



IMPORTANT NOTICE

Notice Regarding Fraudulent Impersonation and Unauthorized Use of Assivo Identity

Alerta de fraude y suplantación de identidad. Alerta de fraude e
falsificação de identidade.

Issued by	Assivo, Inc.
Date	September 5, 2026
Outside counsel	Ian J. Block, Partner, Intellectual Property, Neal, Gerber & Eisenberg LLP
Languages	English · Español · Português

Contents

English

Español

Português

Official Verification Reference

Overview

This notice is Assivo's canonical public reference for identifying official communications and reporting impersonation activity, including activity affecting persons in Latin America. It is published at assivo.com/fraud-alert and linked from the Assivo website.

Official Assivo Channels for Verification

- Official website: www.assivo.com
- Official corporate email domain: @assivo.com
- General contact: hello@assivo.com
- Official LinkedIn company page: linkedin.com/company/assivo
- Corporate office: 444 West Lake Street, Suite 1700, Chicago, Illinois 60606

English

Important Notice

Assivo, Inc. ("Assivo") has become aware of unauthorized third parties using or attempting to use the Assivo name, identity, trademarks, business information, employee identities, or other Assivo materials to impersonate the company or persons associated with it. Assivo has identified activity directed to persons in Latin America and is publishing this notice to help clients, prospective employees, vendors, business partners, and members of the public distinguish official Assivo communications from unauthorized activity.

These third parties are not authorized to represent Assivo. Assivo takes unauthorized use of its name, marks, corporate identity, website content, employee identities, and proprietary materials seriously and may take legal, technical, contractual, or other measures to address misuse of which it becomes aware.

1. Verify Assivo Through Official Channels

The official public website of Assivo is www.assivo.com. Authentic Assivo corporate email communications use the @assivo.com domain. Assivo's publicly listed general contact address is hello@assivo.com. Assivo's official LinkedIn company page is [linkedin.com/company/assivo](https://www.linkedin.com/company/assivo).

A website, email account, social profile, messaging account, document, or person should not be treated as authentic merely because it uses the Assivo name, logo, colors, address, photographs, employee names, biographies, job titles, company descriptions, client references, or content copied from the Assivo website.

When in doubt, navigate independently to www.assivo.com rather than using a link supplied in an unsolicited message. If the communication involves payment, employment, confidential information, or another material matter, verify it using contact information obtained independently from Assivo's official website.

2. Look-Alike Domains, Websites and Email Addresses

Fraudulent parties may register domain names or email addresses designed to resemble legitimate corporate channels. Minor differences can be difficult to detect, particularly on mobile devices. Warning signs include:

- Misspelled versions of assivo.com;
- Domains containing additional words, letters, numbers, punctuation, or hyphens;
- Different top-level domains or country-code extensions;
- Free consumer email accounts displaying the name of a real Assivo employee;
- Subdomains or shortened links that conceal the actual destination;
- Websites that copy Assivo branding, employee information, office information, or other public content;
- Recently created websites or domains that request immediate action, payment, credentials, or personal information.

The displayed sender name in an email is not sufficient verification. Recipients should inspect the complete sending address and domain.

3. Social Media, WhatsApp, Telegram and Private Messaging

Unauthorized persons may use social networks and private messaging platforms to create the appearance of a relationship with Assivo. Particular caution is appropriate with unsolicited communications through WhatsApp, Telegram, Instagram, Facebook, Messenger, Signal, SMS/text messaging, unverified LinkedIn accounts, or other private messaging services.

The use of a messaging platform does not establish that the sender is authorized by Assivo. Even when legitimate Assivo personnel use messaging services in the ordinary course of an established relationship, material employment, contractual, banking, payment, or confidential matters should be independently verifiable through an @assivo.com email address or other official Assivo channel.

4. Recruitment and Employment Fraud

Fraudulent parties may advertise purported Assivo jobs, conduct fake interviews, issue counterfeit offer letters, request personal information, or claim to provide onboarding, payroll, equipment, immigration, or training services on Assivo's behalf. Such communications may use the names or photographs of real Assivo employees or documents copied from legitimate sources.

Assivo does not require a candidate to pay Assivo or an Assivo representative in order to:

- Apply for a position or be considered for employment;
- Obtain or schedule an interview;
- Receive an employment offer;
- Secure or reserve a position;
- Receive training or complete onboarding;
- Purchase access to recruiting or payroll services;
- Obtain ordinary employment documentation; or
- Receive consideration for a legitimate Assivo employment opportunity.

A request for money, cryptocurrency, gift cards, personal transfers, or payment to an individual bank account in connection with purported employment should be treated as highly suspicious. Candidates should independently verify the opportunity through Assivo's official website and @assivo.com communications before providing sensitive information or taking financial action.

5. Personal Information and Account Credentials

Impersonation schemes may be designed to obtain sensitive personal, financial, or account information. Do not provide passwords, multi-factor authentication codes, complete banking credentials, cryptocurrency wallet credentials, payment-card information, or similar security information to a person merely because that person claims to represent Assivo.

Before providing identity, tax, payroll, banking, or other sensitive information in connection with employment or a business relationship, confirm the channel and the identity of the recipient independently.

6. Commercial, Vendor and Procurement Fraud

Businesses, vendors, and service providers should independently verify unusual communications purporting to originate from Assivo. Fraudulent parties may use the identity of a legitimate company to request goods or services, obtain trade credit, place purchase orders, solicit deposits, request advance payments, establish purported vendor relationships, obtain confidential information, or otherwise obtain money, property, services, or information.

The appearance of the Assivo name on an invoice, purchase order, proposal, contract, letterhead, email signature, electronic document, or other communication is not by itself evidence that Assivo issued, approved, or authorized the document.

7. Payment, Banking and Business Email Compromise

Payment fraud frequently involves attempts to change legitimate banking, beneficiary, remittance, or wire instructions. Email threads may be compromised, copied, or imitated. A reply appearing within an existing correspondence chain does not eliminate the need for independent verification when payment instructions change.

Exercise particular caution with unexpected requests involving:

- A new or changed bank account;
- A new beneficiary or payment destination;
- An urgent or unusual wire transfer;
- Payment to an individual rather than an established business account;
- Cryptocurrency or other non-standard payment methods;
- A request to bypass ordinary approval procedures;
- A change that conflicts with previously established payment practices.

Material changes to payment instructions should be verified using independently obtained contact information and established control procedures.

8. False Investment or Financial Solicitations

Assivo is a business process outsourcing and operations company. Assivo does not offer members of the public retail investment products, investment clubs, trading programs, cryptocurrency schemes, wealth-management accounts, or comparable consumer financial opportunities. A person using the Assivo name to promote such an offering should not be presumed to represent Assivo.

9. Impersonation of Real Employees or Executives

A fraudulent party may use the name, photograph, biography, job title, LinkedIn information, signature block, or other publicly available information of a real Assivo employee or executive. The fact that the information corresponds to an actual person does not establish that the sender is that person. Verify through an official Assivo channel.

10. Documents, Logos, Letterhead and Digital Materials

Digital materials can be copied, altered, or fabricated. The presence of any of the following should not be treated as independent proof of authenticity:

- The Assivo name or logo;
- Assivo letterhead or an Assivo office address;
- Employee names, photographs or biographies;
- Electronic signatures or identification cards;
- Contracts, proposals, invoices or purchase orders;
- Employment offers, recruiting or onboarding documents;
- Presentations, company descriptions or client references;
- Screenshots or links to genuine Assivo webpages.

Authenticity should be determined from the communication channel and independent verification, not merely the visual appearance of a document.

11. Latin America and Language-Specific Impersonation

Assivo operates internationally and has become aware of impersonation activity directed to persons in Latin America. A communication conducted in Spanish or Portuguese does not establish that it is authorized by Assivo. The fact that Assivo has international operations or personnel likewise does not mean that every person claiming a regional association with Assivo is authorized to act for the company.

Persons in Latin America should use the same verification standards described in this notice: confirm the domain, confirm the channel, confirm material requests independently, and do not send money or sensitive information solely because a sender uses convincing branding or accurate information about Assivo.

12. If You Receive a Suspicious Communication

1. Do not send money or financial assets.
2. Do not provide passwords, authentication codes, banking credentials, or unnecessary sensitive personal information.
3. Do not install software, mobile applications, browser extensions, or remote-access tools at the sender's request.
4. Do not rely solely on telephone numbers, websites, or links supplied by the suspicious sender.
5. Preserve the original communication and relevant evidence, including email headers where available.
6. Preserve website addresses, email addresses, telephone numbers, user names, screenshots, documents, payment instructions, and dates and times of communication.
7. Verify the communication independently through www.assivo.com or an established Assivo contact.
8. If money or financial information is involved, contact the relevant financial institution promptly and consider reporting the matter to appropriate authorities in your jurisdiction.

13. Reporting Suspected Misuse

Assivo welcomes reports concerning suspected unauthorized use of its identity, name, trademarks, website content, employee identities, or other materials. Reports are most useful when they include the source of the communication, screenshots, domain or profile information, contact details used by the suspected impersonator, copies of relevant documents, and any payment instructions provided.

Routine verification inquiries may be directed to Assivo using contact information published at www.assivo.com. For legal notices to Assivo, the company's public terms identify legal@assivo.com and Assivo, Inc., Attention: General Counsel, 444 West Lake Street, Suite 1700, Chicago, Illinois 60606.

14. Enforcement and Cooperation

Assivo reserves all rights relating to its name, trademarks, business identity, intellectual property, employee identities, and proprietary materials. Where appropriate, Assivo and its counsel may investigate reported misuse; preserve evidence; request the suspension, transfer, or removal of unauthorized domains, websites, accounts, advertisements, or content; communicate with registrars, hosting providers, social-media platforms, telecommunications providers, financial institutions, and other intermediaries; and refer suspected unlawful conduct to relevant governmental or law-enforcement authorities.

Nothing in this notice limits any rights or remedies available to Assivo, its affiliates, employees, or other affected persons.

Reporting to Outside Intellectual Property Counsel

Reports concerning suspected trademark misuse, fraudulent domains, unauthorized websites, impersonation, or misuse of Assivo identity may be directed to Assivo's outside intellectual property counsel:

Ian J. Block
Partner, Intellectual Property
Neal, Gerber & Eisenberg LLP
225 W. Randolph Street, Suite 2800, Chicago, Illinois 60606-1976
Direct: (312) 269-2960 | iblock@nge.com

Contacting counsel through this notice does not create an attorney-client relationship between Neal, Gerber & Eisenberg LLP and the reporting person. Do not send privileged, confidential, financial, or identity information beyond what is reasonably necessary to identify the suspected misuse.

15. No Assumption of Authenticity; No Public Attorney-Client Relationship

This notice is intended to assist the public in identifying official Assivo channels and reporting suspected impersonation. It does not guarantee that every unauthorized communication will display the warning signs described above, and it does not create an attorney-client relationship between any member of the public and Assivo's outside counsel. Persons who believe they have been victims of fraud should consider obtaining independent legal advice and contacting appropriate financial institutions or governmental authorities.

Español

Aviso importante

Assivo, Inc. ("Assivo") ha tenido conocimiento de terceros no autorizados que utilizan o intentan utilizar el nombre, la identidad, las marcas, la información comercial, las identidades de empleados u otros materiales de Assivo para hacerse pasar por la empresa o por personas vinculadas con ella. Assivo ha identificado actividad dirigida a personas en América Latina y publica este aviso para ayudar a clientes, candidatos, proveedores, socios comerciales y miembros del público a distinguir las comunicaciones oficiales de Assivo de actividades no autorizadas.

Estos terceros no están autorizados para representar a Assivo. Assivo toma seriamente el uso no autorizado de su nombre, marcas, identidad corporativa, contenido de su sitio web, identidades de empleados y materiales propietarios, y puede adoptar medidas legales, técnicas, contractuales u otras para responder al uso indebido del que tenga conocimiento.

1. Verifique a Assivo mediante canales oficiales

El sitio web público oficial de Assivo es www.assivo.com. Las comunicaciones corporativas auténticas de Assivo utilizan el dominio @assivo.com. La dirección general de contacto publicada por Assivo es hello@assivo.com. La página corporativa oficial de Assivo en LinkedIn es [linkedin.com/company/assivo](https://www.linkedin.com/company/assivo).

No debe considerarse auténtico un sitio web, cuenta de correo, perfil social, cuenta de mensajería, documento o persona únicamente porque utilice el nombre, logotipo, colores, dirección, fotografías, nombres de empleados, biografías, cargos, descripciones de la empresa, referencias de clientes o contenido copiado del sitio web de Assivo.

En caso de duda, acceda directamente a www.assivo.com en lugar de utilizar un enlace incluido en un mensaje no solicitado. Si la comunicación involucra pagos, empleo, información confidencial u otro asunto material, verifíquela utilizando información de contacto obtenida independientemente del sitio web oficial de Assivo.

2. Dominios, sitios web y correos electrónicos de apariencia similar

Las personas que cometen fraude pueden registrar dominios o direcciones de correo diseñados para parecerse a canales corporativos legítimos. Las diferencias pueden ser mínimas y difíciles de detectar, especialmente en dispositivos móviles. Señales de alerta:

- Versiones mal escritas de assivo.com;
- Dominios con palabras, letras, números, signos o guiones adicionales;
- Extensiones de dominio o códigos de país diferentes;
- Cuentas gratuitas de correo que muestran el nombre de un empleado real de Assivo;
- Subdominios o enlaces abreviados que ocultan el destino real;
- Sitios que copian la marca, información de empleados, oficinas u otro contenido público de Assivo;
- Dominios o sitios recientes que solicitan acción inmediata, pagos, credenciales o información personal.

El nombre mostrado como remitente no constituye verificación suficiente. Revise la dirección completa del remitente y su dominio.

3. Redes sociales, WhatsApp, Telegram y mensajería privada

Personas no autorizadas pueden utilizar redes sociales y plataformas de mensajería privada para aparentar una relación con Assivo. Tenga especial precaución con contactos no solicitados por WhatsApp, Telegram, Instagram, Facebook, Messenger, Signal, SMS, cuentas de LinkedIn no verificadas u otros servicios de mensajería.

El uso de una plataforma de mensajería no demuestra que el remitente esté autorizado por Assivo. Incluso cuando personal legítimo de Assivo utilice mensajería en el curso ordinario de una relación establecida, los asuntos materiales de empleo, contratos, banca, pagos o confidencialidad deben poder verificarse mediante una dirección @assivo.com u otro canal oficial.

4. Fraude de reclutamiento y empleo

Terceros pueden anunciar supuestos empleos en Assivo, realizar entrevistas falsas, emitir cartas de oferta falsificadas, solicitar información personal o afirmar que prestan servicios de incorporación, nómina, equipos, inmigración o capacitación en nombre de Assivo. Pueden utilizar nombres o fotografías de empleados reales o documentos copiados de fuentes legítimas.

Assivo no exige que un candidato pague a Assivo o a un representante de Assivo para:

- Presentar una solicitud o ser considerado para un puesto;
- Obtener o programar una entrevista;
- Recibir una oferta de empleo;
- Reservar o asegurar una vacante;
- Recibir capacitación o completar la incorporación;
- Comprar acceso a servicios de reclutamiento o nómina;
- Obtener documentación laboral ordinaria; o
- Ser considerado para una oportunidad legítima de empleo en Assivo.

Una solicitud de dinero, criptomonedas, tarjetas de regalo, transferencias personales o pagos a una cuenta bancaria individual en relación con un supuesto empleo debe considerarse altamente sospechosa. Antes de proporcionar información sensible o tomar una acción financiera, verifique la oportunidad mediante el sitio oficial de Assivo y comunicaciones desde @assivo.com.

5. Información personal y credenciales de cuenta

Las estafas de suplantación pueden estar diseñadas para obtener información personal, financiera o de acceso. No proporcione contraseñas, códigos de autenticación multifactor, credenciales bancarias completas, credenciales de billeteras de criptomonedas, información de tarjetas de pago u otros datos de seguridad a una persona únicamente porque afirme representar a Assivo.

Antes de proporcionar información de identidad, fiscal, de nómina, bancaria u otra información sensible en relación con un empleo o relación comercial, confirme de manera independiente el canal y la identidad del destinatario.

6. Fraude comercial, de proveedores y compras

Las empresas, proveedores y prestadores de servicios deben verificar de forma independiente comunicaciones inusuales que afirmen provenir de Assivo. Terceros pueden utilizar la identidad de una empresa legítima para solicitar bienes o servicios, obtener crédito comercial, emitir órdenes de compra, solicitar depósitos, pagos anticipados, relaciones de proveedor, información confidencial o de otro modo obtener dinero, propiedad, servicios o información.

La aparición del nombre Assivo en una factura, orden de compra, propuesta, contrato, papel membretado, firma de correo o documento electrónico no demuestra por sí sola que Assivo haya emitido, aprobado o autorizado el documento.

7. Pagos, datos bancarios y compromiso de correo empresarial

El fraude de pagos suele incluir intentos de modificar instrucciones bancarias, beneficiarios, remesas o transferencias. Los hilos de correo pueden ser comprometidos, copiados o imitados. Una respuesta dentro de un hilo existente no elimina la necesidad de verificar independientemente un cambio en las instrucciones de pago.

Tenga especial precaución con solicitudes inesperadas relacionadas con:

- Una cuenta bancaria nueva o modificada;
- Un nuevo beneficiario o destino de pago;
- Una transferencia urgente o inusual;
- Pago a una persona en lugar de una cuenta empresarial establecida;
- Criptomonedas u otros métodos de pago no habituales;
- Una solicitud para omitir controles o aprobaciones ordinarios;
- Cambios incompatibles con prácticas de pago previamente establecidas.

Los cambios materiales en las instrucciones de pago deben verificarse utilizando información de contacto obtenida independientemente y los procedimientos de control establecidos.

8. Falsas solicitudes de inversión o servicios financieros

Assivo es una empresa de externalización de procesos empresariales y operaciones. Assivo no ofrece al público productos de inversión minorista, clubes de inversión, programas de trading, esquemas de criptomonedas, cuentas de gestión patrimonial ni oportunidades financieras de consumo comparables. No debe presumirse que una persona que utilice el nombre Assivo para promover una oferta de este tipo represente a Assivo.

9. Suplantación de empleados o ejecutivos reales

Un tercero puede utilizar el nombre, fotografía, biografía, cargo, información de LinkedIn, firma o información pública de un empleado o ejecutivo real de Assivo. Que la información corresponda a una persona real no demuestra que el remitente sea esa persona. Verifique a través de un canal oficial de Assivo.

10. Documentos, logotipos, papel membretado y materiales digitales

Los materiales digitales pueden copiarse, alterarse o fabricarse. La presencia de cualquiera de los siguientes elementos no debe considerarse prueba independiente de autenticidad:

- El nombre o logotipo de Assivo;
- Papel membretado o dirección de oficina de Assivo;
- Nombres, fotografías o biografías de empleados;
- Firmas electrónicas o tarjetas de identificación;
- Contratos, propuestas, facturas u órdenes de compra;
- Ofertas de empleo y documentos de reclutamiento o incorporación;
- Presentaciones, descripciones de empresa o referencias de clientes;
- Capturas o enlaces a páginas genuinas de Assivo.

La autenticidad debe determinarse mediante el canal de comunicación y la verificación independiente, no únicamente por la apariencia visual de un documento.

11. América Latina y suplantación en español o portugués

Assivo opera internacionalmente y ha tenido conocimiento de actividad de suplantación dirigida a personas en América Latina. Una comunicación en español o portugués no demuestra que esté autorizada por Assivo. Del mismo modo, el hecho de que Assivo tenga operaciones o personal internacional no significa que toda persona que afirme una relación regional con Assivo esté autorizada para actuar en nombre de la empresa.

Las personas en América Latina deben aplicar los mismos estándares de verificación descritos en este aviso: comprobar el dominio, comprobar el canal, verificar independientemente las solicitudes materiales y no enviar dinero ni información sensible únicamente porque el remitente utilice una marca convincente o información exacta sobre Assivo.

12. Si recibe una comunicación sospechosa

1. No envíe dinero ni activos financieros.
2. No proporcione contraseñas, códigos de autenticación, credenciales bancarias ni información personal sensible innecesaria.
3. No instale software, aplicaciones móviles, extensiones de navegador o herramientas de acceso remoto a petición del remitente.
4. No confíe únicamente en teléfonos, sitios o enlaces proporcionados por el remitente sospechoso.
5. Conserve la comunicación original y la evidencia relevante, incluidos encabezados de correo cuando estén disponibles.
6. Conserve direcciones web y de correo, números de teléfono, nombres de usuario, capturas, documentos, instrucciones de pago y fechas y horas de las comunicaciones.
7. Verifique la comunicación independientemente mediante www.assivo.com o un contacto establecido de Assivo.
8. Si hay dinero o información financiera involucrados, contacte rápidamente a la institución financiera correspondiente y considere reportar el asunto a las autoridades competentes de su jurisdicción.

13. Reporte de posible uso indebido

Assivo agradece los reportes sobre posible uso no autorizado de su identidad, nombre, marcas, contenido web, identidad de empleados u otros materiales. Los reportes son más útiles cuando incluyen la fuente de la comunicación, capturas de pantalla, información del dominio o perfil, datos de contacto utilizados por el posible suplantador, copias de documentos relevantes e instrucciones de pago proporcionadas.

Las consultas rutinarias de verificación pueden dirigirse a Assivo utilizando la información publicada en www.assivo.com. Para notificaciones legales a Assivo, los términos públicos de la empresa identifican legal@assivo.com y Assivo, Inc., Attention: General Counsel, 444 West Lake Street, Suite 1700, Chicago, Illinois 60606.

14. Protección, cumplimiento y cooperación

Assivo se reserva todos los derechos relacionados con su nombre, marcas, identidad empresarial, propiedad intelectual, identidades de empleados y materiales propietarios. Cuando corresponda, Assivo y sus abogados pueden investigar reportes; preservar evidencia; solicitar la suspensión, transferencia o eliminación de dominios, sitios, cuentas, anuncios o contenidos no autorizados; comunicarse con registradores, proveedores de alojamiento, plataformas sociales, proveedores de telecomunicaciones, instituciones financieras y otros intermediarios; y remitir posibles conductas ilícitas a autoridades gubernamentales o policiales competentes.

Nada en este aviso limita los derechos o recursos disponibles para Assivo, sus afiliadas, empleados u otras personas afectadas.

Reporte a abogado externo de propiedad intelectual

Los reportes relacionados con el uso indebido de marcas, dominios fraudulentos, sitios web no autorizados, suplantación de identidad o uso indebido de la identidad de Assivo pueden dirigirse al abogado externo de propiedad intelectual de Assivo:

Ian J. Block
Partner, Intellectual Property
Neal, Gerber & Eisenberg LLP
225 W. Randolph Street, Suite 2800, Chicago, Illinois 60606-1976
Direct: (312) 269-2960 | iblock@nge.com

El contacto con el abogado a través de este aviso no crea una relación abogado-cliente entre Neal, Gerber & Eisenberg LLP y la persona que presenta el reporte. No envíe información privilegiada, confidencial, financiera o de identidad más allá de lo razonablemente necesario para identificar el posible uso indebido.

15. Sin presunción de autenticidad; sin relación abogado-cliente con el público

Este aviso pretende ayudar al público a identificar los canales oficiales de Assivo y reportar posibles suplantaciones. No garantiza que toda comunicación no autorizada muestre las señales de advertencia descritas y no crea una relación abogado-cliente entre un miembro del público y los abogados externos de Assivo. Quienes crean haber sido víctimas de fraude deben considerar obtener asesoría legal independiente y contactar a las instituciones financieras o autoridades gubernamentales correspondientes.

Português

Aviso importante

A Assivo, Inc. ("Assivo") tomou conhecimento de terceiros não autorizados que usam ou tentam usar o nome, a identidade, as marcas, informações comerciais, identidades de funcionários ou outros materiais da Assivo para se passar pela empresa ou por pessoas a ela relacionadas. A Assivo identificou atividade direcionada a pessoas na América Latina e publica este aviso para ajudar clientes, candidatos, fornecedores, parceiros comerciais e membros do público a distinguir comunicações oficiais da Assivo de atividades não autorizadas.

Esses terceiros não estão autorizados a representar a Assivo. A Assivo leva a sério o uso não autorizado de seu nome, marcas, identidade corporativa, conteúdo de seu site, identidades de funcionários e materiais proprietários e poderá adotar medidas legais, técnicas, contratuais ou outras para tratar de usos indevidos dos quais tome conhecimento.

1. Verifique a Assivo por meio de canais oficiais

O site público oficial da Assivo é www.assivo.com. Comunicações corporativas autênticas da Assivo utilizam o domínio @assivo.com. O endereço geral de contato publicado pela Assivo é hello@assivo.com. A página corporativa oficial da Assivo no LinkedIn é [linkedin.com/company/assivo](https://www.linkedin.com/company/assivo).

Um site, conta de e-mail, perfil social, conta de mensagens, documento ou pessoa não deve ser considerado autêntico apenas porque usa o nome, logotipo, cores, endereço, fotografias, nomes de funcionários, biografias, cargos, descrições da empresa, referências de clientes ou conteúdo copiado do site da Assivo.

Em caso de dúvida, acesse diretamente www.assivo.com em vez de usar um link fornecido em mensagem não solicitada. Se a comunicação envolver pagamento, emprego, informação confidencial ou outro assunto relevante, confirme-a usando informações de contato obtidas independentemente no site oficial da Assivo.

2. Domínios, sites e endereços de e-mail semelhantes

Terceiros fraudulentos podem registrar domínios ou endereços de e-mail criados para parecer canais corporativos legítimos. Pequenas diferenças podem ser difíceis de perceber, especialmente em dispositivos móveis. Sinais de alerta:

- Versões com grafia alterada de assivo.com;
- Domínios com palavras, letras, números, sinais ou hífen adicionais;
- Extensões de domínio ou códigos de país diferentes;
- Contas gratuitas de e-mail exibindo o nome de um funcionário real da Assivo;
- Subdomínios ou links encurtados que ocultam o destino real;
- Sites que copiam a marca, informações de funcionários, escritórios ou outro conteúdo público da Assivo;
- Sites ou domínios recém-criados que solicitam ação imediata, pagamento, credenciais ou informações pessoais.

O nome exibido como remetente não é verificação suficiente. Confira o endereço completo do remetente e o domínio utilizado.

3. Redes sociais, WhatsApp, Telegram e mensagens privadas

Pessoas não autorizadas podem usar redes sociais e plataformas de mensagens privadas para aparentar uma relação com a Assivo. Tenha especial cuidado com contatos não solicitados via WhatsApp, Telegram, Instagram, Facebook, Messenger, Signal, SMS, contas não verificadas do LinkedIn ou outros serviços de mensagens.

O uso de uma plataforma de mensagens não comprova que o remetente esteja autorizado pela Assivo. Mesmo quando profissionais legítimos da Assivo utilizam mensagens no curso normal de uma relação já estabelecida, assuntos relevantes de emprego, contratos, bancos, pagamentos ou confidencialidade devem poder ser confirmados por um endereço @assivo.com ou outro canal oficial.

4. Fraude de recrutamento e emprego

Terceiros podem divulgar supostas vagas na Assivo, realizar entrevistas falsas, emitir cartas de oferta falsificadas, solicitar dados pessoais ou alegar que prestam serviços de admissão, folha de pagamento, equipamentos, imigração ou treinamento em nome da Assivo. Podem usar nomes ou fotografias de funcionários reais ou documentos copiados de fontes legítimas.

A Assivo não exige que um candidato pague à Assivo ou a um representante da Assivo para:

- Candidatar-se a uma vaga ou ser considerado para emprego;
- Obter ou agendar entrevista;
- Receber uma proposta de emprego;
- Garantir ou reservar uma vaga;
- Receber treinamento ou concluir admissão;
- Comprar acesso a serviços de recrutamento ou folha de pagamento;
- Obter documentação trabalhista ordinária; ou
- Ser considerado para uma oportunidade legítima de emprego na Assivo.

Solicitações de dinheiro, criptomoedas, cartões-presente, transferências pessoais ou pagamentos para conta bancária de pessoa física em conexão com suposto emprego devem ser tratadas como altamente suspeitas. Antes de fornecer dados sensíveis ou realizar qualquer pagamento, confirme a oportunidade pelo site oficial da Assivo e por comunicações no domínio @assivo.com.

5. Dados pessoais e credenciais de acesso

Golpes de falsificação de identidade podem ter como objetivo obter dados pessoais, financeiros ou credenciais de acesso. Não forneça senhas, códigos de autenticação multifator, credenciais bancárias completas, credenciais de carteiras de criptomoedas, informações de cartões ou outros dados de segurança a uma pessoa apenas porque ela afirma representar a Assivo.

Antes de fornecer dados de identidade, fiscais, de folha de pagamento, bancários ou outras informações sensíveis relacionadas a emprego ou relação comercial, confirme de forma independente o canal e a identidade do destinatário.

6. Fraude comercial, de fornecedores e compras

Empresas, fornecedores e prestadores de serviços devem verificar de forma independente comunicações incomuns que aleguem ter origem na Assivo. Terceiros podem usar a identidade de uma empresa legítima para solicitar bens ou serviços, obter crédito comercial, emitir pedidos de compra, solicitar depósitos, pagamentos antecipados, relações de fornecimento, informações confidenciais ou, de outra forma, obter dinheiro, bens, serviços ou informações.

A presença do nome Assivo em uma fatura, pedido de compra, proposta, contrato, papel timbrado, assinatura de e-mail ou documento eletrônico não comprova, por si só, que a Assivo tenha emitido, aprovado ou autorizado o documento.

7. Pagamentos, dados bancários e comprometimento de e-mail empresarial

Fraudes de pagamento frequentemente envolvem tentativas de alterar dados bancários, beneficiários, remessas ou instruções de transferência. Cadeias de e-mail podem ser comprometidas, copiadas ou imitadas. Uma resposta que aparece dentro de uma conversa existente não elimina a necessidade de verificação independente quando há mudança nas instruções de pagamento.

Tenha especial cuidado com solicitações inesperadas envolvendo:

- Conta bancária nova ou alterada;
- Novo beneficiário ou destino de pagamento;
- Transferência urgente ou incomum;
- Pagamento para pessoa física em vez de conta empresarial estabelecida;
- Criptomoedas ou outros métodos de pagamento não usuais;
- Solicitação para contornar aprovações ou controles normais;
- Mudança incompatível com práticas de pagamento previamente estabelecidas.

Mudanças relevantes nas instruções de pagamento devem ser verificadas com informações de contato obtidas independentemente e com os procedimentos de controle já estabelecidos.

8. Falsas ofertas de investimento ou serviços financeiros

A Assivo é uma empresa de terceirização de processos empresariais e operações. A Assivo não oferece ao público produtos de investimento de varejo, clubes de investimento, programas de trading, esquemas de criptomoedas, contas de gestão patrimonial ou oportunidades financeiras de consumo semelhantes. Uma pessoa que use o nome Assivo para promover uma oferta desse tipo não deve ser presumida como representante da empresa.

9. Falsificação da identidade de funcionários ou executivos reais

Um terceiro pode usar o nome, fotografia, biografia, cargo, informações do LinkedIn, bloco de assinatura ou outras informações públicas de um verdadeiro funcionário ou executivo da Assivo. O fato de as informações corresponderem a uma pessoa real não comprova que o remetente seja essa pessoa. Confirme por meio de um canal oficial da Assivo.

10. Documentos, logotipos, papel timbrado e materiais digitais

Materiais digitais podem ser copiados, alterados ou fabricados. A presença de qualquer dos elementos abaixo não deve ser considerada prova independente de autenticidade:

- Nome ou logotipo da Assivo;
- Papel timbrado ou endereço de escritório da Assivo;
- Nomes, fotografias ou biografias de funcionários;
- Assinaturas eletrônicas ou cartões de identificação;
- Contratos, propostas, faturas ou pedidos de compra;
- Ofertas de emprego e documentos de recrutamento ou admissão;
- Apresentações, descrições empresariais ou referências de clientes;
- Capturas de tela ou links para páginas genuínas da Assivo.

A autenticidade deve ser determinada pelo canal de comunicação e por verificação independente, e não apenas pela aparência visual de um documento.

11. América Latina e falsificação em espanhol ou português

A Assivo opera internacionalmente e tomou conhecimento de atividade de falsificação de identidade direcionada a pessoas na América Latina. Uma comunicação em espanhol ou português não comprova que tenha sido autorizada pela Assivo. Da mesma forma, o fato de a Assivo possuir operações ou profissionais internacionais não significa que toda pessoa que alegue uma associação regional com a Assivo esteja autorizada a agir em nome da empresa.

Pessoas na América Latina devem aplicar os mesmos padrões de verificação descritos neste aviso: conferir o domínio, conferir o canal, confirmar solicitações relevantes de forma independente e não enviar dinheiro ou informações sensíveis apenas porque o remetente utiliza uma marca convincente ou informações corretas sobre a Assivo.

12. Se você receber uma comunicação suspeita

1. Não envie dinheiro nem ativos financeiros.
2. Não forneça senhas, códigos de autenticação, credenciais bancárias ou dados pessoais sensíveis desnecessários.
3. Não instale software, aplicativos móveis, extensões de navegador ou ferramentas de acesso remoto a pedido do remetente.
4. Não confie apenas em telefones, sites ou links fornecidos pelo remetente suspeito.
5. Preserve a comunicação original e as evidências relevantes, incluindo cabeçalhos de e-mail quando disponíveis.
6. Preserve endereços de sites e e-mails, números de telefone, nomes de usuário, capturas de tela, documentos, instruções de pagamento e datas e horários das comunicações.
7. Confirme a comunicação de forma independente por meio de www.assivo.com ou de um contato já estabelecido da Assivo.
8. Se houver dinheiro ou informações financeiras envolvidas, entre em contato prontamente com a instituição financeira relevante e considere relatar o caso às autoridades competentes de sua jurisdição.

13. Relato de possível uso indevido

A Assivo agradece relatos sobre possível uso não autorizado de sua identidade, nome, marcas, conteúdo do site, identidades de funcionários ou outros materiais. Os relatos são mais úteis quando incluem a origem da comunicação, capturas de tela, informações de domínio ou perfil, dados de contato utilizados pelo possível falsificador, cópias de documentos relevantes e quaisquer instruções de pagamento fornecidas.

Consultas rotineiras de verificação podem ser encaminhadas à Assivo usando as informações publicadas em www.assivo.com. Para notificações legais à Assivo, os termos públicos da empresa identificam legal@assivo.com e Assivo, Inc., Attention: General Counsel, 444 West Lake Street, Suite 1700, Chicago, Illinois 60606.

14. Proteção, aplicação e cooperação

A Assivo reserva todos os direitos relacionados a seu nome, marcas, identidade empresarial, propriedade intelectual, identidades de funcionários e materiais proprietários. Quando apropriado, a Assivo e seus advogados poderão investigar relatos; preservar evidências; solicitar suspensão, transferência ou remoção de domínios, sites, contas, anúncios ou conteúdos não autorizados; comunicar-se com registradores, provedores de hospedagem, plataformas sociais, provedores de telecomunicações, instituições financeiras e outros intermediários; e encaminhar possíveis condutas ilícitas às autoridades governamentais ou policiais competentes.

Nada neste aviso limita direitos ou medidas disponíveis à Assivo, suas afiliadas, funcionários ou outras pessoas afetadas.

Relato ao advogado externo de propriedade intelectual

Relatos relacionados a uso indevido de marca, domínios fraudulentos, sites não autorizados, falsificação de identidade ou uso indevido da identidade da Assivo podem ser encaminhados ao advogado externo de propriedade intelectual da Assivo:

Ian J. Block
Partner, Intellectual Property
Neal, Gerber & Eisenberg LLP
225 W. Randolph Street, Suite 2800, Chicago, Illinois 60606-1976
Direct: (312) 269-2960 | iblock@nge.com

O contato com o advogado por meio deste aviso não cria relação advogado-cliente entre Neal, Gerber & Eisenberg LLP e a pessoa que apresenta o relato. Não envie informações privilegiadas, confidenciais, financeiras ou de identidade além do razoavelmente necessário para identificar o possível uso indevido.

15. Sem presunção de autenticidade; sem relação advogado-cliente com o público

Este aviso tem o objetivo de ajudar o público a identificar os canais oficiais da Assivo e relatar possíveis falsificações de identidade. Ele não garante que toda comunicação não autorizada apresentará os sinais de alerta descritos e não cria relação advogado-cliente entre qualquer membro do público e os advogados externos da Assivo. Pessoas que acreditem ter sido vítimas de fraude devem considerar buscar orientação jurídica independente e contatar as instituições financeiras ou autoridades governamentais apropriadas.

Official Verification Reference

Referencia oficial de verificación · Referência oficial de verificação

Website	www.assivo.com
Email domain	@assivo.com
General contact	hello@assivo.com
Legal contact	legal@assivo.com
LinkedIn	linkedin.com/company/assivo
Corporate office	444 West Lake Street, Suite 1700, Chicago, Illinois 60606
Outside counsel	Ian J. Block, Partner, Intellectual Property, Neal, Gerber & Eisenberg LLP
	225 W. Randolph Street, Suite 2800, Chicago, Illinois 60606 (312) 269-2960 iblock@nge.com

Table 1. Official Assivo channels and counsel of record.

Assivo | 444 West Lake Street, Suite 1700, Chicago, IL 60606 | [assivo.com](https://www.assivo.com)