# Les pirates ne volent pas que le fromage : protégez vos données !

*Article rédigé par Karine Majeau, gestionnaire du développement stratégique et des affaires*

CEPOQ
CENTRE D'EXPERTISE EN PRODUCTION OVINE DU QUÉBEC

Entre la gestion du troupeau, les registres de production, la comptabilité et la vente en ligne, nos activités sont désormais connectées. Ces outils nous aident à mieux produire, mais ils ouvrent aussi une nouvelle porte : celle du risque numérique.

On pourrait croire que tout cela concerne surtout les grandes compagnies, les banques ou les gouvernements... et bien non, ça nous concerne aussi !

Voici quelques mythes pour faire face à cette gestion de risque, car comme dans toute bonne gestion d'élevage, un peu de prévention peut nous éviter bien des pertes.

## Mythe 1

**« Je suis une petite ferme, personne ne s'intéresse à moi. »**
Au contraire, les attaques se font maintenant par des logiciels automatiques qui balayent Internet à la recherche d'appareils mal protégés. Peu importe la taille de votre entreprise, si votre routeur, votre caméra ou votre ordinateur est vulnérable, il peut devenir une porte d'entrée. Si vous avez de l'équipement sans pare-feu ni mises à jour, vous êtes une cible facile.

💡 **Conseils :** changez toujours les mots de passe d'origine et mettez vos appareils à jour régulièrement.

*En savoir plus : sécurisez vos appareils*

## Mythe 2

**« Je reconnais toujours les courriels suspects. »**
Même les plus prudents se font parfois prendre. Les courriels d'hameçonnage imitent à la perfection des fournisseurs, le MAPAQ ou même votre institution financière.

Un clic sur un lien ou une pièce jointe, et vos mots de passe peuvent être volés.

💡 **Conseils :** Avant de cliquer, vérifiez toujours l'adresse de l'expéditeur, cherchez les fautes ou incohérences, et contactez directement l'entreprise si vous avez un doute.

*En savoir plus : les 7 signaux d'alarme de l'hameçonnage*

## Mythe 3

**« Mes données sont sur mon ordinateur/tablette, elles sont donc en sécurité. »**
Les rançongiciels peuvent verrouiller tous vos fichiers en quelques minutes. Sans sauvegarde, c'est la paralysie : factures, registres de production, données de qualité... tout devient inaccessible. Même une simple tablette peut être paralysée.

💡 **Conseils :** Faites des copies de sauvegarde automatiques : sur un disque dur externe et dans un service infonuagique sécurisé (OneDrive, Google Drive, etc.).

*En savoir plus : stockage et sauvegardes*

## Mythe 4

**« Mon téléphone, c'est personnel. Personne n'ira là. »**
Les téléphones sont aujourd'hui de vrais ordinateurs : courriels, applications de gestion, photos, connexions bancaires... Une simple perte, une application non mise à jour ou une connexion Wi-Fi publique non sécurisée peut exposer vos données.

💡 **Conseils :** Activez le code d'accès et la vérification en deux étapes. Installez rapidement les mises à jour.

N'installez pas d'applications provenant de sources inconnues. Évitez de vous connecter à un réseau Wi-Fi public sans mot de passe, comme ceux des hôtels ou des restaurants.

*En savoir plus : téléphones et tablettes*

## Mythe 5

**« Le Wi-Fi de la ferme, c'est juste pour moi. »**

Les caméras, capteurs, balances électroniques ou tablettes connectées utilisent souvent le même réseau Wi-Fi que votre ordinateur personnel. Si un seul appareil est compromis, tout le réseau devient vulnérable.

💡 **Conseils :** Séparez vos réseaux : un pour les équipements agricoles, un pour la famille. Changez le mot de passe du routeur. Ne laissez pas les mots de passe par défaut (admin123, password, etc.).

*En savoir plus : sécurisez vos connexions*

## Mythe 6

**« Je ne garde pas mes données bancaires sur l'ordinateur, donc je ne risque rien. »**

Un pirate peut s'introduire dans vos fichiers clients, vos factures ou vos plateformes de commande pour détourner de l'argent ou usurper votre identité. Même sans données bancaires, une adresse courriel piratée suffit à envoyer de fausses factures à vos clients ou fournisseurs.

💡 **Conseils :** Utilisez des mots de passe uniques et complexes pour chaque service. Enregistrez-les dans un gestionnaire de mots de passe fiable (pas dans votre navigateur web !). Activez la double authentification (2FA) dès que possible.

*En savoir plus : Sécurisez vos comptes*

## Mythe 7

**« Je n'ai pas besoin d'antivirus, je fais attention. »**

Même les sites légitimes peuvent être infectés. Un antivirus à jour détecte les fichiers dangereux, les sites frauduleux et les connexions suspectes. C'est un peu comme un vaccin : ce n'est pas parfait, mais ça évite bien des problèmes.

💡 **Conseils :** Installez un antivirus et laissez-le se mettre à jour automatiquement.

## Mythe 8

**« Mes données ne valent rien pour les pirates. »**

Vos données sont plus précieuses que vous le pensez : identifiants, données de reproduction, contrôle laitier, coordonnées clients, recettes exclusives, contrats de vente, etc. Ces informations peuvent être revendues ou exploitées pour de la fraude. Et la perte de ces données peut **ralentir toutes vos activités**.

💡 **Conseils :** Sauvegardez vos registres officiels dans deux endroits différents. Vérifiez que vos fournisseurs de logiciels appliquent eux aussi des normes de sécurité.

## Mythe 9

**« Mon technicien s'en occupe, je n'ai rien à craindre. »**

Même si un fournisseur ou un conseiller configure vos systèmes, la **responsabilité finale** vous revient. Souvent, les techniciens laissent des accès temporaires, des mots de passe simples ou des paramètres par défaut.

💡 **Conseils :** Demandez un rapport de configuration après chaque intervention et changez les mots de passe dès que le technicien a terminé.

## Mythe 10

**« La cybersécurité, c'est juste de la technique. »**

La cybersécurité, c'est avant tout une culture de vigilance. Comme la biosécurité en élevage, elle repose sur des **gestes simples, constants et partagés** par toute l'équipe. Former vos employés, votre famille et même vos partenaires, c'est la meilleure façon de réduire les risques.

💡 **Conseils :** Une petite formation annuelle ou un rappel lors d'une réunion d'équipe peut faire toute la différence.

## C'est le moment de passer à l'action !

Bref, vous aurez compris que chaque appareil connecté, chaque mot de passe et chaque courriel reçu représente un risque si la sécurité n'est pas bien gérée. Protéger vos données, c'est aussi protéger votre troupeau, vos clients et la réputation de votre entreprise. **Octobre étant le mois de la sensibilisation à la cybersécurité, c'est le moment parfait pour vous inviter à passer à l'action et réviser vos pratiques pour vous éviter bien des désagréments.** Par ailleurs, prévoyez en même temps un plan d'urgence. En cas d'attaque ou de panne, un plan clair évite la panique et accélère le redémarrage !