Dans le monde des affaires d'aujourd'hui, assurer la sécurité des données est devenu une priorité. Des études récentes montrent qu'une société a 26 % de risque de faire face à une importante fuite de données dans un délai déterminé de 24 mois[1]. Il peut paraitre surprenant d'apprendre qu'une mauvaise gestion et que les pratiques de travail des employés sont responsables de la plupart des atteintes à la sécurité — plus encore que les attaques malveillantes ou les actes criminels. Pour une entreprise, les atteintes à la sécurité peuvent entrainer des conséquences sur le plan financier et sur sa réputation, et finalement conduire à un manque de confiance à l'égard de sa marque.

Si vous échangez des renseignements sensibles, essentiels ou critiques avec des clients et des partenaires et que vous utilisez des technologies de communication non sécurisées telles que des courriels, des serveurs FTP, des solutions de synchronisation et de partage de fichiers en entreprise sans assurer une véritable protection et sans appliquer une stratégie de conformité rigoureuse, vous pourriez prendre des risques importants et inutiles.

UTILISEZ-VOUS L'UNE DES MÉTHODES SUIVANTES POUR ÉCHANGER DES RENSEIGNEMENTS SENSIBLES ?

Courriel

Le courriel n'a pas été conçu en tenant compte des normes en matière de sécurité et de vie privée. Les courriels sont transmis en texte clair sur Internet et stockés à divers emplacements liés à différents fournisseurs de services, ce qui augmente de façon exponentielle les possibilités de piratage.

Fichiers zip protégés par mot de passe

Il existe de nombreux outils et tutoriels gratuits qui permettent de « craquer » facilement des mots de passe de fichiers zip, et ce, en quelques minutes.

Envoi de deux courriels séparés

Il est courant d'envoyer un courriel contenant des renseignements sensibles suivi d'un deuxième courriel contenant des renseignements sensibles complémentaires. Cette pratique n'est absolument pas sûre. Si quelqu'un parvient à accéder à une boîte de réception, il aura accès aux deux courriels.

Chargement de fichiers sur un serveur FTP

De nombreux fournisseurs de service Internet et systèmes de messagerie d'entreprise empêchent l'envoi de gros fichiers. Par conséquent, les employés se tournent vers les serveurs FTP standards ou vers des services de partage de fichiers. Ces solutions ne permettent pas de protéger les données sensibles et peuvent être difficiles à utiliser.

Envoi de CD, DVD ou clés USB par courrier ou coursier

L'envoi de données par la poste ou par le biais d'un coursier est en réalité l'une des méthodes les moins fiables pour l'échange de données sensibles et peut devenir dispendieux. En effet, la probabilité que le paquet contenant les données se perde en route est élevée.

À PROPOS DE LA SOLUTION XMediusSENDSECURE CLOUD

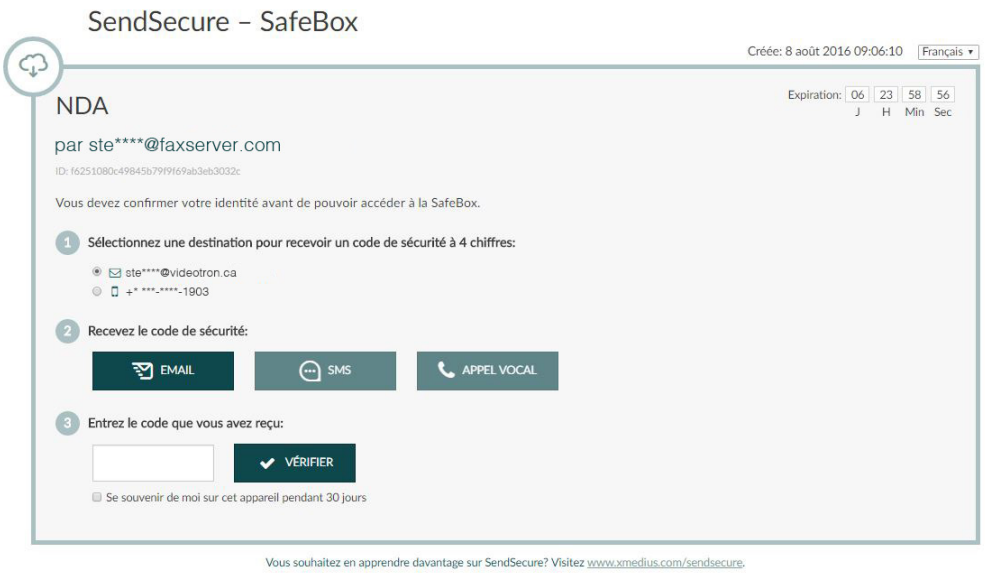
SendSecure est une plateforme d'échange de fichiers de pointe hautement sécurisée et conviviale. Elle a été conçue pour permettre l'échange et le stockage de fichiers de nature sensible dans un coffre-fort virtuel. Ces documents sont cryptés à l'envoi comme à la réception. De plus, SendSecure requiert l'authentification de l'expéditeur ainsi que la double authentification du destinataire. Enfin, elle supprime automatiquement les anciens fichiers en vertu de la durée de vie qui est déterminée au moment de la création d'un coffre-fort éphémère et fournit une piste d'audit de toutes les communications.

[1] Source : Ponemon Institute LLC, 2016

Hautement sécurisée

- Authentification à deux facteurs (A2F)

  Une fois que l'expéditeur a créé le coffre-fort, le destinataire reçoit un courriel comportant le lien de téléchargement. Il doit alors entrer un code secondaire à usage unique (authentification à deux facteurs), qui a été transmis par SMS, par appel vocal ou par courriel.



- Cryptage

  SendSecure utilise des méthodes de cryptage recommandées par les experts des institutions bancaires et en sécurité. Toutes les communications sont chiffrées à l'aide du protocole TLS 1.2 (avec confidentialité persistante). Lorsque les fichiers sont inactifs, ils sont chiffrés à l'aide de l'algorithme de chiffrement AES de 256 bits.

- Double cryptage

  SendSecure protège le coffre-fort des intrus ou des employés non habilités grâce à un double cryptage. L'une des deux clés nécessaires au décryptage du contenu du coffre-fort doit être fournie par l'expéditeur ou le destinataire avant de pouvoir accéder au contenu.

- Coffre-fort éphémère

  SendSecure permet de personnaliser la durée de vie d'un coffre-fort. Une fois l'expiration de la durée de vie, tous les fichiers placés dans le coffre-fort sont effacées et ne sont plus accessibles par aucun intervenant. L'expéditeur peut également fermer un coffre-fort à tout moment et choisir le niveau de sécurité.

- Installations d'hébergement

  XMedius s'est associée avec « Amazon Web Services» (AWS), une des infrastructures de serveurs les plus sécurisées au monde. AWS publie son « Web Risk and Compliance Program », qui comprend toutes les certifications, rapport et attestations tierces (disponible sur demande). En outre, XMedius a obtenu les certifications et accréditations (ISO/IEC 27001) de sécurité appropriées pour démontrer la sécurité de son infrastructure et ses services.

Conviviale

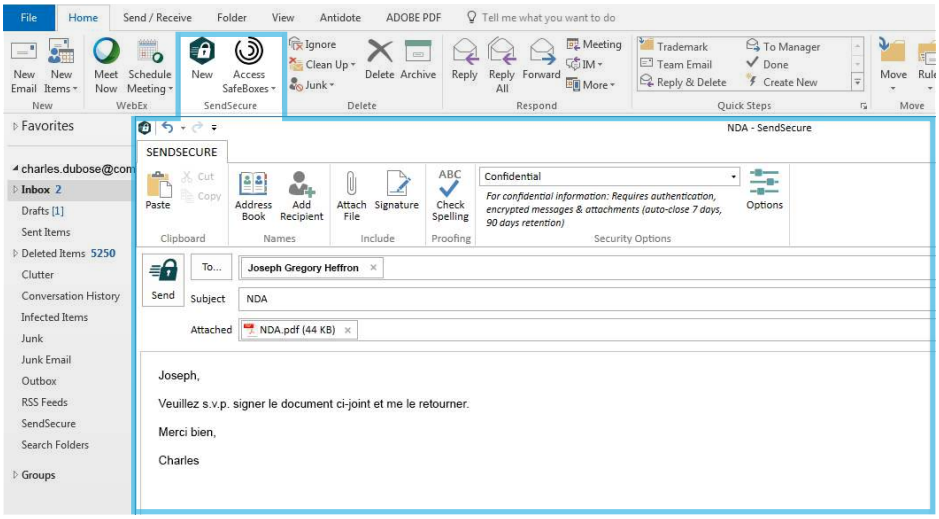
- Expérience usager supérieure

  De conception intuitive, SendSecure est aussi facile à utiliser que d'envoyer un courriel. De plus, la solution ne requière pas d'abonnement, ni aucun téléchargement de logiciels ni matériel pour le destinataire. Seuls des appareils de communication sont nécessaires, comme un ordinateur, un téléphone mobile ou une tablette et un navigateur web. Sa conception étonnamment simple signifie que la formation des employés ne constitue plus un problème, et qu'on peut l'adopter facilement.

Conviviale (cont.)

- **Intégration en toute simplicité**

  L'intégration facile de SendSecure avec Outlook (Office 365) permet d'envoyer tout type de fichiers, petits ou volumineux, à partir d'Outlook sans devoir ouvrir une autre application. Les utilisateurs peuvent également envoyer des fichiers cryptés, petits ou volumineux, à partir d'un téléphone mobile ou d'une tablette à une ou plusieurs personnes à l'aide d'un navigateur web.



- **Véritable solution mobile**

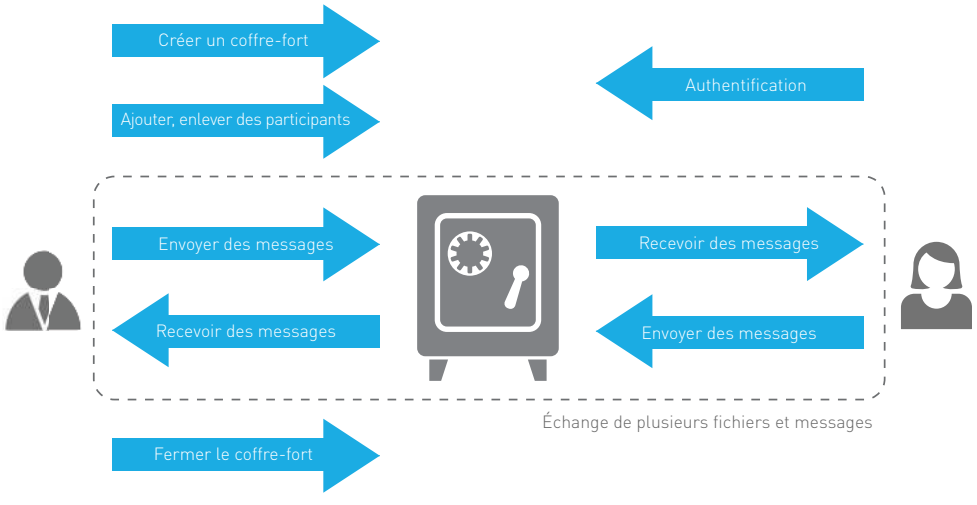
  SendSecure permet aux utilisateurs habilités d'échanger des fichiers de toute taille en toute sécurité depuis n'importe quel appareil professionnel ou personnel (y compris les smartphones et les tablettes), que ce soit au bureau ou en déplacement. Il s'agit donc d'un outil de rendement supérieur.

- **Aucune limite de taille pour les fichiers**

  SendSecure permet de transférer tout type de fichier (texte, image, audio et vidéo) jusqu'à 5 GB/message ainsi qu'un nombre illimité de messages par mois. La majorité des serveurs de messagerie restreignent la taille des pièces jointes à moins de 10 Mo.

- **Travail en collaboration**

  SendSecure permet au destinataire d'opter pour une conversation bidirectionnelle en plus de recevoir une transmission de document sécurisée. Cette collaboration est possible en cliquant simplement sur le bouton « Répondre »



Échange de plusieurs fichiers et messages

- **Gestion des destinataires**

  SendSecure vous permet de rappeler ou de supprimer facilement un message ou un fichier avant que son destinataire ne l'ait vu. De plus, la solution permet d'inviter des destinataires supplémentaires pendant une conversation en cours.

Une traçabilité

- Preuve d'audit

  La solution SendSecure conserve des rapports de transmission signés numériquement qui consignent tous les accès à un coffre-fort. L'expéditeur reçoit automatiquement des courriels confirmant toutes les actions réalisées par le destinataire lors des différentes étapes du processus. Un rapport détaillé de transmission pouvant être imprimé, téléchargé ou envoyé par courriel en format PDF est créé après la fermeture du coffre-fort.

- Archivage

  Cette solution permet d'archiver, sur la plateforme ou vers un espace de stockage ou un lecteur externe, tous les documents qui ont été échangés.

POURQUOI ADOPTER XMediusSENDSECURE ?

Protection des renseignements et atténuation du risque de réputation

Ces dernières années, de nombreuses entreprises se sont fait voler des renseignements internes sensibles – quand ils n'ont pas été perdus ou divulgués intentionnellement. Leur image ainsi que leurs marques peuvent en avoir souffert sérieusement. Le préjudice est impossible à évaluer et les impacts négatifs peuvent se faire sentir encore pendant de nombreuses années. SendSecure contribue à réduire au minimum ces risques.

Limiter d'éventuels litiges et amendes

Certaines réglementations en vigueur dans l'industrie – telles que HIPAA (Health Insurance Portability and Accountability Act), Sarbanes-Oxley, la Gramm-Leach-Bliley, etc. – exigent de la part des entreprises qu'elles prennent les mesures appropriées pour protéger leurs données confidentielles. SendSecure répond aux normes de conformité les plus élevées. La plateforme XMedius Cloud est certifiée ISO/IEC 27001:2013. Cette certification offre une assurance objective que les employés qui utilisent le service SendSecure peuvent gérer efficacement un programme de sécurité complet ainsi que les risques liés à la sécurité de l'information.

DES SOLUTIONS ADAPTÉES À L'ENTREPRISE

Marque blanche

Le service SendSecure peut être soit fourni sous la marque XMedius, soit personnalisé pour s'ajuster à une marque ou une identité propre (« marque blanche »).

Administration et création de rapports

Pour gérer les utilisateurs, générer des rapports et bien plus encore, les administrateurs de SendSecure peuvent s'appuyer sur l'interface Web sécurisée.

Diffusion mondiale

Les langues disponibles pour communiquer avec le client (courriels, interface utilisateur, rapports PDF) sont l'anglais, le français et l'allemand.

À QUI LA SOLUTION SENDSECURE DE XMEDIUS EST-ELLE DESTINÉE ?

Santé

Les professionnels de la santé – médecins, infirmières, administrateurs, etc. – et les établissements médicaux – cliniques, hôpitaux, etc. – peuvent recourir à SendSecure pour :

- L'envoi sécurisé de messages, de dossiers et de documents médicaux aux patients, aux compagnies d'assurance, recherche clinique, etc.

- L'échange de résultats d'IRM, de scanners et d'autres fichiers de diagnostic volumineux entre les médecins et leurs patients.

Finance

Les clients des établissements financiers ne peuvent généralement utiliser que les systèmes de communication électronique mis à leur disposition par l'établissement. Ces systèmes requièrent souvent le téléchargement de logiciels et la création de comptes. Pire encore, le système est parfois différent à l'envoi et au retour des documents.

Secteur bancaire

- La solution SendSecure permet d'alléger la charge de travail des responsables des prêts qui transmettent des documents de nature délicate à faire signer à leurs clients
- Elle garantit la confidentialité des documents juridiques envoyés aux organismes de réglementation, aux conseillers juridiques indépendants ou aux partenaires commerciaux
- Elle protège les communications des équipes exécutives qui doivent échanger des informations, que ce soit entre elles ou avec leur conseil d'administration, des conseillers indépendants ou des organismes de réglementation

Sociétés de prêt hypothécaire ou courtiers

- SendSecure est la solution idéale pour les responsables des prêts qui doivent envoyer et recevoir des documents sensibles
- Elle facilite le travail des services qui reçoivent des documents de la part d'experts, de sociétés de titres, d'entités gouvernementales, de banques et d'autres intervenants extérieurs

Compagnies d'assurance et courtiers

- Elle facilite l'échange d'informations dans le cadre des réclamations d'assurance
- Elle permet de recevoir des plans de construction détaillés ou d'autres données pertinentes pour établir des devis précis destinés aux clients

Juridique

Les avocats doivent régulièrement gérer des informations client confidentielles et ont l'obligation de les protéger, qu'elles aient été détournées accidentellement ou délibérément.

Les utilisations courantes de SendSecure comprennent :

- L'envoi de contrats à d'autres avocats en interne ou appartenant à d'autres firmes
- L'envoi de courriels et de fichiers sensibles à des particuliers et des entreprises
- L'utilisation de l'accusé de réception qui prouve que les destinataires ont bien reçu et ouvert les courriels sécurisés

Organismes gouvernementaux

Les organismes gouvernementaux traitent de grandes quantités de données personnelles de nature délicate sur les citoyens qui doivent être protégées.

- Communiquer en toute sécurité les numéros de sécurité sociale
- Échanger sans risques des renseignements sur la déclaration de taxe

Distributeur / Revendeur :

XMedius
info@xmedius.com
Amériques : 1-888-766-1668
EMEA : +33 1 70 92 13 10
XMEDIUS.COM