https://repository.uaeh.edu.mx/revistas/index.php/tepexi/issue/archive

TEPEXI Boletín Científico de la Escuela Superior Tepeji del Río

Publicación semestral, Vol. 12, No. 23 (2025) 46-50

Tepexi

ISSN: 2007-7629

Dos pasos adelante: la importancia de la autenticación en dos factores dentro de aplicaciones de uso común

Two steps forward: the importance of two-factor authentication within commonly used applications

Edwin Y. Sandoval-Muciño [a], Nubia B. Pérez-Olguin [b]

Abstract:

This article presents several topics around two-step authentication (2FA), which is an important security technique today to protect our personal accounts. It explains how it works as well as the importance of using it to prevent unauthorized access, presents the ideal way to use two-step authentication, the challenges that certain age groups present in adopting it in their daily lives (adults and young people), and the various alternatives that exist to this, knowing their strengths and most common failures, we also review certain success cases in which the implementation of this method guaranteed an improvement with the users of said platforms, the state in which this type of authentication is found. , the trends that it has been adopting for its correct functioning.

Keywords:

Authentication, 2FA, access, accounts, platforms.

Resumen:

El presente artículo presenta varios temas en torno a la autenticación en dos pasos (2FA), la cual es una técnica de seguridad importante hoy en día para proteger nuestras cuentas personales. Explica su funcionamiento así como su importancia de su uso para evitar accesos no autorizados, presenta la manera ideal de usar la autenticación en dos pasos, los desafíos que presentan ciertos grupos de edades para adoptarlo en su vida diaria (adultos y jóvenes), y las diversas alternativas que existen a esta, conociendo sus fortalezas y fallas más comunes, también repasamos ciertos casos de éxito en los que la implementación de este método garantizo una mejora con los usuarios de dichas plataformas, el estado en el que este tipo de autenticación se encuentra, las tendencias que ha ido adoptando para su correcto funcionamiento.

Palabras Clave:

Autenticación, 2FA, accesos, cuentas, plataformas.

Introducción

Las redes sociales juegan un papel importante en el día a día de nuestra sociedad, según datos obtenidos: El 59,4% de la población mundial usa redes sociales. Hay 4.760 millones de usuarios de redes sociales (el 94,9% de la población internauta) (Giménez, 2023) , de las cuales al menos se tiene acceso a 71 millones de correos electrónicos y 100 millones de contraseñas, siendo que el 65,03% de las direcciones publicadas ya se encontraban almacenadas en la base de datos de su plataforma Have I Been Pwned, lo que sugiere que son datos de filtraciones más antiguas que ya han sido alertadas. Mientras tanto, casi 25 millones de los 71 millones de direcciones de correo electrónico incluidas en la lista han sido expuestas por primera vez a través de la base de datos Naz.AP (Higuera, 2024). Es en base a ello que la autenticación en dos factores viene a ser una solución sencilla pero eficaz, en la que no basta con colocar un nombre de usuario y una contraseña para dar acceso, si no que exige de otro paso extra para la confirmación de que realmente es el usuario quien lo desea.

Según cifras proporcionadas por Google, menos del 10% de los usuarios de Gmail utilizan verificación en dos pasos (Pérez, 2018) resultando importante tener activada la misma para evitar estos ciberataques. Pero ¿en que consta una autenticación en dos pasos? Surge como una

[a] Autor de Correspondencia, Universidad Autónoma del Estado de Hidalgo | Escuela Superior de Tlahuelilpan | Tlahuelilpan-Hidalgo | México, https://orcid.org/0009-0009-3169-4811, Email: sa376136@uaeh.edu.mx

[b] Universidad Autónoma del Estado de Hidalgo | Escuela Superior de Tlahuelilpan | Tlahuelilpan-Hidalgo | México, https://orcid.org/0000-0002-1303-861X, Email: nubiab@uaeh.edu.mx

Fecha de recepción: 13/05/2024, Fecha de aceptación: 14/08/2024, Fecha de publicación: 05/01/2025

DOI: https://doi.org/10.29057/estr.v12i23.13020

mejora a sistemas más ambiguos que se usaban al momento, uno de ellos es el conocido Transaction Authentication Number (TAN), el cual era usado en bancos, en este se enviaba una lista de TAN's (códigos) y al querer realizar una transacción teníamos que ingresar uno de esos códigos otorgados. [4] En la actualidad, la autenticación en dos pasos ha evolucionado de manera positiva y que comparándolo a métodos tradicionales como el uso de cuentas y contraseñas (sin ningún paso extra), resultan menos propensos a ataques de phishing (técnicas de suplantación de identidad), el cual recurre a la ingeniería social para que los usuarios otorguen sus datos sensibles. [5] La autenticación en dos pasos nos permite agregar una barrera extra de seguridad a nuestras cuentas en línea que va desde nuestras redes sociales que solemos usar diariamente hasta cuentas corporativas, educativas o bancarias, aunque logra ir más allá de ello, tal es el caso de apps de mensajerías que usan la autenticación en dos pasos para realizar un cifrado y que gente externa al chat no pueda ver la conversación o en el caso de redes como Instagram/Facebook y X lo ocupan para negar o permitir el acceso a nuestro perfil. Resaltando entonces que esta autenticación no simplemente busca mejorar la seguridad de nuestras cuentas, sino que también busca mejorar la privacidad para que no exista una brecha. La finalidad de este artículo es que las personas consideren importante aplicar este método en todas sus cuentas de uso diario, así como conocer su funcionamiento a un nivel teórico y sobre todo fomentar un concepto como lo es la ciberseguridad.

Metodología

La metodología usada para este artículo se basó en cinco fases, cada una de ellas teniendo diferentes propósitos que fortalecieran a la entrega de un trabajo de investigación completa.

1. **Revisión de trabajos previos:** Se llevo a cabo una revisión de artículos y documentos que tengan relación con la autenticación en dos factores. Esto incluirá definiciones, tipos de autenticación en dos factores y su aplicación en diferentes contextos, así como de otros métodos de verificación.
2. **Selección de recursos:** Entre todos los documentos revisados se seleccionaron a aquellos que hicieran uso de fuentes confiables y actualizada sobre el tema que planteaban.
3. **Organización de la información:** Se recopilo la información más relevante de cada documento y se ordenó de manera comprensible para facilitar la realización del documento.
4. **Redacción del contenido:** Se redacto el contenido de la manera más clara y comprensible posible para que sea accesible a cualquier tipo de público evitando caer en aspectos muy técnicos que no se comprenderían del todo.

¿Cómo funciona la autenticación en dos pasos?

Al intentar acceder a cualquiera de nuestras cuentas de uso diario, nos encontramos con que se nos solicita un usuario o correo junto a una contraseña (datos que se supone solo nosotros conocemos), el problema radica cuando alguien más posee esos datos sin nosotros estar enterados, es ahí donde la autenticación en dos pasos entra ya que solicitara algo a lo que nosotros tengamos acceso.

Hay distintas maneras de implementar este tipo de autenticación, pero las dos más usadas son:

- **Estándar:** Consiste en solicitar un número de teléfono o un correo electrónico al cual se vinculará la cuenta para posteriormente al iniciar sesión, mandar un código de seis dígitos e ingresarlo. Esto para las empresas resulta un tanto problemático porque el servicio de telefonía no depende de ellos entonces puede existir cierta taza de errores además de que pagar un servicio de este tipo a largo plazo resulta en un gasto considerable.
- **TOTP:** Time-based One Time Password o por su traducción: Contraseña de un único uso basada en el tiempo, consta en un código que solo es posible usarlo una vez. Primeramente, el servicio que usemos nos proporcionara una clave que funcionara como una contraseña principal que dará acceso a que las contraseñas aleatorias se generen, para ello es necesario que usemos una aplicación de autenticador, dentro de la app se nos solicitara un código QR, el cual será complementado con un código de autenticación para evitar errores a la hora de vincular ambos. Una vez configurado esto. A ingresar a nuestra cuenta se solicitará un código para acceder, este mismo código se calcula mediante algoritmos que toman nuestra fecha y hora al momento de realizar la acción junto a nuestra clave principal.

Ahora, si aplicamos esto a un caso práctico, podemos imaginar que queremos iniciar sesión en nuestra cuenta de correo electrónico.

Primeramente, se nos solicitara nuestro correo electrónico y nuestra contraseña (algo que ya sabemos) y es muy común en todos los servicios hoy en día.

Figura 1. Inicio de sesión (Gmail).

Después viene un paso importante el cual es solicitar el código (ya sea de la manera estándar o TOTP). Si el código ingresado coincide con el que se generó y envió desde un principio se concederá el acceso.

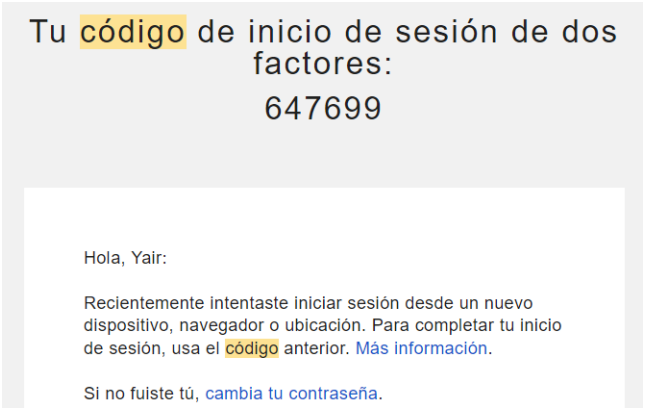

Figura 2. Código de inicio de sesión.

Pero si el mismo caduco o hubo un error al escribirlo este acceso se detecta como uno no autorizado y niega el acceso (en algunos casos como es el de Facebook, instantáneamente notifica mediante correo al usuario que hubo un intento fallo de inicio de sesión).

Figura 3. Inicio de sesión fallido.

Algunas recomendaciones que se dan a la hora de realizar la implementación de este tipo de autenticación es que primeramente se guarden de manera segura los códigos que el propio servicio que desees configurar te otorga debido a que si en algún momento presentas alguna problemática, se te van a solicitar alguno de los códigos para tener acceso y a esto se le añade el uso de aplicaciones recomendados por grandes empresas para almacenar contraseñas y que nos generen códigos, ejemplos de ellas son:

- Google Authenticator.
- Authy.
- KeePass.
- Microsoft Authenticator.

Problemática y estado actual

Si la autenticación en dos pasos busca ofrecer una capa de seguridad extra, ¿Por qué los usuarios no la agregan a sus cuentas personales?

Esto se debe a varios factores que se han adoptado desde años anteriores en los que los hackeos a cuentas si bien eran existentes, no eran tan comunes a un nivel individual (usuario) si no de una manera masiva a grandes empresas, tal tenemos el caso ocurrido en 2021 en el que de manera inesperada se expusieron un total de 533 millones de datos personales que usaban la red social Facebook en un total de 106 países [6].

Aunque muchas veces también hemos escuchado a algún conocido decir; ¡Me han hackeado mi cuenta!, esto resulta potencialmente peligroso debido a que cualquier persona que tenga malas intenciones y con las credenciales deseadas puede suplantar la identidad de algún usuario y causarle conflictos graves, uno de los mayores públicos al que afecta esta problemática es a los adultos mayores debido a que son uno de los sectores que menos conocimientos de “tecnologías nuevas” tienen lo cual recae en fraudes elaborados a base de ingeniería social siendo el 93% de las brechas de seguridad en condiciones normales e incrementando el número de incidentes de ‘phishing’ en organismos públicos a un 70 % (Blanco, 2020).

Muchas de las formas de fraude que se han elaborado para que este grupo selecto de persona otorgue sus datos personales es haciendo se pasar por algún representante de la empresa o servicio que desean utilizar, solicitando correo y contraseña prometiendo algún premio o beneficio inventado o el fraude surgido en 2019, que constaba en un fraude del soporte técnico, en el que se ofrece un grupo de personas a solucionar un caso hipotético del computador de la víctima y estos cayendo. El Informe sobre Delitos en Internet de 2019 del FBI recoge que las personas mayores de 60 años representan la mayoría de las víctimas reportadas de este tipo de fraude [7].

Por otro lado, tenemos el caso de un grupo comprendido de jóvenes que deciden de manera errónea evitar el uso de una autenticación extra, esto principalmente por la falta de conocimiento de estas tecnologías o simplemente por tener el pensamiento de que los hackeos individuales no son tan comunes, a esto se le añade el uso de contraseñas débiles que no siguen la recomendación de creación de estas**.** A la par de ello se desarrollan dentro del ámbito informático los famosos “script kiddies” los cuales son jóvenes que quieren llevar a cabo alguna actividad maliciosa -entrar a un sistema o robar credenciales, sin tener necesariamente conocimiento informático o habilidades para la programación

(Euronews, 2023), estos al tener la curiosidad por el conocer los datos de personas cercanas buscan herramientas elaboradas por otros usuarios del mismo entorno y realizan el hackeo, lo cual es un riesgo potencial para ambos de los grupos de personas previamente mencionados.

Aunque las empresas han hecho su máximo esfuerzo porque absolutamente todos sus usuarios adopten esta autenticación en su día a día, resulta difícil por el desfase tecnológico que existe en los mismos, al no tener los mismos conocimientos, aunque estas mismas empresas han hecho mucho énfasis en su importancia.

Alternativas a la autenticación en dos pasos

La autenticación en dos pasos a pesar de ser una gran opción con una fácil configuración no es la única que se conoce y es usada en el mercado, hoy en día se conocen dos tipos de autenticación, primero tenemos a Universal Authentication Factors o factores universales de autenticación (UAF)y después tenemos a la ya conocida Universal Second Factor Authentication o autenticación en dos pasos (U2F).

La elección de una u otra autenticación dependerá del nivel de seguridad que se busque y sobre todo de la facilidad que esta tecnología tenga para adaptarse a los requerimientos de la plataforma o aplicación en la que se quiere implementar, recordando que como toda tecnología esta puede presentar desventajas. A continuación, se menciona sus datos importantes:

- **Factores Universales de Autenticación (UAF):** Este consta en que el usuario que desea acceder lo logre mediante un servicio que usara uno o más factores de seguridad dentro de su celular, lográndolo mediante la tecnología **FIDO UAF.** El mismo mecanismo lo logra con ayuda de un sensor biométrico (huella dactilar, escaneo fácil o de iris), un conocimiento en base a alguna pregunta o en base a algo que el usuario posea, la principal diferencia a la ya conocida U2F, es que esta evita solicitar la contraseña al usuario, aunque su principal desventaja es que este solo se limita a su uso en dispositivos móviles.

A pesar de ser mecanismos que tienen estructuras completamente diferentes, la UAF y la U2F, logran compartir varias características técnicas que son fundamentales para su funcionamiento. Tenemos el ejemplo de generar una única clave aleatoria que es generada al momento, ambas usan un dispositivo físico (celular) para generar la clave, así como la presencia del usuario o algún ser humando para confirmar los cambios. Mientras que por otro lado las principales diferencias que encontramos es la cantidad de autenticaciones para el inicio de sesión, mientras que en UAF solo basta con confirmar una vez, en U2F es necesario colocar nuestra contraseña y después nuestra clave, mientras que el U2F es capaz de trabajar en diversos entornos, el UAF no lo logra, pero esto le da posibilidades de trabajar con tecnologías como la conexión Bluetooth Low Energy, NFC, HID e inclusive el GPS. [11]

Tendencias en la actualidad

Al tener una base de datos de usuarios más grande, año con año en las diversas redes sociales, es común que los hackers busquen maneras de vulnerar la autenticación en dos pasos, esto resulta preocupante por diversos motivos, por lo que alrededor del mundo se han desarrollado nuevas soluciones que aumenten la seguridad del usuario. Claro ejemplo de ello es el proyecto conocido como AudioMark desarrollado por Andrea Fariña en el año 2020 en el cual se encripta el código que usualmente se recibe por un SMS o un correo electrónico a un audio comprensible para el verificador, esto le ahorra al usuario la tarea de memorizar dicho código y escribirlo en el verificador, eliminando de cierta forma una pequeña taza de error común. [12]

Por otro lado, también tenemos la opción para entornos laborales planteada por Carpio A., Jazmín R., Orrala P. y Yanina M. En la que al tener un entorno con dos alternativas en cuanto a sistemas operativos (Linux y Windows) se encontraban dificultades en cuando a la autenticación del controlador de dominio de Windows, para ello recurrieron a métodos de integración como System Security Services Daemon (SSSD) y Winbind, los que a su vez hacían uso de dos protocolos importantes para llevar a cabo dicha tarea: Lightweight Directory Access Protocol (LDAP) y Kerberos. Lo cual les permitió obtener la administración centralizada de los usuarios que usaban Windows 8 y Windows Server 2012 R2 con los usuarios que hacían uso de Ubuntu 14.04 y CentOS 7.0. [13]

Y finalmente tenemos su implementación dentro de la plataforma HomeOfi la cual no solo funciono como un método de seguridad extra si no que con la misma lograron realizar la validación y detección de aquellos usuarios reales y usuarios falsos que buscaban realizar un arque informático mediante el método Delphi. [14]

Es en base a estos ejemplos que podemos corroborar que el uso de esta autenticación no está desfasado tecnológicamente y año con año se realiza una ardua labor por mejorarlo.

Conclusiones

Repasando la evolución que esta tecnología ha tenido, así como sus casos de éxito, podemos decir que la autenticación en dos pasos es una herramienta confiable

y esencial para muchas empresas y sobre todo para los usuarios de estas, su funcionamiento e implementación es sencillo ya que basta con introducir la contraseña de nuestra cuenta y posteriormente introducir un código de seis dígitos que llega a nuestro teléfono, esto dificulta en gran medida los posibles ciberataques de personas externas a nosotros. Sin embargo y a pesar de sus múltiples beneficios su adopción no ha sido bienvenida por todos los sectores poblacionales debido a la falta de conocimiento de esta o simplemente por la falta de conciencia, generando así una brecha importante para los hackers. Para dar solución a esta problemática es fundamental educar a los usuarios sobre estos procesos y si es necesario explorar más alternativas que nos brinden una mayor seguridad, tal es el caso de los factores universales de autenticación (UAF), lo cuales, mediante métodos biométricos, conocimientos del usuario y sobre todo posesiones del usuario logra conceder acceso con un solo toque. Sin olvidar que esta tecnología cada año resulta ser más relevante y ofrecer mejoras significativas para los usuarios como el reemplazo del código de seis dígitos por un audio comprensible para el verificador o la forma en la que dos sistemas operativos completamente ajenos logran una autenticación entre si mediante ciertos protocolos, sin olvidar la importancia que tiene este tipo de autenticación en otros ámbitos más allá de la seguridad, específicamente en la privacidad de los usuarios.

Referencias

[1] Giménez, S. (2023, 27 junio). Informe OBS: Redes Sociales, estado actual y tendencias 2023. OBS Business School. https://www.obsbusiness.school/actualidad/informes-de-investigacion/informe-obs-redes-sociales-estado-actual-y-tendencias-2023

[2] Higuera, A. (2024, 22 enero). 100 millones de contraseñas robadas: el último macro 'hackeo' del que puedes formar parte. 20bits. https://www.20minutos.es/tecnologia/ciberseguridad/100-millones-contrasenas-robadas-macro-hackeo-5211221/

[3] Perez, D. (2018, enero 21). Sólo uno de cada diez usuarios utiliza la verificación en dos pasos, ¿por qué es una mala noticia? El Español. https://www.elespanol.com/omicrono/software/20180121/solo-usuarios-utiliza-verificacion-pasos-mala-noticia/278972896_0.html#:~:text=Seg%C3%BAn%20datos%20de%20Google%2C%20menos,o%20un%20mensaje%20de%20verificaci%C3%B3n.

[4] Donohue, B. (2020, 26 febrero). ¿Qué es la Autenticación de Dos Factores y Dónde Debo Utilizarla? Blog Oficial de Kaspersky. https://latam.kaspersky.com/blog/que-es-la-autenticacion-de-dos-factores-y-donde-debo-utilizarla/3270/

[5] Jaimovich, D. (2023, 23 noviembre). Los 14 tipos de ciberataques más comunes (y cómo prevenirlos). Invgate. https://blog.invgate.com/es/tipos-de-ciberataque

[6] Holmes, A. (2021, 21 abril). 533 million Facebook users' phone numbers and personal data have been leaked online. Business Insider. https://www.businessinsider.com/stolen-data-of-533-million-facebookusers-leaked-online-2021-4?r=MX&IR=T

[7] Blanco, A. G. (2020, 23 abril). Cómo proteger a los mayores de los «hackers» en tiempos de COVID-19. BBVA NOTICIAS. https://www.bbva.com/es/como-proteger-a-los-mayores-de-loshackers-en-tiempos-de-covid-19/

[8] Euronews. (2023, 30 mayo). Los «script kiddies»: el aumento de jóvenes que se involucran con el jaqueo informático. Euronews. https://es.euronews.com/next/2023/05/26/los-script-kiddies-elaumento-de-jovenes-que-se-involucran-con-el-jaqueo-informatico

[9] Taylor, C. (2023, 7 febrero). Universal Authentication Framework (UAF). CyberHoot. https://cyberhoot.com/cybrary/universal-authentication-framework-uaf/

[10] Arrieta, A. G., Sánchez, D. L., Lázaro, Á. L. S., Lancho, M. B. P., García-Bermejo-Ginner, J. R., Simón, J. A. H., & Vega, P. (2021c). Verificación en dos pasos en el proceso enseñanza/aprendizaje - [Twostep verification in the teaching / learning process]. Innovaciones Docentes En Tiempos de Pandemia. https://doi.org/10.26754/cinaic.2021.0108

[11] Octopus, C. (2021, 28 mayo). An In-depth Guide to FIDO Protocols: U2F, UAF, and WebAuthn (FIDO2). https://blog.strongkey.com/blog/guide-to-fido-protocols-u2f-uafwebauthn-fido2

[12] Ramiro, F. S. A., Pisano, A., & De Ingeniería, U. P. C. E. T. S. (2020). AudioMark: Autenticación de dos factores por medio de audio. http://hdl.handle.net/11531/43410

[13] Del Rocío, A. C. J., & Yanina, P. o. M. (2016, 8 septiembre). Diseño e implementación de una solución de integración de autenticación entre plataformas Windows y Linux, utilizando el directorio activo de Windows como controlador de dominio. https://www.dspace.espol.edu.ec/handle/123456789/43719

[14] Tinoco, L. M. E., Rivera, B. B., Navarrete, J. I., & Alarcón, C. H. M. (2022). Seguridad informática aplicando la Autentificación por Doble factor para la plataforma HomeOfi. Dialnet. https://dialnet.unirioja.es/servlet/articulo?codigo=8637935