herramientas para analizarlas y responder a ellas.
- **RF4:** Los jugadores deben poder responder a incidentes de phishing y contener el daño.
- **RF5:** El juego debe proporcionar retroalimentación sobre la efectividad de las defensas y las respuestas a incidentes.

3. Requisitos No Funcionales

- **RNF1:** La interfaz del juego debe ser intuitiva y fácil de usar.
- **RNF2:** El juego debe ser compatible con PCs de gama media.
- **RNF3:** La experiencia de usuario debe ser fluida y sin retrasos significativos.
- **RNF4:** El juego debe ser accesible para personas con discapacidades, siguiendo las pautas de accesibilidad WCAG.

4. Requisitos Educativos

- **RE1:** El juego debe enseñar conceptos clave de phishing, incluyendo su identificación y prevención.
- **RE2:** Cada nivel debe incluir un resumen de los conceptos de ciberseguridad aprendidos.
- **RE3:** El juego debe incluir cuestionarios periódicos para evaluar la comprensión del jugador.

- **RE4:** El contenido educativo debe ser validado por expertos en ciberseguridad.

5. Usuarios Finales y sus Necesidades

- **Estudiantes de TI:** Necesitan aprender y practicar conceptos de ciberseguridad en un entorno interactivo.
- **Profesionales de TI:** Necesitan mejorar sus habilidades de respuesta a incidentes de phishing.
- **Educadores:** Necesitan una herramienta interactiva para enseñar ciberseguridad de manera efectiva.

6. Conclusión

- Este documento de requisitos servirá como guía para todas las fases del desarrollo del juego "CyberSecure: Defend the Network", asegurando que se cumplan los objetivos educativos y de jugabilidad.

B. Documento de Objetivos Educativos

1. Introducción

- **Propósito:** Definir los objetivos educativos y los resultados de aprendizaje específicos del juego, centrados en la prevención del phishing.

2. Objetivos Educativos

- **OE1:** Enseñar a los jugadores a identificar correos electrónicos y mensajes de phishing.
- **OE2:** Educar sobre las técnicas comunes utilizadas en los ataques de phishing.
- **OE3:** Proporcionar estrategias efectivas para prevenir y mitigar ataques de phishing.
- **OE4:** Fomentar la toma de decisiones rápidas y efectivas en respuesta a incidentes de phishing.

3. Resultados de Aprendizaje

- **RA1:** Los jugadores serán capaces de identificar al menos tres técnicas de phishing comunes.

- **RA2:** Los jugadores podrán implementar medidas de prevención de phishing en un entorno de red simulado.
- **RA3:** Los jugadores desarrollarán habilidades para responder a incidentes de phishing y minimizar el daño.
- **RA4:** Los jugadores demostrarán un conocimiento sólido de las mejores prácticas en ciberseguridad para la prevención del phishing.

4. Metodología de Evaluación

- **Cuestionarios:** Evaluaciones periódicas durante el juego para medir la comprensión de los conceptos de phishing.
- **Escenarios Prácticos:** Situaciones simuladas donde los jugadores aplican lo aprendido para resolver problemas de phishing.
- **Retroalimentación:** Análisis de desempeño con recomendaciones para mejorar las habilidades de ciberseguridad.

5. Conclusión

- Este documento de objetivos educativos guiará el diseño de los niveles y la jugabilidad del juego, asegurando que los jugadores adquieran los conocimientos necesarios para prevenir el phishing de manera efectiva.

C. Guion Lúdico

1. Introducción

- **Propósito:** Describir la narrativa, los personajes y los niveles del juego, integrando los conceptos educativos de ciberseguridad relacionados con el phishing.

2. Narrativa

- **Historia:** El jugador asume el rol de un gerente de seguridad de red en una gran organización. La empresa enfrenta una serie de ciberataques de phishing por parte de un misterioso grupo de hackers conocido como "Phantom Phishers". El jugador debe defender la red, identificar las amenazas y neutralizarlas.
- **Ambientación:** El juego se desarrolla en diversos entornos, incluyendo oficinas corporativas, centros de datos y configuraciones de trabajo remoto.

3. Personajes

- **Jugador (Gerente de Seguridad de Red):** Avatar del jugador, responsable de proteger la red.
- **Equipo de TI:** Miembros del equipo que brindan consejos y asistencia al jugador.
- **Phantom Phishers:** Grupo de hackers que lanza ataques de phishing contra la organización.

4. Niveles y Desafíos

- **Nivel 1: Introducción al Phishing**
  - **Objetivo:** Enseñar los conceptos básicos del phishing y cómo identificar correos sospechosos.
  - **Desafío:** Identificar y neutralizar un ataque de phishing básico.
- **Nivel 2: Técnicas Avanzadas de Phishing**
  - **Objetivo:** Educar sobre técnicas avanzadas de phishing como spear-phishing y phishing por voz.
  - **Desafío:** Defender la red contra ataques más sofisticados.
- **Nivel 3: Implementación de Medidas de Prevención**
  - **Objetivo:** Implementar firewalls y sistemas de detección de intrusos para prevenir ataques de phishing.
  - **Desafío:** Configurar y gestionar defensas en tiempo real.
- **Nivel 4: Respuesta a Incidentes**
  - **Objetivo:** Desarrollar habilidades para responder a incidentes de phishing y minimizar el daño.
  - **Desafío:** Responder a un gran ataque de phishing que compromete múltiples sistemas.

5. Conclusión

- Este guion lúdico proporciona una estructura clara para el desarrollo del juego, asegurando que la narrativa y los desafíos educativos estén bien integrados.

D. Mecánicas de Juego Refinadas

1. Introducción

- **Propósito:** Describir las mecánicas de juego refinadas y la interfaz de usuario optimizada para una experiencia educativa efectiva.

2. Mecánicas de Juego

- **Construcción y Mejora de Defensas:**
  - **Descripción:** Los jugadores construyen y mejoran firewalls, sistemas antivirus y otros mecanismos de defensa.
  - **Función:** Proteger la red contra amenazas de phishing.
- **Gestión de Recursos:**
  - **Descripción:** Los jugadores deben gestionar recursos como ancho de banda y potencia de procesamiento.
  - **Función:** Asegurar que las defensas sean sostenibles y efectivas.
- **Análisis de Amenazas:**
  - **Descripción:** Los jugadores analizan correos electrónicos y mensajes sospechosos para identificar phishing.
  - **Función:** Detectar y neutralizar ataques antes de que comprometan la red.
- **Respuesta a Incidentes:**
  - **Descripción:** Los jugadores deben responder a incidentes de phishing y contener el daño.
  - **Función:** Minimizar el impacto de los ataques y restaurar la seguridad de la red.

3. Interfaz de Usuario

- **Dashboard Central:**
  - **Descripción:** Panel de control donde los jugadores monitorean el estado de la red y gestionan sus defensas.
- **Menú de Mejoras:**
  - **Descripción:** Interfaz para mejorar defensas y comprar nuevas herramientas de seguridad.
- **Panel de Respuesta a Incidentes:**
  - **Descripción:** Vista detallada de los ataques en curso donde los jugadores pueden desplegar respuestas.

4. Prototipado y Pruebas Iterativas

- **Prototipos Funcionales:** Se desarrollaron prototipos jugables de las mecánicas clave y la interfaz de usuario.
- **Pruebas Iterativas:** Se realizaron pruebas con usuarios para obtener retroalimentación y mejorar las mecánicas y la interfaz.

5. Conclusión

- Las mecánicas de juego refinadas y la interfaz de usuario optimizada aseguran una experiencia educativa efectiva y atractiva para los jugadores.

E. Juego Pulido y Educativo

1. Introducción

- **Propósito:** Describir el juego final, destacando cómo enseña eficazmente la prevención del phishing.

2. Características del Juego Final

- **Narrativa Atractiva:**
  - Historia inmersiva sobre la lucha contra los ataques de phishing de los "Phantom Phishers".
- **Mecánicas Educativas:**
  - Mecánicas de juego que enseñan conceptos clave de phishing y ciberseguridad.
- **Interfaz Intuitiva:**
  - Interfaz de usuario optimizada para una navegación fácil y efectiva.
- **Escenarios Realistas:**
  - Niveles y desafíos basados en situaciones reales de ciberseguridad.
- **Evaluación Continua:**
  - Cuestionarios y análisis de desempeño para reforzar el aprendizaje.

3. Pruebas y Refinamiento

- **Pruebas Exhaustivas:**
  - Realización de pruebas de juego con usuarios finales y ajustes basados en la retroalimentación.
- **Evaluación Educativa:**
  - Análisis de la efectividad educativa y ajustes para maximizar el impacto del aprendizaje.

4. Lanzamiento y Soporte

- **Lanzamiento:**
  - Planificación de eventos de lanzamiento y distribución del juego.
- **Soporte Inicial:**
  - Soporte post-lanzamiento para solucionar problemas y realizar mejoras.

5. Conclusión

- "CyberSecure: Defend the Network" es un juego serio pulido y educativo, listo para enseñar eficazmente la prevención del phishing a estudiantes y profesionales de TI.