Identidad Digital 2024

Por **Revista Empresarial & Laboral** en **TECNOLOGÍA**

Revista Empresarial & Laboral

Escrita por & para Empresarios

Durante el 2023, el volumen de ataques de identidad generados por IA aumentó a tal nivel que se ha convertido en un tema de consideración para consumidores, organizaciones e incluso líderes mundiales. La biometría se erige como una fuerza transformadora en la remodelación de la forma en que las personas interactúan con los sistemas digitales y la forma en que las organizaciones protegen la información confidencial.

Para el 2024, el panorama de la identidad digital está preparado para avances significativos, con innovaciones que redefinirán la verificación, elevarán los estándares de seguridad y mejorarán las experiencias de los usuarios.

iProov, líder en autenticación biométrica facial, da a conocer sus tendencias y predicciones de la identidad digital para este 2024, en el que aborda el futuro inminente de la biometría, donde la fusión de la ciencia y la seguridad promete un cambio de paradigma en la forma en que autenticamos, identificamos y protegemos dentro del ámbito digital.

1. **La biometría se convertirá en la piedra angular de la infraestructura de seguridad del mercado de servicios financieros de EE. UU.**

Durante el último año, muchas organizaciones de servicios financieros han ampliado el acceso digital remoto para satisfacer la demanda de los usuarios. Sin embargo, esto ha ampliado la superficie de ataque digital y ha creado oportunidades para los estafadores. El sector de servicios financieros de EE. UU. ha sido más lento en adoptar tecnologías de identidad digital que otras regiones, lo que podría atribuirse a los desafíos que enfrenta en torno a la regulación de la interoperabilidad y el intercambio de datos. Sin embargo, dado que se espera que el fraude de identidad sintética genere al menos 23.000 millones de dólares en pérdidas para 2030, la presión está aumentando desde todos los ángulos. Los consumidores esperan abrir cuentas y acceder a los servicios de forma remota con rapidez y facilidad, mientras que los estafadores socavan la seguridad a través de canales en línea y desvían dinero. Al mismo tiempo, existe la grave amenaza del incumplimiento de la norma Conozca a su Cliente (en inglés Know Your Customer – KYC) y de Prevención Blanqueo de Capitales (en inglés Anti-Money Laundering – AML)

Las sanciones por esto incluyen enormes multas e incluso procedimientos penales. Además, existe un mayor riesgo de eludir las sanciones y financiar a los adversarios del Estado. En respuesta, muchas instituciones financieras se están viendo obligadas a tomar medidas. Esto ha implicado reemplazar los engorrosos procesos de incorporación y suplantar los métodos de autenticación obsoletos, como contraseñas y códigos de acceso, con tecnologías avanzadas para incorporar y autenticar de forma remota a los clientes existentes de banca en línea.

Uno de los principales avances es la tecnología de verificación biométrica facial, que ofrece una comodidad y accesibilidad inigualables para los clientes y, al mismo tiempo, desafíos de seguridad inigualables para los adversarios. De acuerdo con iProov, más instituciones financieras reconocerán cómo la verificación biométrica remodelará y redefinirá el impacto positivo que la tecnología puede tener en el equilibrio de la seguridad con la experiencia del cliente y harán el cambio.

2. **Habrá un rápido aumento en el número de países en desarrollo que construyan programas de identidad digital basados en la identidad descentralizada**

Se estima que 850 millones de personas en todo el mundo carecen de una forma legal de identificación y, sin identidad, las personas luchan por abrir una cuenta bancaria, obtener empleo y acceder a la atención médica, lo que las deja excluidas financieramente. Los programas de identidad digital mejoran el acceso a servicios y oportunidades digitales. Permiten a las personas afirmar su identidad, acceder a plataformas en línea y participar en iniciativas de gobierno digital. Con el apoyo de la inversión de fondos del Banco Mundial, los programas de identidad digital pueden ayudar a las economías menos avanzadas a prevenir el robo de identidad y el fraude, así como proporcionar una forma alternativa de demostrar su identidad y acceder a servicios esenciales como beneficios, atención médica y educación. Basados en una identidad descentralizada, estos programas permitirán a los usuarios almacenar e intercambiar digitalmente documentos de identidad, como una licencia de conducir, y credenciales, como diplomas, y autenticarse sin una autoridad central. Una identidad descentralizada pone al usuario en control al permitirle administrar su identidad en un enfoque distribuido. En este sentido, según los expertos de iProov, los programas de identidad digital, ofrecerán la comodidad que los usuarios finales exigen ahora y abrirán vías esenciales para que las personas anteriormente desfavorecidas o marginadas accedan a servicios financieros y de bienestar.

2. **Se prohibirán las videollamadas remotas para verificar la identidad**

La verificación de videollamadas implica una videollamada individual entre el usuario y un operador capacitado. Se le pide al usuario que sostenga un documento de identidad y el operador lo compara con su cara. Sin embargo, se ha demostrado que la verificación de videollamadas proporciona pocas garantías de que el usuario final sea una persona «viva» y no imágenes artificiales generativas producidas por IA superpuestas de manera convincente en la cara del actor de amenazas.

Por ejemplo, en 2022, los investigadores del Chaos Computer Club lograron eludir la tecnología de verificación de videollamadas mediante el uso de IA generativa y una identificación falsificada. El caso mostró cómo esta tecnología, y los operadores humanos de los que depende, son altamente susceptibles a los ataques de imágenes sintéticas. Desde entonces, la Oficina Federal Alemana de Seguridad de la Información ha advertido contra la verificación por videollamadas por su vulnerabilidad a estos ataques.

Si los programas de identidad digital no pueden defenderse contra la amenaza de los deepfakes en la incorporación y la autenticación, serán explotados con fines delictivos, como el fraude en los pagos, el blanqueo de capitales y la financiación del terrorismo. Como tal, veremos movimientos por parte de los reguladores de servicios financieros para prohibir los métodos de verificación de videollamadas con una directiva para elegir métodos más confiables basados en híbridos que combinen la coincidencia automatizada de IA y la detección de vida con la supervisión humana del proceso de aprendizaje automático.

4. **Las organizaciones introducirán la autenticación mutua entre los empleados para la comunicación de alto riesgo y la incorporación remota de nuevos empleados**

A medida que las organizaciones confían cada vez más en los medios digitales para la comunicación confidencial, la necesidad de medidas sólidas de ciberseguridad es primordial para mitigar el riesgo. La introducción de la autenticación mutua para las comunicaciones y transacciones de alto riesgo es una medida de seguridad crucial que añade una capa adicional de protección contra el acceso no autorizado y las posibles amenazas. Además, en ciertas industrias, el cumplimiento normativo exige la implementación de medidas de seguridad sólidas. La autenticación mutua ayuda a las organizaciones a cumplir con estos requisitos de cumplimiento al demostrar un compromiso para garantizar canales de comunicación seguros y proteger la información confidencial.

5. **Las filtraciones de datos corporativos se triplicarán debido a los ataques exitosos generados por IA**

Desde hace algunos años, las organizaciones y las personas han confiado en la detección de correos electrónicos de phishing a través de errores ortográficos y gramaticales. Ese tiempo ya pasó. Tal es la calidad de Chat GPT que los actores de amenazas ahora pueden usarlo para generar ataques de phishing de alta calidad en comunicaciones muy convincentes y sin pistas sospechosas. En consecuencia, 2024 será testigo de un fuerte aumento tanto en la calidad como en el volumen de los ataques de phishing generados por IA. La formación en materia de seguridad se convertirá en una herramienta redundante y las organizaciones se verán obligadas

a buscar métodos alternativos y más fiables para autenticar de forma fiable a los usuarios internos y externos de sus plataformas.

Etiquetas: 2024 | Edición 175 | Identidad Digital | Revista empresarial y laboral

Deja una respuesta

Tu dirección de correo electrónico no será publicada. Los campos obligatorios están marcados con *

Comentario *

Nombre *

Correo electrónico *

Web

Guarda mi nombre, correo electrónico y web en este navegador para la próxima vez que comente.

PUBLICAR EL COMENTARIO

Artículos Recientes

- ¿Cómo Proteger tu Información Personal en un Mundo Digital?
- ¿Cómo potenciar su rutina laboral con Inteligencia Artificial?
- Los seguros de mascotas crecen un 40%
- La Transformación del Acceso a los Servicios Financieros en Colombia a través de la Banca Digital
- ¿Ya apareció la IA de META en tu aplicación de WhatsApp? Experta despeja temores y brinda recomendaciones de uso