ESCUELA POLITÉCNICA NACIONAL

ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

JUEGOS INTERACTIVOS

GDD EXAMEN 02 “CYBERSECURE: PHISING”

Autor:

- Santiago León

PERIODO: 2024 A

Índice

1. Información del juego

Nombre del Juego: CyberSecure: Phising
Género: Juego Educativo
Jugadores: 1 jugador

1.1. Elementos del juego

1.1.1. Identificación de Phishing

- **Interfaz de Correo:** Los jugadores reciben correos electrónicos en una bandeja de entrada simulada y deben determinar si cada correo es phishing o legítimo.
- **Marcado de Correo:** El jugador puede marcar un correo como phishing o como real, lo que desencadena una respuesta educativa.

1.1.2. Feedback Educativo

- **Explicaciones Post-Decisión:** Después de cada decisión, el juego proporciona una explicación detallada, ayudando al jugador a entender las señales de phishing.

1.1.3. Tutorial Interactivo

- **Introducción al Phishing:** Un tutorial inicial que explica qué es phishing y cómo identificarlo, utilizando ejemplos interactivos.

---

2. Especificaciones técnicas

2.1. Forma técnica

- **Estilo de arte:** Pixel art 2D con una estética clara y minimalista.
- **Vista:** Introducción al Phishing: Un tutorial inicial que explica qué es phishing y cómo identificarlo, utilizando ejemplos interactivos.
- **Plataformas:** PC
- **Lenguaje:** C#
- **Dispositivos:** PC

---

3. Jugabilidad

3.1. Esquema de jugabilidad

- **Abrir la aplicación del juego:** El jugador inicia lanzando la aplicación "CyberSecure: Phising" en su PC.
- **Opciones del juego:** Menú principal con opciones para iniciar el juego y salir del juego.

3.1.1. Sinopsis de la historia

- **Premisa:** En un mundo digital donde los ataques cibernéticos son una amenaza constante, los jugadores deben proteger una red informática de ciberataques. El juego se centra en la identificación de correos electrónicos maliciosos, enseñando a los jugadores cómo reconocer y prevenir phishing a través de decisiones informadas.

3.1.2. Modos

- **Modo Tutorial:** Una breve introducción interactiva que enseña los fundamentos del phishing.
- **Modo Principal:** Los jugadores enfrentan una serie de correos electrónicos y deben decidir si son phishing o no.

3.2. Controles Básicos

- **Seleccionar Correo:** Clic izquierdo para seleccionar un correo electrónico.
- **Marcar como Phishing:** Botón con un visto para marcar un correo como phishing.
- **Marcar como Real:** Botón con una equis para marcar un correo como real.

3.3. Elementos del juego

- **Correos Electrónicos:** Los principales elementos interactivos, que el jugador debe analizar y clasificar.
- **Feedback Educativo:** Mensajes que explican si la selección del jugador fue correcta o incorrecta, y por qué.

3.4. Niveles del juego

El juego tiene un único nivel dividido en etapas, donde cada etapa presenta diferentes correos electrónicos para analizar.

3.5. Controles del jugador

- **Interacción:**
  - **Clasificación de Correos:** Decidir si un correo es phishing o real.
  - **Recepción de Feedback:** Entender el por qué detrás de cada decisión.

3.6. Ganar

- **Objetivos:**
  - Aprender a identificar correos electrónicos de phishing y tomar decisiones informadas.

3.7. Fin

- **Conclusión:**
  - El juego concluye después de que el jugador ha completado todas las etapas y ha recibido feedback educativo.

3.8. ¿Por qué es todo esto divertido?

- **Educativo:** El juego enseña habilidades valiosas para la vida real en cuanto a la identificación de amenazas cibernéticas.
- **Divertido:** La mecánica de toma de decisiones rápida y el feedback inmediato hacen que el proceso de aprendizaje sea dinámico e interesante.

---

4. Características claves

- **Tutorial Interactivo:** Introduce a los jugadores a los conceptos clave de phishing.
- **Mecánica de Decisiones:** Seleccionar correos electrónicos y clasificar si son phishing o no.
- **Feedback Educativo:** Explicaciones detalladas después de cada decisión.

---

5. Documento de diseño

5.1. Directrices de diseño

Restricciones creativas:

- **Estilo de arte:** Pixel art 2D, minimalista y claro.
- **Plataforma:** Exclusivo para PC.
- **Lenguaje de programación:** Desarrollado en C#.
- **Vista del juego:** Vista estática de la bandeja de entrada.
- **Combate y mecánicas de juego:** Decisiones estratégicas basadas en la clasificación de correos.

Objetivos generales del diseño:

- **Educación y Concienciación:** El principal objetivo es educar a los jugadores sobre las técnicas de phishing y cómo detectarlas, brindándoles las herramientas necesarias para protegerse en situaciones reales.
- **Accesibilidad:** El juego debe ser accesible para una amplia audiencia, incluyendo personas con discapacidades, asegurando que todos los usuarios puedan aprender y disfrutar del juego.
- **Interactividad y Feedback:** Ofrecer una experiencia interactiva donde las decisiones del jugador se reflejen inmediatamente con un feedback claro y educativo, reforzando el aprendizaje.
- **Engagement:** Mantener al jugador comprometido mediante una mecánica de juego simple pero desafiante, que motive la repetición para mejorar sus habilidades de identificación de phishing.
- **Narrativa Envolvente:** A través del tutorial y del feedback educativo, el juego debe contar una narrativa que no solo informe, sino que también entretenga al jugador, integrando educación y juego de manera fluida.
- **Simulación Realista:** Crear una simulación de bandeja de entrada que se asemeje a la realidad, proporcionando una experiencia educativa que los jugadores puedan aplicar en sus propias interacciones digitales.

5.2. Aplicación de la metodología iPlus

Teoría de iPlus:

La metodología iPlus es un enfoque centrado en el usuario para el diseño de juegos serios, desarrollada con el objetivo de crear juegos que no solo sean entretenidos, sino también efectivos en la enseñanza de conceptos específicos. Esta metodología se basa en un proceso colaborativo y multidisciplinario, involucrando a diseñadores de juegos, expertos en la

materia, educadores y usuarios finales. Aquí se presenta un resumen de las fases y componentes clave de la metodología iPlus:

Fase 1: Identificación

Objetivo: Definir el problema y los requisitos del usuario, identificando a los principales interesados en el desarrollo del juego.

Participantes:

- Diseñadores de juegos
- Expertos en ciberseguridad
- Educadores
- Usuarios finales (estudiantes y profesionales de TI)

Actividades:

1. **Reuniones iniciales:**
    - **Propósito:** Comprender los objetivos educativos y las expectativas de los usuarios.
    - **Resultado:** Identificación de los conceptos clave de ciberseguridad a enseñar, específicamente relacionados con el phishing.
2. **Lluvia de ideas:**
    - **Propósito:** Generar ideas sobre cómo integrar conceptos de phishing en la jugabilidad.
    - **Resultado:** Lista de posibles mecánicas de juego y escenarios educativos.
3. **Recolección de requisitos:**
    - **Propósito:** Detallar los requisitos funcionales y no funcionales del juego.
    - **Resultado:** Documento de requisitos que incluya las necesidades del usuario, objetivos educativos, y expectativas de jugabilidad.

Resultado Final: Un documento detallado de requisitos que sirva como guía para las siguientes fases del desarrollo.

Fase 2: Objetivos Pedagógicos

Objetivo: Definir los objetivos educativos y los resultados de aprendizaje específicos relacionados con la prevención del phishing.

Participantes:

- Educadores
- Expertos en ciberseguridad
- Diseñadores instruccionales

Actividades:

1. **Desarrollo de objetivos educativos:**
    - **Propósito:** Establecer qué conceptos de phishing se enseñarán y cómo se medirán los resultados de aprendizaje.
    - **Resultado:** Lista de objetivos educativos claros y medibles.
2. **Creación de resultados de aprendizaje:**
    - **Propósito:** Definir los conocimientos y habilidades que los jugadores deben adquirir al completar el juego.
    - **Resultado:** Resultados de aprendizaje detallados para cada nivel del juego.
3. **Alineación con estándares educativos:**
    - **Propósito:** Asegurar que los objetivos educativos estén alineados con los estándares educativos relevantes.
    - **Resultado:** Documentación que muestra la alineación de los objetivos del juego con los estándares educativos.

Resultado Final: Un documento de objetivos educativos que guíe el diseño de los niveles y la jugabilidad del juego.

Fase 3: Guion Lúdico

Objetivo: Desarrollar la narrativa del juego y las mecánicas de juego, integrando los conceptos educativos de manera efectiva.

Participantes:

- Guionistas de juegos
- Diseñadores de juegos
- Expertos en ciberseguridad

Actividades:

1. **Escritura de la historia:**
    - **Propósito:** Crear una narrativa atractiva que envuelva a los jugadores en la temática del phishing.
    - **Resultado:** Guion del juego con una historia que involucre ataques de phishing y la lucha del jugador para prevenirlos.
2. **Diseño de personajes:**

    - **Propósito:** Desarrollar personajes que representen tanto a los defensores de la red como a los atacantes de phishing.
    - **Resultado:** Descripciones y arte conceptual de los personajes principales.
3. **Creación de niveles y desafíos:**
    - **Propósito:** Diseñar niveles que enseñen y refuercen conceptos de phishing a través de la jugabilidad.
    - **Resultado:** Mapas de niveles y diseño de desafíos específicos para cada concepto de phishing.

Resultado Final: Un guion lúdico completo que describe la narrativa, personajes y niveles del juego.

Fase 4: Jugabilidad

Objetivo: Diseñar y desarrollar las mecánicas de juego principales que enseñen conceptos de phishing.

Participantes:

- Diseñadores de juegos
- Desarrolladores
- Diseñadores de UI/UX

Actividades:

1. **Prototipado de mecánicas de juego:**
    - **Propósito:** Crear prototipos funcionales de las mecánicas principales, como la detección y prevención de phishing.
    - **Resultado:** Prototipos jugables de las mecánicas clave.
2. **Pruebas iterativas:**
    - **Propósito:** Probar las mecánicas de juego con usuarios para obtener retroalimentación y hacer mejoras.
    - **Resultado:** Informe de pruebas con recomendaciones para refinamiento.
3. **Desarrollo de la interfaz de usuario:**
    - **Propósito:** Diseñar una interfaz intuitiva y accesible que permita a los jugadores interactuar eficazmente con el juego.
    - **Resultado:** Prototipos de UI y pruebas de usabilidad.

Resultado Final: Mecánicas de juego refinadas y una interfaz de usuario optimizada para una experiencia educativa efectiva.

Fase 5: Refinamiento

Objetivo: Refinar el juego basado en la retroalimentación de las pruebas y asegurar la efectividad educativa.

Participantes:

- Testers
- Educadores
- Desarrolladores
- Diseñadores

Actividades:

1. **Pruebas de juego:**
    - **Propósito:** Realizar pruebas exhaustivas con el público objetivo para recopilar retroalimentación detallada.
    - **Resultado:** Informe de pruebas con sugerencias de mejora.
2. **Análisis de efectividad educativa:**
    - **Propósito:** Evaluar si el juego cumple con sus objetivos educativos y ajustar el contenido según sea necesario.
    - **Resultado:** Informe de evaluación con recomendaciones para mejoras.
3. **Refinamiento de contenido:**
    - **Propósito:** Ajustar las mecánicas de juego, la interfaz de usuario y el contenido educativo basado en la retroalimentación.
    - **Resultado:** Versión final del juego lista para lanzamiento.

Resultado Final: Un juego pulido y educativo que enseña eficazmente la prevención del phishing, listo para su lanzamiento y uso educativo.

Aplicación en este GDD:

- **Fase 1: Análisis de Necesidades**
  Se determinó la necesidad de un juego educativo que enseñe a los usuarios a identificar correos electrónicos de phishing.
- **Fase 2: Definición de Objetivos Educativos**
  Se establecieron los objetivos de que el jugador aprenda a reconocer técnicas comunes de phishing y cómo prevenir estos ataques.
- **Fase 3: Diseño Lúdico**
  Se diseñaron las mecánicas de selección de correos y se estableció un feedback inmediato para educar al jugador.

- **Fase 4: Prototipado y Refinamiento**
  Se creó un prototipo jugable, se realizaron pruebas de usuario, y se refinó la interfaz para asegurar la claridad y efectividad educativa.
- **Fase 5: Implementación y Validación**
  El juego fue implementado y validado mediante pruebas con usuarios y expertos en ciberseguridad.

---

6. Propiedades del jugador

Descripción rápida del jugador:

- **Rol del jugador:** Analista de ciberseguridad.
- **Objetivo principal:** Identificar y prevenir correos de phishing.

Propiedades del jugador:

- **Experiencia educativa:** Conocimiento sobre phishing.
- **Progreso:** Mejora en la identificación de correos de phishing.

---

7. Interfaz de usuario

Interfaz de usuario:

- **Menús:** Menú principal con opciones para jugar y salir.
- **Juego:** Interfaz de la bandeja de entrada, con botones de decisión.
- **Feedback:** Mensajes de texto que explican las decisiones del jugador.