RISQUES ET RESSOURCES EN MATIÈRE DE CYBERSÉCURITÉ :

Protéger le secteur canadien de l'agriculture et de l'agroalimentaire

À mesure que les entreprises agricoles et agroalimentaires deviennent plus numérisées et connectées en ligne, il est d'autant plus important qu'elles se protègent contre la cybercriminalité. L'agriculture de précision, l'automatisation et les technologies d'agriculture intelligente contribuent à l'efficacité et à la productivité, mais en l'absence de mesures de protection adéquates, la porte s'ouvre à des vulnérabilités cybernétiques qui peuvent avoir des effets dévastateurs en paralysant les entreprises, en diminuant la rentabilité et en nuisant à la confiance des consommateurs.

Dans ce contexte numérique, il est essentiel de **comprendre les risques cybernétiques et de s'en prémunir**.

Qu'est-ce que la cybersécurité ?

La cybersécurité est la pratique qui consiste à protéger les systèmes informatiques, les réseaux et les données contre les perturbations numériques. Des exemples de cyberincidents touchant le secteur agricole et agroalimentaire comprennent **des messages frauduleux, des courriels d'hameçonnage visant à obtenir des renseignements personnels et l'accès aux systèmes, et des demandes de rançongiciel**, pour n'en nommer que quelques-uns.

Quels systèmes agricoles sont à risque ?

Les cibles peuvent comprendre les données sur la production, les finances et les clients et d'autres données, les capteurs sans fil, la machinerie automatisée et robotisée, les véhicules et l'équipement autonomes et semi-autonomes, ainsi que les commandes et les systèmes de chauffage, de réfrigération, d'éclairage et de ventilation.

Conseils pour réduire les risques au minimum

- **Assurez-vous de créer des mots de passe différents pour tous vos comptes**, de préférence d'une longueur de 12 caractères, dont au moins une lettre minuscule, une lettre majuscule et un caractère spécial. **Modifiez fréquemment vos mots de passe**.
- **Activez l'authentification multifactorielle** pour tous vos comptes, dans la mesure du possible.
- **Sauvegardez régulièrement** les renseignements importants, y compris les données et les renseignements des fournisseurs et des clients. Conservez une copie des renseignements hors ligne ou sur un lecteur externe.
- **N'ouvrez pas de courriels inconnus et ne cliquez pas sur des liens ou des pièces jointes** à moins d'en connaître la provenance et la légitimité.
- **N'enregistrez pas de données personnelles ou financières dans les navigateurs** si on vous invite à le faire et évitez les fonctions de remplissage automatique.
- **Consultez d'autres conseils à l'adresse agriculture.canada.ca/cybersecurite-entreprise-agricole**.

Commencez dès aujourd'hui à utiliser ces outils et ressources

Centre canadien pour la cybersécurité

Une ressource de référence pour obtenir des conseils d'expert, une orientation, des services et du soutien, et pour signaler les incidents cybernétiques.

cyber.gc.ca

Sécurité publique Canada

Accédez aux évaluations des outils canadiens de cybersécurité en sélectionnant « Sécurité nationale » puis « Cybersécurité ».

securitepublique.gc.ca

Community Safety Knowledge Alliance (en anglais seulement)

Accédez à des ressources ciblées pour aider à protéger votre entreprise agricole.

cskacanada.ca/projects/strengthening-the-cyber-security-capacity-of-canadas-agricultural-sector

Agriculture et Agroalimentaire Canada | Agriculture and Agri-Food Canada

Canada

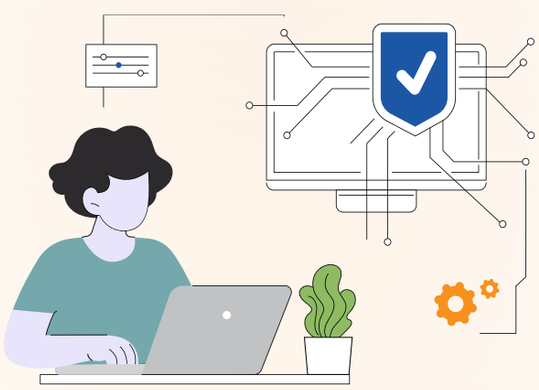
LISTE DE VÉRIFICATION EN MATIÈRE DE CYBERSÉCURITÉ POUR LES PETITES ET MOYENNES ENTREPRISES

La cybersécurité et votre enterprise agricole

Vous pouvez prendre des mesures **simples** et **efficaces** pour **renforcer votre protection** contre les incidents de cybersécurité courants

Sécurisez vos appareils et vos données

- [ ] J'ai **changé tous les mots de passe par défaut de tous les appareils** qui sont connectés à Internet (IdO) ou qui sont munis d'un GPS, aussi bien dans mon exploitation agricole que chez moi.
  - Ces appareils comprennent notamment les **routeurs de mes réseaux Wi-Fi et les appareils des tracteurs et des machines au champ**.
- [ ] J'utilise un mot de passe **unique et robuste** pour chacun de mes comptes.
- [ ] J'ai établi une **politique relative aux mots de passe** pour mes employés.
  - **Je rappelle aux employés qu'ils doivent changer leur mot de passe tous les trimestres** et qu'ils ne peuvent pas réutiliser un mot de passe.
- [ ] J'ai activé **l'authentification à facteurs multiples (AFM)** pour tous mes comptes.
  - Cette mesure **ajoute un niveau de sécurité** et rend l'accès à mes comptes plus difficile pour les auteurs de menaces.



Restez à jour et protégez-vous

- [ ] J'ai **téléchargé et installé** un logiciel antivirus réputé provenant d'une source fiable.
- [ ] J'ai **mis à jour les micrologiciels de tous les systèmes** de mon environnement à partir de sources fiables afin de réduire au minimum le risque d'attaque de la chaîne d'approvisionnement.
- [ ] J'ai **activé la mise à jour automatique des logiciels** afin de ne pas manquer une mise à jour de sécurité importante.
- [ ] Je passe en revue **la liste des employés autorisés à accéder au réseau et aux données** tous les six mois, et je supprime les autorisations, au besoin.
- [ ] Tous les six mois, **je passe en revue les applications que j'ai téléchargées** sur mes appareils et je désinstalle celles que je n'utilise plus.
  - Je vérifie régulièrement **les autorisations des applications** pour m'assurer qu'elles ne demandent pas l'accès à des données qui ne sont pas pertinentes pour leur fonction.
  - Je **désactive l'autorisation** qui permet à une application de connaître ma position lorsque je n'utilise pas l'application.
- [ ] J'ai pour principe de **sauvegarder les renseignements importants tous les trimestres et d'en conserver une copie hors ligne** ou hors réseau. Je pourrai ainsi récupérer mes dossiers en cas de faille.
  - Il s'agit notamment des **principales coordonnées des clients, des fournisseurs et des partenaires ainsi que de toutes les données agricoles** exclusives recueillies à l'aide des appareils technologiques agricoles de l'exploitation.

Pour de plus amples renseignements sur la façon de **réduire les risques liés à la cybersécurité**, consultez le site **agriculture.canada.ca/cybersecurite-entreprise-agricole**

Pour des ressources supplémentaires sur la façon de rester en sécurité en ligne, visitez **pensezcybersecurite.gc.ca**

Agriculture et Agroalimentaire Canada
Agriculture and Agri-Food Canada
Canada

QUESTIONS RELATIVES À LA CYBERSÉCURITÉ À PRENDRE EN COMPTE AVANT VOTRE PROCHAIN ACHAT DE TECHNOLOGIES AGRICOLES

Protégez votre entreprise agricole contre les risques de la cybersécurité

À mesure que votre entreprise agricole devient de plus en plus numérisée et connectée, il est essentiel de se prémunir contre les risques de la cybersécurité. Les questions suivantes peuvent vous aider à lancer la conversation avec les fournisseurs pour que vous puissiez prendre des décisions éclairées sur les personnes à qui vous faites confiance pour protéger votre entreprise contre les risques liés à la cybersécurité et protéger vos données et vos opérations.

Le fournisseur a-t-il une bonne réputation ?

- Depuis combien de temps exerce-t-il ses activités ?
- Avez-vous entendu parler de ce fournisseur avant d'envisager de faire un achat ?

Le fournisseur travaille-t-il avec des entreprises de votre secteur ?

- Connaît-il votre secteur d'activité ou votre produit ?
- S'agit-il d'un fournisseur qui cherche à élargir son champ d'action ou d'un nouveau fournisseur ?
- A-t-il une bonne réputation ?
- Pouvez-vous vous adresser à d'autres clients pour connaître leur expérience (clients de référence) ?

Quelles mesures le fournisseur prendra-t-il en cas d'atteinte à la protection des données stockées qui vous concernent, vous et votre entreprise ?

- Une telle situation s'est-elle déjà produite ? Dans l'affirmative, que s'est-il passé ?
- Peut-il vous expliquer simplement comment vos données sont stockées ?
- Possède-t-il un plan d'intervention d'urgence qu'il peut vous montrer ou vous expliquer ?

Le fournisseur peut-il expliquer votre contrat en langage clair ?

- Peut-il fournir des réponses directes à vos questions sur les clauses de votre contrat ?
- Peut-il vous dire où vos informations sont stockées, qui y a accès et comment elles sont protégées ?

Cette liste de questions n'est pas exhaustive. Elle se veut un point de départ pour vous aider à examiner vos possibilités en matière de fournisseurs.

Pour de plus amples renseignements sur la façon de **réduire les risques liés à la cybersécurité**, consultez le site **agriculture.canada.ca/cybersecurite-entreprise-agricole**

Pour des ressources supplémentaires sur la façon de rester en sécurité en ligne, visitez **pensezcybersecurite.gc.ca/fr**

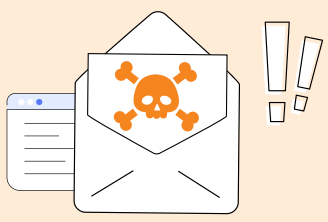
Agriculture et Agroalimentaire Canada
Agriculture and Agri-Food Canada
Canada

CYBERSÉCURITÉ : UNE ÉTUDE DE CAS DANS LE SECTEUR LAITIER

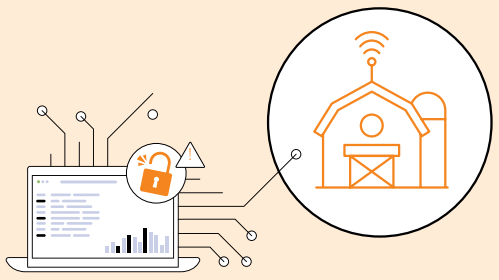
Les agroentreprises de toutes tailles sont vulnérables aux cyberincidents. Voici un exemple de la façon dont une attaque par hameçonnage pourrait avoir une incidence sur votre entreprise et de ce que vous pouvez faire pour la protéger.

Alex, propriétaire d'une **petite exploitation laitière**, reçoit un **courriel supposément de la banque** sur son ordinateur d'entreprise.

Le courriel indique que le **compte bancaire d'Alex a été bloqué**. Voulant le réactiver, **Alex clique sur le lien**.



Malheureusement, le **courriel et le lien sont frauduleux**. Au lieu de mener au site web de la banque, le lien télécharge un rançongiciel sur l'ordinateur d'Alex.



L'ordinateur portable d'Alex est **connecté à l'ensemble du réseau de l'exploitation**. Le rançongiciel se propage rapidement et crypte toutes les données de l'exploitation.

Cette attaque a de graves conséquences

Trayeuses automatiques

Le rançongiciel **arrête** les trayeuses autonomes, ce qui **perturbe** le programme de traite et a des **répercussions** sur la santé des vaches et la production de lait.

Perturbation de la chaîne d'approvisionnement

Toutes les **coordonnées** et les **communications** de la chaîne d'approvisionnement sont cryptées, ce qui interrompt les commandes et la distribution.

- Alex ne peut pas passer de commandes d'aliments pour animaux, de fournitures vétérinaires ou d'équipements, et ne peut pas recevoir de mises à jour sur les livraisons.
- Le processus de distribution est paralysé. Les livraisons de lait sont interrompues, les inventaires et l'état des commandes sont affectés.

Arrêt des activités

Les logiciels de gestion agricole et les dossiers essentiels sont **inaccessibles**, ce qui a des conséquences sur les activités de l'exploitation.

- L'exploitation ne peut pas communiquer avec ses partenaires ou gérer la logistique, ce qui entraîne des retards, des délais non respectés et une atteinte potentielle à la réputation.
- Alex ne peut pas accéder à ses courriels pour joindre les clients.
- Beaucoup de commandes sont retardées, des livraisons sont oubliées et la confiance des partenaires est érodée.

L'exploitation agricole d'Alex **ne dispose pas d'une équipe de TI ni d'une cyberassurance**. En l'absence de services de restauration en cas d'incident, Alex **sent une obligation de payer la rançon pour décrypter les données et reprendre ses activités**. Les pertes financières et les perturbations des activités sont dévastatrices.

La situation d'Alex aurait pu être atténuée

- Alex et **les employés auraient dû être formés** pour reconnaître les courriels d'hameçonnage et éviter de cliquer sur des liens suspects.
- **Des logiciels antivirus et anti-logiciels malveillants** auraient pu détecter et bloquer le rançongiciel avant qu'il ne se propage.
- **La segmentation du réseau** peut empêcher la propagation des logiciels malveillants.
- **Des sauvegardes régulières** sur un site isolé, hors réseau, auraient permis à Alex de restaurer plus facilement les systèmes. La sauvegarde des données crée des copies des informations importantes, et le stockage séparément du système principal, p. ex. sur un disque dur externe ou un service sécurisé en nuage, renforce le degré de sécurité.
- **Une cyberassurance** peut fournir un soutien financier et un accès à des services professionnels d'intervention en cas d'incident.
- **Les interventions en cas d'incident** permettent de s'assurer que tous les employés savent comment réagir en cas de cyberincident.

Soyez vigilant pour protéger votre entreprise

Visitez notre **site web** pour plus de renseignements

agriculture.canada.ca/cybersecurite-entreprise-agricole

Agriculture et Agroalimentaire Canada
Agriculture and Agri-Food Canada
Canada

GLOSSAIRE DE LA CYBERSÉCURITÉ

Logiciel antivirus/anti-maliciel : programme utilisé pour prévenir, cerner et supprimer les virus et autres logiciels malveillants d'un ordinateur.

Continuité des activités : capacité d'une organisation à maintenir ses fonctions essentielles en cas de perturbation, comme un cyberincident ou une catastrophe naturelle. Un plan de continuité des activités (PCA) décrit le protocole et les processus suivis par une organisation pour assurer la continuité de ses opérations avec le moins de perturbations possible.

Cyberincident : tentative par des auteurs de menace de causer des dommages à des renseignements de nature délicate dans un système informatisé en réseau, d'y obtenir un accès non autorisé ou de les détruire.

Mesures de cyberprotection : mesures prises pour protéger les données, les réseaux et les systèmes informatiques contre l'accès non autorisé, le vol ou les dommages.

Temps d'arrêt : période pendant laquelle il est impossible d'accéder à un système, à une application ou à l'ensemble du réseau d'une entreprise en raison de sa défaillance. Les temps d'arrêt peuvent survenir en raison d'activités de maintenance, de coupures de courant ou de défaillances techniques inattendues attribuables à un cyberincident. Les conséquences peuvent prendre la forme d'une perte de revenus, d'une baisse de la productivité, de coûts de rétablissement des systèmes, et d'atteinte à la réputation.

Lecteur externe : périphérique de stockage qui se connecte à un ordinateur, souvent au moyen d'un connecteur USB (bus série universel), FireWire ou Thunderbolt.

Plan d'intervention en cas d'incident : document écrit, approuvé officiellement par l'équipe de la haute direction, qui aide l'organisation avant, pendant et après un incident de cybersécurité confirmé ou présumé.

Internet des objets (IdO) : réseau d'appareils physiques permettant le transfert de données d'un appareil à l'autre sans intervention humaine. L'IdO ne se limite pas aux ordinateurs et peut englober tout appareil équipé d'un capteur, d'un logiciel et d'une connexion réseau.

Maliciel : regroupement des mots « logiciel malveillant ». Les maliciels sont conçus pour perturber les systèmes informatiques ou nuire à leur bon fonctionnement.

Authentification multifactorielle (AMF) : utilisation de deux méthodes d'authentification ou plus pour se connecter à un système. Par exemple, on vous demande de saisir un code à partir d'une application d'authentification après avoir saisi votre mot de passe pour vous connecter. L'AMF empêche les auteurs de menace d'obtenir l'accès avec un seul mot de passe.

Intrusion de réseau : contournement de la sécurité par un auteur de menace pour pénétrer dans un réseau. Une fois qu'un auteur de menace a accès à un système, il peut accéder sans autorisation aux données, aux applications et aux appareils.

Hameçonnage : forme d'escroquerie qui consiste à communiquer avec les victimes par courriel, téléphone ou message texte pour les inciter à transmettre des renseignements personnels. Les fraudes par hameçonnage visent souvent à persuader les victimes de transférer de l'argent, de divulguer des renseignements financiers ou de communiquer leurs identifiants de système, tels que leurs mots de passe.

Rançongiciel : type de logiciel malveillant conçu pour bloquer l'accès à un système informatique jusqu'à ce qu'une somme d'argent soit versée.

Correctif de sécurité : mise à jour logicielle qui permet de remédier aux vulnérabilités et aux bogues et de corriger les incohérences d'un logiciel.

Messages de masse non sollicités : communications non sollicitées envoyées en masse. Ces messages peuvent être envoyés par courriel, par téléphone, par message texte et sur les médias sociaux.

Auteur de menace : personne ou groupe qui tente d'accéder à des données qu'il n'a pas l'autorisation de consulter, ou de causer des dommages à des systèmes numériques. Ces personnes sont souvent appelées « pirates » ou « cybercriminels ».

Réseau privé virtuel (VPN) : connexion Internet chiffrée qui vise à assurer une connexion privée et sécurisée au réseau pour transférer des données en provenance et à destination d'appareils en réseau.

Pour de plus amples renseignements sur la façon de **réduire les risques liés à la cybersécurité**, consultez le site **agriculture.canada.ca/cybersecurite-entreprise-agricole**

Pour des ressources supplémentaires sur la façon de rester en sécurité en ligne, visitez **pensezcybersecurite.gc.ca**

Agriculture et Agroalimentaire Canada
Agriculture and Agri-Food Canada
Canada