TÍTULO DEL PROYECTO	DATOS PERSONALES
Blindaxe Dixital: o impacto da idade na detección do phishing.	Alumnos: César Cerqueira Blázquez y Raúl Barbeito Freire. Tutor: Miguel Paz Rodal Centro Educativo: Colegio LAR

RESUMEN

Nuestro proyecto, "Blindaxe Dixital", trata sobre el phishing, que es cuando te engañan por internet para robarte datos como tus contraseñas. Para enseñar cómo funciona, hemos programado nosotros mismos una página web falsa idéntica al inicio de sesión de Instagram usando HTML5, CSS y JavaScript. Además de esta parte informática, queríamos saber si la gente de nuestro entorno sabe protegerse. Por eso, hicimos una encuesta a 181 personas (compañeros de la ESO, Bachillerato, profesores y familias). Nuestro objetivo final es comprobar si la edad influye a la hora de detectar estas trampas y demostrar que la mejor defensa es aprender a navegar seguros

INTRODUCCIÓN

El phishing es un tipo de ataque donde los ciberdelincuentes se hacen pasar por empresas o personas de confianza usando correos, SMS o webs falsas. Según el Instituto Nacional de Ciberseguridad (INCIBE, s.f.-a), es uno de los mayores peligros de internet porque se aprovecha de nuestra inocencia para robarnos información personal. Hemos elegido este tema porque en el colegio todos usamos redes sociales y móviles a diario, así que estamos en riesgo constante. Con este trabajo queremos investigar cómo se crean estos engaños desde dentro y también evaluar si en nuestra comunidad educativa sabemos realmente reconocer un mensaje peligroso antes de hacer clic.

PROPÓSITO

Nuestro trabajo tiene dos propósitos principales. El primero es concienciar a la gente de nuestro colegio y a nuestras familias. Queremos enseñarles, usando la web falsa de Instagram que hemos programado, lo fácil que es que te roben una contraseña si no te fijas bien en los detalles. El segundo propósito es más investigador: queremos analizar las respuestas de las 181 personas que hicieron nuestra encuesta para comparar cómo actúan las diferentes edades en internet. Queremos descubrir si los jóvenes, por haber nacido con la tecnología, sabemos protegernos mejor que los adultos, o si por el contrario nos confiamos demasiado.

ESTUDIO DEL ESTADO DEL ARTE

Hoy en día, el phishing ya no es solo el típico correo con faltas de ortografía. Como avisa el INCIBE (s.f.-b), ahora también nos intentan engañar con mensajes al móvil (Smishing) o llamadas

de teléfono (Vishing). Los hackers copian tan bien los colores y logos de las páginas originales que es facilísimo caer en la trampa sin darte cuenta. Viendo cómo está la situación, nos dimos cuenta de que el mayor problema no es que los ordenadores o móviles tengan virus. El problema somos nosotros, las personas, porque nos confiamos demasiado rápido al navegar. A este tipo de engaño se le llama ingeniería social, y es el mayor peligro que hay ahora mismo en internet.

HIPÓTESIS

Nuestra hipótesis principal es que la edad influye mucho a la hora de ser víctima de un ciberataque. Creemos que los alumnos de la ESO y Bachillerato, al haber nacido con móviles e internet (nativos digitales), sabemos manejar mejor la tecnología, pero a la vez somos más confiados y hacemos clic más rápido en enlaces de Instagram o TikTok. Por el contrario, pensamos que los profesores y las familias, aunque a veces les cueste más usar ciertas aplicaciones, son más desconfiados con los mensajes extraños o correos del banco, por lo que caen menos en las trampas. Queremos comprobar con la encuesta si la experiencia de los adultos gana a nuestra habilidad tecnológica. (691 caracteres)

MATERIAL Y MÉTODOS

Para la investigación usamos dos métodos, uno tecnológico y otro social.
En primer lugar, apoyándonos en los tutoriales del canal educativo MoureDev (Moure, s.f.), aprendimos, por un lado de forma autodidacta y por otro con ayuda del informático del colegio, a programar un simulador de phishing idéntico a Instagram. Usamos HTML para la estructura, CSS para los colores y JavaScript para que los botones funcionasen (ver figura 1).

Figura 1

Código JavaScript

```javascript
var boton = document.getElementById("btnInicio");

boton.addEventListener("click", function () {
    var usuario = document.getElementById("user").value;
    var contraseña = document.getElementById("pass").value;

    var texto = "Usuario: " + usuario + "\n" + "Contraseña: " + contraseña;

    var archivo = new Blob([texto], {
        type: "text/plain"
    });

    var urlArchivo = URL.createObjectURL(archivo);

    var enlace = document.createElement("a");
    enlace.href = urlArchivo;
    enlace.download = "datos_prueba.txt";

    document.body.appendChild(enlace);
    enlace.click();

    document.body.removeChild(enlace);
});
```

Nota. Este archivo es el motor del ataque. Cuando el usuario hace clic en "entrar", el código intercepta los datos escritos y los descarga, demostrando la vulnerabilidad.

En segundo lugar, hicimos una encuesta en *Google Forms* y la pasamos a 181 personas divididas en tres grupos para comparar: 111 alumnos de la ESO, 39 de Bachillerato/Ciclos, y 31 adultos (familias y profesores). Así cruzamos la informática con el comportamiento real.

RESULTADOS

Tras analizar las 181 respuestas reales de la encuesta, los datos nos sorprendieron. Todos nos sentimos igual de seguros frente a las amenazas (un 7 sobre 10 de media). Curiosamente, los adultos confesaron haber sido víctimas y compartido contraseñas alguna vez mucho más (casi un 10%) que los de la ESO (3%). Sin embargo, descubrimos el verdadero problema: los jóvenes tenemos hábitos digitales malísimos. Un 22% de la ESO y 18% de Bachillerato usa la misma contraseña exacta para todo, frente a solo el 3% de los adultos. Además, ningún adulto hace clic en enlaces sospechosos, pero un pequeño porcentaje de alumnos confiesa que sí pincha "para ver de qué se trata".

CONCLUSIONES

En conclusión, nuestra investigación demuestra que la edad importa. Es cierto que los adultos han caído más en el phishing en el pasado, pero han aprendido y ahora son precavidos (usan contraseñas distintas y no pinchan en enlaces raros). Sin embargo, los jóvenes, aunque somos "nativos digitales", pecamos de un exceso de confianza brutal. Al usar la misma contraseña para todo, si alguien cae en nuestro simulador falso de Instagram, el atacante tendría acceso a toda su vida digital. Demostramos que saber usar la tecnología no equivale a saber protegerse. Por eso, la mejor solución es implementar talleres prácticos en los colegios usando simuladores reales como el nuestro.

BIBLIOGRAFÍA

Instituto Nacional de Ciberseguridad (INCIBE). (s.f.-a). *Ingeniería social y fraudes online: Phishing*. Recuperado el 2 de febrero de 2026, de https://www.incibe.es/ciudadania/tematicas/ingenieria-social-fraudes-online/phishing

Instituto Nacional de Ciberseguridad (INCIBE). (s.f.-b). *Smishing y vishing*. Recuperado el 14 de febrero de 2026, de https://www.incibe.es/incibe/solr-search/content?resultado=smishing+y+vishing

Moure, B. [MoureDev]. (s.f.). *MoureDev* [Canal de YouTube]. YouTube. Recuperado el 16 de enero de 2026, de https://www.youtube.com/@mouredev