MEJORA DE LA SEGURIDAD DIGITAL

CON AUTENTICACIÓN MULTIFACTOR

¿QUÉ ES LA AUTENTICACIÓN MULTIFACTOR?

La autenticación multifactor (MFA, por sus siglas en inglés) es un método de seguridad que requiere que los usuarios proporcionen dos o más factores de verificación para acceder a un recurso, como puede ser una aplicación, una cuenta en línea o una VPN. Con el creciente número de amenazas cibernéticas y violaciones de datos, es crucial contar con métodos de autenticación sólidos para proteger las cuentas en línea y la información confidencial.

La MFA a menudo combina algo que conoce (una contraseña), algo que ya tiene (un token de seguridad) y su apariencia física (biometría) para mejorar la seguridad. Esto añade una capa adicional de protección más allá de una sola contraseña.

TIPOS DE AUTENTICACIÓN MULTIFACTOR

1. AUTENTICACIÓN BASADA EN SMS

Cómo funciona: Se envía a su teléfono un código de acceso de un solo uso (OTP) a través de un mensaje SMS. A continuación, debe introducir el código recibido en el sistema para obtener acceso.

Pros: Es fácil de usar, no se necesita disponer de hardware especializado.

Contras: Puede ser interceptado por piratas informáticos, depende de la disponibilidad de la red móvil.

2. AUTENTICACIÓN BASADA EN CORREO ELECTRÓNICO

Cómo funciona: Se envía un OTP o un enlace de verificación a su dirección de correo electrónico registrada.

Pros: Cómodo, no se necesita de dispositivos adicionales.

Contras: Susceptible a ataques de phishing, puede tardar si los servidores de correo electrónico son lentos.

3. APLICACIONES DE AUTENTICACIÓN

Cómo funciona: Las aplicaciones de software generan OTP temporales que deberá introducir tras la contraseña.

Pros: Es un método más seguro que el envío de SMS, funciona sin necesidad de tener conexión a Internet.

Contras: Se necesita un smartphone, puede ser un inconveniente si se pierde el dispositivo.

4. AUTENTICACIÓN BIOMÉTRICA

Cómo funciona: Utiliza huellas dactilares, reconocimiento facial o escaneo de retina para verificar la identidad.

Pros: Se trata de un método altamente seguro, rápido y cómodo.

Contras: Se necesita hardware especializado, puede generar preocupaciones sobre la privacidad.

5. TOKENS DE HARDWARE

Cómo funciona: Los dispositivos físicos generan OTP o utilizan etiquetas USB/NFC para realizar la autenticación.

Pros: Es un método extremadamente seguro, inmune al phishing.

Contras: Es caro, puede perderse o ser objeto de un robo.

¿POR QUÉ SE DEBE UTILIZAR LA AUTENTICACIÓN MULTIFACTOR?

- **Seguridad mejorada:** La implementación de la MFA proporciona una capa adicional de seguridad más allá de las contraseñas.
- **Protección de los datos confidenciales:** Es crucial para salvaguardar la información personal y empresarial.
- **Conformidad:** Ayuda a cumplir con los requisitos corporativos y normativos para la protección de datos.
- **Reducción del fraude:** Minimiza el riesgo de acceso no autorizado y fraude.

La MFA es una herramienta simple pero de gran valor para reforzar significativamente la seguridad en línea. Al utilizar uno o más de los diversos tipos de MFA, puede protegerse a sí mismo/a y a su organización frente al acceso no autorizado a su información y frente a las posibles amenazas cibernéticas.

PHISHME COFENSE
SEGURIDAD DEL CORREO ELECTRÓNICO

CÓMO DETECTAR UN CORREO ELECTRÓNICO DE PHISHING

La capacidad de identificar un correo electrónico de phishing es crucial para proteger la información confidencial de los ciberdelincuentes. Debido a que los correos electrónicos de phishing tienen como objetivo engañar a los destinatarios para que divulguen información confidencial como contraseñas, detalles de tarjetas de crédito y otros datos personales, conllevan importantes riesgos.

Los actores de las amenazas a menudo se hacen pasar por entidades de confianza, lo que dificulta la detección de estas estafas. Ser víctima de un ataque de phishing puede tener graves consecuencias, como pueden ser el robo de identidad, pérdidas financieras y el acceso no autorizado a cuentas personales y corporativas.

La capacidad de reconocer y denunciar eficazmente los correos electrónicos de phishing es fundamental para mantenerse a usted y a su organización a salvo de un ciberataque. Entre los principales indicadores de un correo electrónico de phishing se encuentran los siguientes:

1. DIRECCIÓN SOSPECHOSA DEL REMITENTE

A menudo, los correos electrónicos de phishing provienen de una dirección que parece legítima, pero que contiene ligeras faltas de ortografía o caracteres adicionales.

2. SALUDOS DESCONOCIDOS O GENÉRICOS:

Los correos electrónicos de phishing suelen utilizar saludos genéricos como “Estimado cliente” en lugar de dirigirse a usted por su nombre.

3. LENGUAJE QUE IMPLICA URGENCIA O AMENAZA:

Los ciberdelincuentes a menudo intentan crear una sensación de urgencia, sugiriendo que se cerrará su cuenta o que debe actuar de inmediato para rectificar un problema.

4. ARCHIVOS ADJUNTOS O ENLACES INUSUALES

Los correos electrónicos de phishing pueden contener archivos adjuntos o enlaces. Para confirmar la legitimidad de un enlace, desplace el cursor sobre él antes de hacer clic.

5. SOLICITUD DE INFORMACIÓN PERSONAL:

Las organizaciones legítimas nunca le pedirán que facilite información confidencial como contraseñas, detalles de tarjetas de crédito o números de la seguridad social por correo electrónico. Si el remitente le pide que divulgue este tipo de información por correo electrónico, es muy probable que se trate de un intento de phishing.

6. ERRORES ORTOGRÁFICOS Y GRAMATICALES:

Muchos correos electrónicos de phishing contienen errores ortográficos y gramaticales importantes, poco comunes en las comunicaciones profesionales.

7. URL NO COINCIDENTES:

Un correo electrónico de phishing puede incluir URL que no coinciden con el texto al que están vinculados, o pueden dirigirle a un sitio web diferente al mencionado.

Reconocer estos indicadores puede ayudarle a evitar ser víctima de estafas de phishing. Una vez que sepa cómo detectar un phishing, ¡podrá detectar más ataques de phishing!

CÓMO INTENTAN ENGAÑARLE LOS PIRATAS INFORMÁTICOS

A medida que los ataques cibernéticos se vuelven más sofisticados, los empleados deben estar atentos y ser conscientes de la multitud de formas en que los piratas informáticos pueden obtener acceso a información confidencial. Desde esquemas de phishing hasta deepfakes, los ciberdelincuentes evolucionan constantemente sus métodos.

ESTAS SON ALGUNAS DE LAS FORMAS EN QUE PODRÍA ESTAR EN RIESGO DE SER VÍCTIMA DE UN DELITO CIBERNÉTICO:

ESCANEAR UN CÓDIGO QR

Los códigos QR están en todas partes, desde restaurantes hasta anuncios e incluso tarjetas de visita. Si bien son muy cómodos, también representan un riesgo significativo. Los ciberdelincuentes utilizan códigos QR malintencionados que enlazan directamente con sitios web de phishing para robar información personal o infectar su dispositivo con malware.

Tres maneras de mantenerse a salvo:

- Verificar el origen del código QR.
- Evite escanear códigos QR desde fuentes desconocidas o sospechosas.
- Utilice escáneres de códigos QR que puedan comprobar las URL antes de abrirlas.

A TRAVÉS DE UN MENSAJE DE TEXTO

Los piratas informáticos envían mensajes de texto engañosos para engañar a las personas y hacer que compartan datos privados o hagan clic en un enlace malintencionado. Estos mensajes a menudo parecen provenir de una fuente de confianza, como un banco o una agencia gubernamental.

Tres maneras de mantenerse a salvo:

- Tenga cuidado con los mensajes de texto no solicitados, especialmente aquellos que soliciten información personal.
- No haga clic en enlaces ni descargue archivos adjuntos de remitentes desconocidos.
- Verifique la legitimidad del texto poniéndose en contacto con la organización directamente.

POR TELÉFONO

Los estafadores a menudo llaman a las personas y se hacen pasar por entidades legítimas para sonsacar información confidencial. Las personas que llaman suelen utilizar un lenguaje manipulador para crear una sensación de urgencia o miedo.

Tres maneras de mantenerse a salvo:

- No proporcione información personal por teléfono a menos que conozca a ciencia cierta la identidad de la persona que llama.
- Verifique las credenciales de la persona que llama poniéndose en contacto con la organización directamente.
- Desconfíe de las llamadas no solicitadas que le piden que proporcione información confidencial.

PERSONAS QUE ESPÍAN POR ENCIMA DEL HOMBRO

Los atacantes miran por encima del hombro para observar la pantalla o el teclado y robar información confidencial, como contraseñas y PIN. Esta táctica, denominada “espiar por encima del hombro”, puede ocurrir en lugares públicos como cafeterías, aeropuertos o incluso dentro de su oficina.

Tres maneras de mantenerse a salvo:

- Esté atento/a a su entorno al introducir información confidencial.
- Utilice pantallas de privacidad en sus dispositivos y bloquéelos siempre cuando estén desatendidos.
- Proteja su teclado al escribir contraseñas o códigos de acceso.

TÉCNICA DE HACERSE PASAR POR ALGUIEN EN QUIEN CONFÍA

Los deepfakes utilizan la inteligencia artificial para crear vídeos o grabaciones de audio hiperrealistas, pero falsos. Los ciberdelincuentes pueden utilizar deepfakes para hacerse pasar por ejecutivos de empresas u otras personas de confianza, lo que provoca importantes violaciones de seguridad.

Tres maneras de mantenerse a salvo:

- Tenga cuidado con las solicitudes inesperadas o inusuales, incluso si parecen provenir de individuos conocidos.
- Verifique la identidad de la persona que realiza la solicitud a través de múltiples canales.
- Manténgase al tanto de los últimos desarrollos en tecnología deepfake.

CÓMO MANTENERSE A SALVO

AL USAR CHATBOTS DE IA

Los chatbots de inteligencia artificial (IA) ofrecen comodidad, pero también pueden plantear riesgos de seguridad. Dado el uso cada vez más habitual de chatbots de IA, tales como ChatGPT, esto es lo que debe hacer para proteger la privacidad de sus datos y evitar una violación.

1. COMPRENDA LOS RIESGOS

- ***Ataques de phishing:*** Los bots malintencionados se hacen pasar por servicios legítimos para robar su información.
- ***Distribución de malware:*** Los bots de IA se pueden utilizar para: Difundir software dañino.
- ***Privacidad de los datos:*** La información confidencial que se comparte en los bots pueden ser interceptada o mal utilizada.

2. UTILICE SERVICIOS DE CONFIANZA

- ***Verifique la legitimidad:*** Utilice solo chatbots de empresas de renombre.
- ***Busque sellos de seguridad:*** Asegúrese de que el servicio tenga las certificaciones de seguridad adecuadas.

3. PROTEJA SU INFORMACIÓN PERSONAL

- ***Evite compartir datos confidenciales:*** Nunca revele datos personales, financieros o de inicio de sesión a los chatbots de IA.
- ***Utilice contraseñas seguras:*** Asegúrese de que sus contraseñas sean complejas y únicas.

4. ACTUALICE EL SOFTWARE CON REGULARIDAD

- ***Mantenga el software actualizado:*** Asegúrese de que tanto su antivirus como el resto de software de seguridad estén actualizados.
- ***Busque actualizaciones de bots:*** Utilice chatbots que actualicen regularmente sus protocolos de seguridad.

5. SUPERVISE LA ACTIVIDAD

- ***Revise regularmente los estados de cuenta:*** Supervise los estados de cuenta bancarios y de tarjetas de crédito para detectar transacciones no autorizadas.
- ***Manténgase siempre informado/a:*** Manténgase al día con las últimas noticias de seguridad informática para estar al tanto de las nuevas amenazas.

6. DENUNCIE ACTIVIDADES SOSPECHOSAS

- ***Póngase en contacto con el servicio de asistencia:*** Si sospecha que un bot es malintencionado, informe de ello al proveedor de servicios de inmediato.
- ***Alerte a las autoridades:*** Notifique a las autoridades de seguridad informática locales o nacionales sobre cualquier violación de seguridad.

PHISHME
COFENSE
SEGURIDAD DEL
CORREO ELECTRÓNICO