



1. Título: Detrás de la pantalla: ¿Jugamos realmente seguros?

2. Datos Personales:

Nombre: Martina Collazo Sánchez

Centro: Colegio Apóstol Santiago de Vigo.

3. Resumen

Mi trabajo trata sobre la ciberseguridad, concretamente sobre el phishing en los videojuegos. El objetivo es investigar la vulnerabilidad de los menores cuando reciben estos mensajes en los chats, ya que pueden ser más susceptibles a caer en el engaño que los adultos.

Para realizar la investigación he hecho una encuesta online a niños de entre 10 y 11 años para comprobar si son capaces de detectar estos mensajes y ver si es necesario tomar medidas de prevención.

Los resultados de la encuesta muestran que muchos podrían caer en este tipo de fraude, por lo que sería importante aplicar algunas medidas para que los niños puedan jugar y navegar por internet de forma más segura.

4. Introducción

La ciberseguridad es la práctica de proteger a las personas, los sistemas y los datos de los ciberataques. Se utiliza para evitar amenazas a través de internet, como el phishing. Este tipo de ataque busca suplantar la identidad de una marca, web o persona con el objetivo de obtener datos personales con fines lucrativos. Esta temática ocupa un lugar importante en nuestra sociedad, ya que, según la Asociación Española de Videojuegos (AEVI), 8 de cada 10 menores usan videojuegos. Esto les expone y les hace más vulnerables, pues los juegos online son espacios atractivos para los ciberdelincuentes. El objetivo del estudio es dar visibilidad a esta situación y fomentar la mejora de herramientas de detección de estos ataques.

5. Propósito del trabajo

El objetivo de este trabajo es detectar el nivel de vulnerabilidad que pueden sufrir los menores de 12 años al estar expuestos en la red mientras juegan online. Como ya mencioné anteriormente, el phishing es un intento de robo mediante engaño digital y los niños, al no tener la información suficiente para manejarse con seguridad en internet, pueden caer fácilmente en este tipo de fraude. Para comprender la magnitud de esta situación, se realizará una encuesta a niños de 5º de primaria y con los datos extraídos, comprender la magnitud del riesgo.

6. Estado del arte

Según Bit Life Media, en el phishing, los atacantes utilizan dos métodos principales. El primero, ofrecen versiones anticipadas o gratuitas de los juegos más demandados creando páginas falsas que simulan ser oficiales. El segundo, lanzan ofertas muy atractivas de venta de skins y monedas virtuales a precios excesivamente bajos. Empresas como Kaspersky y Google han desarrollado herramientas para prevenir estos ataques, como filtros antiphishing y sistemas de navegación segura. Además, organismos como INCIBE también ofrecen información y recomendaciones para reducir estos riesgos en adultos y niños.

7. Hipótesis

Los menores de 12 años tienen dificultad para identificar intentos de phishing en chats de videojuegos, ya que cuando el mensaje incluye algún tipo de recompensa no suelen pensar en las posibles consecuencias. Aunque pueden reconocer un mensaje dudoso, cuando el tono es amistoso resulta más fácil que confíen y caigan. Por esta razón, se prevé que una gran parte de los alumnos encuestados no detecte tan fácilmente estas situaciones.

8. Material y métodos

Mi tipo de estudio consiste en una encuesta realizada mediante Google Forms. Los participantes son 16 alumnos de 5º de primaria del colegio Apóstol Santiago de Vigo (10 y 11 años). La encuesta tiene dos objetivos: comprobar si los niños son capaces de detectar el phishing y analizar si han sido víctimas de fraude en internet.

Las preguntas incluyen ejemplos de mensajes de phishing que podrían recibir en chats de videojuegos para ver cómo reaccionarían ante estas situaciones. También contiene algunas preguntas básicas sobre seguridad digital.

Las respuestas se recopilaron automáticamente y después se analizaron en Google Sheets para contar las respuestas y calcular porcentajes que permitieran hacer los gráficos.

9. Resultados

Una vez realizada la encuesta y analizados los datos, se creó un Índice de Riesgo de Ciberseguridad para entender mejor los resultados. Este índice sirve para saber si un jugador podría caer o no en una estafa según sus respuestas.

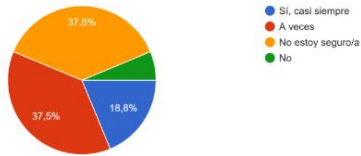
En riesgo bajo está el 19% de los alumnos. Esto significa que saben reconocer un mensaje de phishing y es poco probable que caigan en este tipo de fraude.

En riesgo medio está el 44%. Estos alumnos podrían detectar mensajes sospechosos, aunque también podrían caer si el mensaje parece real.

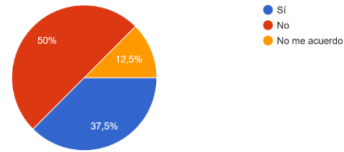
En riesgo alto está el 37%. Esto indica que les resulta más difícil identificar un mensaje de phishing y podrían caer con más facilidad.

En general, los resultados muestran que muchos alumnos todavía tienen dificultades para reconocer este tipo de estafas.

¿Crees que sabes reconocer cuándo un mensaje es falso?
16 respuestas



¿Has recibido alguna vez un mensaje prometiendo monedas, Robux o mods gratis?
16 respuestas



10. Conclusiones

Los resultados muestran que, aunque algunos niños detectan el fraude, muchos tienen dificultades para reconocer mensajes de phishing en los videojuegos.

La hipótesis se ha cumplido en parte, ya que bastantes alumnos no consiguen detectar estas estafas. Uno de los problemas que hemos visto es que solo el 50% asegura no haber recibido nunca un mensaje de un desconocido prometiendo monedas. Esto significa que muchos niños están expuestos y nos hace preguntarnos: ¿los videojuegos son realmente seguros? Para que los niños puedan jugar sin preocuparse por estas estafas, sería importante hablar más sobre este problema en los colegios. Este estudio muestra que es importante aprender más sobre ciberseguridad para jugar online de forma más segura.

11. Bibliografía

<https://www.kaspersky.es/about/press-releases/crecen-un-57-los-ciberataques-a-ninos-a-traves-de-videojuegos> // <https://bitlifemedia.com/2025/09/videojuegos-hijos-ciberataques/> // <https://www.ciberseguridadpyme.es/actualidad/estafas-de-phishing-en-la-comunidad-de-jugadores/> // <https://www.redeszone.net/noticias/seguridad/ataques-phishing-jugar-online/> // <https://www.incibe.es/menores/blog/deberian-preocuparles-las-familias-los-videojuegos-online> // <https://www.incibe.es/ciudadania/tematicas/ingenieria-social-fraudes-online/phishing> // <https://aevi.org.es/resultados-anuales-2/> // <https://www.revistaciberseguridad.com/2025/09/cuando-lo-ludico-se-vuelve-peligroso-espacios-digitales-donde-acechan-los-depredadores-de-menores/>