

Transformación Tecnológica en Entidades Financieras



Las entidades financieras han experimentado una transformación tecnológica en los últimos años, esto se debe a las nuevas generaciones y el acceso a la información. En una parte la banca tecnológica o digital ha revolucionado el sector financiero, ofreciendo alternativas importantes para integrar a la población a través del acceso y uso de servicios financieros. Por otra, la pandemia del Covid-19 ha acelerado aún más este proceso, impulsando la adopción de tecnologías en el sector financiero. Los temas que más se han visto impactados son:

- Experiencia del cliente: Las tecnologías empleadas por las entidades financieras permiten que sus clientes puedan realizar transacciones interbancarias, pagos

de operaciones crediticias, tarjetas de crédito, servicios públicos, apertura de inversiones, revisar saldos y realizar otras transacciones directamente desde tu dispositivo móvil o computadora, sin necesidad de visitar una sucursal.

- Inclusión financiera: Permite que más personas tengan acceso a servicios innovadores, impulsando así el crecimiento económico.
- Innovación de productos: Billetera digital, móvil empresarial, conectividad con empresas, móvil personal, Monex, internet banking corporativo y personal, apertura de cuentas, solicitud de créditos, transferencias internacionales, firma digital, ahorros programados, inversiones

a la vista y largo, sinpe móvil, tarjetas virtuales, alertas instantáneas sobre transacciones, saldos y otros eventos financieros, lo que facilita el seguimiento y control de las cuentas.

- La billetera digital: Las personas usuarias ingresan las tarjetas de débito y crédito de la entidad para usuarios de Android la entidad tiene su aplicación o Apple pay para los usuarios de iOS, con esta billetera digital se pueden realizar compras de forma fácil y segura en comercios sin necesidad de efectivo o tarjetas físicas, no solicita el pin para las compras mayores a ¢30.000, inclusive se pueden enlazar con algunos relojes inteligentes.

La Banca digital elimina la necesidad de hacer fila, lo que ahorra tiempo significativo en transacciones financieras cotidianas, algunos bancos digitales ofrecen tasas de interés más competitivas en productos como cuentas de ahorro y certificados de depósito, además de permitir acceder a tus cuentas en todo momento, desde cualquier lugar, eliminando las restricciones de horarios de las sucursales tradicionales. Otro aspecto a resaltar de la banca digital es que esta contribuye a la reducción del uso de papel, al eliminar la necesidad de documentos físicos y estados de cuenta impresos.

La mayoría de las plataformas de banca digital utilizan autenticación de dos factores, mejorando la seguridad pues requieren una verificación adicional más allá de la contraseña. Algunas de ellas ofrecen alertas personalizadas sobre gastos, ayudando a mantener el control del presupuesto y evitar sorpresas financieras. Además, esta permite

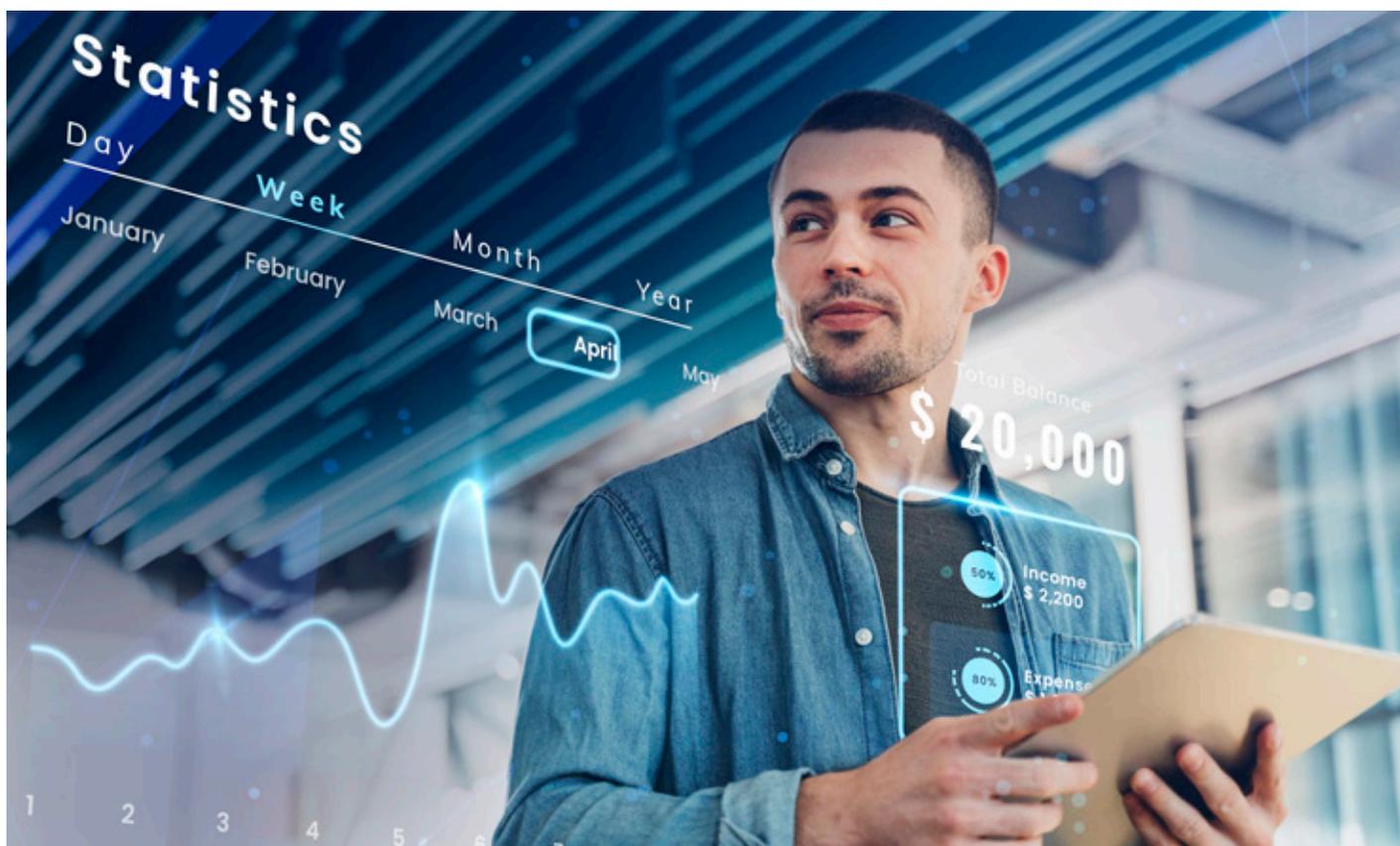
hacer uso de aplicaciones web de las instituciones financieras de una manera ágil y segura.

A pesar de sus beneficios, una entidad financiera puede tener desafíos o amenazas como fraudes, estafas, phishing o el uso de malware para hurtar o estafar a sus usuarios. Sobre el phishing, podríamos describirlo como el conjunto de técnicas que persiguen el engaño a una víctima, haciéndose pasar por una persona, empresa o servicio de confianza, para manipularla y hacer que realice acciones que no debería ejecutar, por ejemplo, revelar información o credenciales, para realizar algún trámite o solicitud.

Independiente de si se desarrollan por correo electrónico, por redes sociales, por SMS o mediante cualquier otro sistema, el ataque envía una comunicación dirigida con el fin de persuadir a la víctima para que le haga clic en un enlace, descargue un archivo adjunto, envíe información solicitada o incluso para que complete un pago. En adición, el phishing le permite a los ciberdelincuentes, instalar programas malignos (virus, gusanos, troyanos, keyloggers, botnets, spyware, entre otros) al dar clic al enlace, imágenes o archivos adjuntos con el único fin de capturar información personal o de la empresa.

Algunos temas tendencia o comúnmente usados para el phishing/vishing/smishing son: IBAN, fondo de capitalización laboral, factura electrónica, marchamo, firma digital, ofertas de trabajo, devolución de impuestos, transferencias bloqueadas, ofrecimiento de líneas de crédito, acceso bloqueado al canal electrónico, falso soporte técnico.

Asimismo, no debemos abrir correos con direcciones que no tienen relación con la empresa,



correos con faltas de ortografías, con errores gramaticales o ideas incongruentes, correos que soliciten o de actualización de información personal o credenciales de acceso, además de obtención de beneficios como gane de premios, amenazas como cancelación o cierre de cuenta bancarias, problemas legales por no responder a trámites pendientes no solicitados. Es por eso que las entidades financieras realizan múltiples campañas para evitar el robo de información confidencial, fraudes, tanto interna como externamente.

Por último, los datos sensibles de una tarjeta y con los cuales debemos ser particularmente cuidadosos son: números de tarjeta del cliente, fecha de vencimiento, código de seguridad, con lo cual pueden hacer compras por medio de datafonos abiertos, que se usan en paginas web para vender servicios o artículos.

Debido a lo anterior, se recomienda: mantener actualizada su información (teléfono, correo), active alertas financieras (le llegan correos o SMS por cada transacción o ingreso a la página web o aplicación), optimice su método de autenticación (token o firma digital), defina límites transaccionales. No utilice contraseñas de formato débil (fechas de nacimiento), evite redes públicas, en especial las de Internet tipo WIFI para realizar operaciones financieras por medio de los canales electrónicos, ya que sus datos pueden ser clonados.



Lic. Mauricio Lizano Calvo
Administración de Negocios y Finanzas, con más de 25 años de experiencia laboral en el Banco Nacional, ejecutando funciones como responsable de la Supervisión y Administración de personal, encargado de la coordinación de procesos operativos. Amplio conocimiento en legitimación de capitales, y control interno y demás productos bancarios.