Seguridad Informática: Doble factor de Autenticación (2FA)

Dottore, Mauricio; Micheletti, Nicolás Alejandro; Miñón, Lorenzo; Roatta, Santiago

CAETI – Universidad Abierta Interamericana

DV. Montes de Oca 725 – Buenos Aires - Argentina

{Mauricio.Dottore; NicolasAlejandro.Micheletti; Lorenzo.Mion}@alumnos.uai.edu.ar
{Santiago.Roatta}@uai.edu.ar

RESUMEN

Este paper examina en detalle la implementación del doble factor de autenticación (2FA) en el sector bancario de Argentina, destacando su importancia como medida de seguridad contra amenazas cibernéticas como lo es la ingeniería social. Se analizan métodos de autenticación secundarios usados por bancos argentinos y se exploran desafíos y estrategias para mitigar riesgos de acceso no autorizado. El estudio proporciona en sí una comprensión profunda del papel crucial del 2FA en la seguridad cibernética bancaria argentina.**[1]**

Palabras clave: 2FA, Amenazas cibernéticas, Ingeniería social, Seguridad en línea, Prevención de ataques.

1. INTRODUCCIÓN

En la era digital actual, donde la tecnología se ha convertido en una parte integral de nuestra vida diaria, la ciberseguridad emerge como un elemento crucial para proteger nuestra información personal y financiera. Con el crecimiento exponencial de las transacciones en línea, el acceso a servicios digitales y la gestión de datos sensibles, la necesidad de salvaguardar nuestras identidades y activos frente a las amenazas cibernéticas nunca ha sido más acuciante.

La autenticación, el proceso de verificar la identidad de un usuario, se rige como una primera línea de defensa en este contexto. Sin embargo, con el aumento de la sofisticación de los ataques cibernéticos, los métodos de autenticación tradicionales, como las contraseñas estáticas, se han vuelto cada vez más vulnerables. En respuesta a este desafío, el concepto de doble factor de autenticación (2FA) ha surgido como una solución efectiva para fortalecer la seguridad en línea.

En este contexto, este paper se propone explorar en detalle el concepto de doble factor de autenticación (2FA), su implementación en el sector bancario argentino y su eficacia en la protección de las cuentas en línea frente a la ingeniería social y otras amenazas cibernéticas. A través de este análisis, esperamos proporcionar una comprensión más profunda de la

importancia del 2FA en la seguridad digital cotidiana y destacar su papel crucial en la defensa contra las crecientes amenazas cibernéticas en el mundo actual.

2. CONCEPTOS BÁSICOS DE CIBERSEGURIDAD

En el entorno digital actual, la ciberseguridad es un campo multidisciplinario que abarca una amplia gama de conceptos y prácticas destinadas a proteger sistemas, redes y datos contra ataques cibernéticos. Para comprender la importancia del doble factor de autenticación (2FA) en este contexto, es fundamental familiarizarse con algunos conceptos básicos de ciberseguridad:

Autenticación: Verificación de la identidad del usuario mediante la presentación de credenciales.

Seguridad de la información: Protección de la confidencialidad, integridad y disponibilidad de los datos.

Amenazas cibernéticas: Incluyen virus, malware, phishing, ataques de denegación de servicio (DDoS), entre otros.

Ataques de ingeniería social: Engaños para obtener acceso no autorizado.

3. DOBLE FACTOR DE AUTENTICACIÓN

El doble factor de autenticación (2FA) es un método de seguridad que agrega una capa adicional de protección al proceso de autenticación tradicional basado en contraseñas. En lugar de depender únicamente de una contraseña estática, el 2FA requiere que los usuarios proporcionen dos formas diferentes de identificación antes de acceder a una cuenta o servicio en línea. Estas formas de identificación pueden incluir:

Algo que el usuario sabe: Esta primera forma de autenticación suele ser la contraseña tradicional.

Algo que el usuario posee: La segunda forma de autenticación implica el uso de un dispositivo físico o una aplicación móvil que genera códigos de verificación únicos. Esto puede incluir Tokens, SMS, Apps de autenticación, datos biométricos, etc

La combinación de estas dos formas de autenticación hace que sea considerablemente más difícil para los ciberdelincuentes comprometer una cuenta, incluso si logran obtener la contraseña de un usuario.

El 2FA ofrece varias ventajas sobre la autenticación basada únicamente en contraseñas:

Mayor seguridad: Al agregar una capa adicional de protección, el 2FA hace que sea mucho más difícil para los atacantes acceder a cuentas en línea incluso si tienen la contraseña de un usuario.

Reducción del riesgo de acceso no autorizado: El 2FA ayuda a mitigar el riesgo de acceso no autorizado al requerir que los usuarios proporcionen una segunda forma de identificación, lo que reduce las posibilidades de comprometer la seguridad de una cuenta.

Mejora de la experiencia del usuario: Aunque el 2FA puede agregar una breve capa de complejidad al proceso de inicio de sesión, la seguridad adicional que proporciona puede ayudar a los usuarios a sentirse más seguros al utilizar servicios en línea

4. IMPLEMENTACIÓN DEL 2FA EN LA BANCA ARGENTINA

La implementación del doble factor de autenticación (2FA) en el sector bancario argentino revela una diversidad de enfoques entre las distintas entidades financieras, cada una adoptando estrategias específicas para garantizar la seguridad de las cuentas de sus clientes en línea. Durante nuestra investigación, hemos estudiado varios bancos argentinos prominentes y hemos observado diferencias significativas en los métodos de 2FA utilizados.

A partir de estudios y análisis del sector bancario argentino, se observan diferencias significativas en la implementación del 2FA entre diversas entidades financieras en distintos grados. Observamos diferencias en los métodos utilizados, con algunas entidades adoptando tecnologías más avanzadas, mientras que otras se mantienen en métodos más tradicionales, lo que impacta directamente en la seguridad de las cuentas de los usuarios.. Estas diferencias en los métodos de autenticación tienen un impacto directo en la seguridad percibida de cada banco, ya que algunos métodos son inherentemente más robustos y menos susceptibles a ataques que otros.

Por ejemplo, hemos observado un banco que ha implementado un sistema de reconocimiento facial que requiere que los usuarios verifiquen su identidad mediante un escaneo facial cada vez que intentan iniciar sesión en su cuenta en línea. Además, este banco utiliza un segundo factor de autenticación en forma de un token de seguridad generado en el dispositivo del usuario, que se requiere para realizar cualquier transacción financiera. Este enfoque combina medidas biométricas avanzadas con una capa adicional de autenticación, lo que hace que las cuentas de los clientes sean altamente seguras y menos susceptibles a ataques de suplantación de identidad.

En contraste, otros bancos pueden depender exclusivamente de métodos de autenticación menos sofisticados, como códigos de verificación por SMS o contraseñas estáticas, que pueden ser más vulnerables a ataques de phishing o interceptación de comunicaciones. Estas diferencias en la implementación del 2FA tienen importantes implicaciones para la seguridad de las cuentas en línea de los clientes, y es crucial que los usuarios estén informados sobre las distintas opciones de autenticación disponibles y sus niveles relativos de seguridad.

Además, hemos observado que la implementación de 2FA no es uniforme entre los bancos, lo que sugiere la necesidad de una mayor atención a la seguridad en la industria bancaria en su conjunto. Si bien algunos bancos han adoptado medidas avanzadas de autenticación, otros aún dependen de métodos más tradicionales y potencialmente menos seguros. Esta disparidad resalta la importancia de la educación y concienciación de los usuarios sobre la importancia de elegir instituciones financieras que ofrezcan las mejores prácticas de seguridad en línea**[2]**.

En resumen, nuestro estudio destaca la importancia crítica de la implementación adecuada del 2FA en la banca en línea para garantizar la protección de los activos financieros y la privacidad de los clientes. Al elegir bancos que prioricen la seguridad y la adopción de medidas avanzadas de autenticación, los usuarios pueden contribuir significativamente a mitigar los riesgos de acceso no autorizado y protegerse contra las crecientes amenazas cibernéticas en un entorno digital en constante evolución.

5. INGENIERÍA SOCIAL Y 2FA

A pesar de ser una medida efectiva para mejorar la seguridad en línea, el doble factor de autenticación (2FA) no está exento de vulnerabilidades, especialmente cuando se trata de ataques de ingeniería social. La ingeniería social es una táctica utilizada por los ciberdelincuentes para engañar a los usuarios y obtener acceso no autorizado a sistemas o datos**[4]**.

Algunos ejemplos de ataques de ingeniería social que pueden eludir el 2FA incluyen:

- **Phishing:** Los ataques de phishing involucran el envío de correos electrónicos fraudulentos que se hacen pasar por comunicaciones legítimas de instituciones confiables, como bancos o empresas de servicios en línea. Estos correos electrónicos suelen contener enlaces maliciosos que redirigen a los usuarios a sitios web falsos diseñados para robar información de inicio de sesión y códigos de verificación de 2FA **[5]**.
- **Ingeniería social por teléfono:** Los ciberdelincuentes también pueden recurrir a llamadas telefónicas fraudulentas para engañar a los usuarios y obtener acceso a sus cuentas. Pueden hacerse pasar por representantes de servicios legítimos y solicitar información confidencial, como contraseñas y códigos de verificación de 2FA.
- **Ataques de intercambio de SIM:** En algunos casos, los atacantes pueden intentar persuadir a los proveedores de servicios móviles para que transfieran el número de teléfono de la víctima a un nuevo dispositivo controlado por ellos. Esto les permite recibir los códigos de verificación de 2FA.

Aunque el 2FA puede ayudar a mitigar el riesgo de acceso no autorizado al requerir una segunda forma de autenticación, es importante reconocer sus limitaciones y estar alerta ante posibles ataques de ingeniería social. Los usuarios deben ser educados sobre las mejores prácticas de seguridad en línea, cómo verificar la autenticidad de los correos electrónicos y las llamadas telefónicas, y utilizar métodos de autenticación secundarios, como aplicaciones

de autenticación móvil, en lugar de depender únicamente de los códigos de verificación por SMS.

6. COMPARACIÓN DE CIBERSEGURIDAD BANCARIA ARGENTINA CON LA DE OTROS PAÍSES

En comparación con otros países de América Latina, Argentina muestra un avance considerable en la implementación del 2FA en el sector bancario. Sin embargo, países como Brasil también están haciendo progresos notables. En Brasil, el Banco Central ha implementado regulaciones **[1]** que fomentan la adopción de tecnologías de autenticación avanzadas y ha lanzado campañas de concienciación sobre la ciberseguridad. Además, el uso de aplicaciones móviles para la autenticación y la verificación de transacciones es cada vez más común.

En países como Japón **[6]**, la ciberseguridad bancaria también ha avanzado significativamente. Las entidades financieras en estos países utilizan una combinación de autenticación basada en biometría, tokens físicos y aplicaciones de autenticación móvil. Además, la cultura de alta tecnología y la conciencia del usuario sobre la ciberseguridad contribuyen a la efectividad de estas medidas.

En Hong Kong **[7]**, las entidades financieras también han adoptado rigurosas medidas de seguridad para proteger las transacciones bancarias en línea, utilizando el doble factor de autenticación (2FA). Un ejemplo notable es el Bank of East Asia (BEA), que requiere el uso de contraseñas de un solo uso (OTP) enviadas por SMS a los usuarios registrados para autorizar diversas transacciones sensibles, como transferencias a cuentas no registradas y pagos de facturas

En la Unión Europea, la Directiva de Servicios de Pago 2 (PSD2) ha sido un catalizador significativo para la implementación del 2FA y MFA en el sector bancario. La PSD2 exige que los bancos utilicen la Autenticación Reforzada del Cliente (SCA).

En términos generales, A pesar de que Argentina ha avanzado en la adopción de 2FA, la dependencia de métodos como los SMS o códigos por correo electrónico la posiciona en una desventaja comparativa respecto a estos países.

7. CONCLUSIONES

La implementación del doble factor de autenticación (2FA) en la banca argentina y su efectividad en la protección contra las amenazas cibernéticas, incluida la ingeniería social, es un tema de gran relevancia en el contexto actual de seguridad en línea **[3]**. A partir del análisis realizado, podemos extraer varias conclusiones importantes

Importancia del 2FA: El 2FA se ha establecido como una medida esencial para fortalecer la seguridad en línea al agregar una capa adicional de protección al proceso de autenticación tradicional basado en contraseñas. Su implementación en la banca argentina ha contribuido significativamente a mejorar la seguridad de las cuentas en línea y a proteger los activos financieros de los clientes contra el acceso no autorizado.

Variedad de métodos de 2FA: Los bancos argentinos han adoptado diferentes enfoques para implementar el 2FA, ofreciendo una variedad de métodos de autenticación secundarios, como códigos de verificación por SMS, aplicaciones de autenticación móvil y tokens físicos. Esta diversidad proporciona a los usuarios opciones para elegir el método que mejor se adapte a sus necesidades y preferencias.

Desafíos de seguridad: A pesar de su eficacia, el 2FA no está exento de vulnerabilidades, especialmente cuando se trata de ataques de ingeniería social. Los usuarios deben estar alerta ante posibles intentos de phishing, suplantación de identidad y otros ataques destinados a eludir el 2FA y comprometer la seguridad de sus cuentas en línea.

Educación y concienciación: Los usuarios deben estar informados sobre las mejores prácticas de seguridad en línea y ser conscientes de los riesgos asociados con compartir información confidencial o realizar acciones impulsadas por la urgencia.

BIBLIOGRAFÍA

1. BCRA. (2023, 03 10). *Requisitos mínimos para la gestión y control de los riesgos de tecnología y seguridad de la información.* https://www.bcra.gob.ar/. https://www.bcra.gob.ar/pdfs/comytexord/A7724.pdf
2. *Cómo prevenir estafas virtuales*. (n.d.). BCRA. Retrieved May 13, 2024, from https://www.bcra.gob.ar/BCRAyVos/Como-prevenir-estafas-virtuales-i.asp
3. Mantovani, V. (2019). *Autenticación de Múltiples factores (MFA)*. http://bibliotecadigital.econ.uba.ar/. http://bibliotecadigital.econ.uba.ar/download/tpos/1502-1524_MantovaniV.pdf
4. Ministerio de Justicia de la República Argentina. (2024, 03). *¿Qué es la ingeniería social y cómo me protejo?* https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-la-ingenieria-social-y-como-protegerte
5. Bisquert, S. O. (n.d.). *La figura del "phishing" como modalidad delictiva. Problemática en cuanto a su encuadre jurídico*. http://www.saij.gob.ar/. Retrieved 2006, from http://www.saij.gob.ar/doctrina/dacf060096-bisquert-figura_phishing_como_modalidad.htm
6. Japan Bank Transfer: https://stripe.com/in/resources/more/furikomi-an-in-depth-guide#:~:text=Two%2Dfactor%20authentication%20(2FA)%3A,generated%20by%20a%20security%20device
7. Bank of East Asia: Hong Kong https://www.hkbea.com/pdf/en/cyberbanking/en_security_faq.pdf