

# Avez-vous un comportement cyberprudent ?

## 11 bonnes pratiques pour se protéger des cyberattaques

### Mots de passe

Choisissez des mots de passe uniques et robustes.

Un gestionnaire de mots de passe peut vous en suggérer et les conserver pour vous.

### Courriels

Soyez vigilant face aux courriels que vous recevez. Portez attention à l'identité de l'expéditeur et au sentiment d'urgence que la demande suscite.

### Pièces jointes

N'ouvrez pas de pièce jointe dont vous n'êtes pas sûr de la source, ni de quoi il s'agit.

### Hyperliens

Ne cliquez pas sur un hyperlien de source inconnue ou non sollicité. Sans cliquer, survolez-le de votre curseur pour voir la destination. Dans le doute, passez par votre moteur de recherche.



### Mises à jour

Effectuez les mises à jour des systèmes et logiciels que vous utilisez de manière automatique ou dès qu'elles sont disponibles.

### Sauvegardes

Sauvegardez régulièrement les documents sur lesquels vous travaillez et faites-en une copie à un autre endroit.

### Anti-virus

Protégez tous vos appareils, incluant votre téléphone intelligent, avec un anti-virus performant.

### Données personnelles

Partagez vos renseignements personnels uniquement lorsque nécessaire et avec des personnes connues.

### Réseau Wi-Fi

Utilisez un réseau sécurisé par mot de passe et préférez le VPN de l'Université Laval. Positionnez votre routeur au centre de votre logement.

### Réseaux sociaux

Réglez vos paramètres de sécurité pour limiter le partage de renseignements. Évitez de cliquer sur des liens douteux, même s'ils proviennent de connaissances.

### Signalez une fraude

Contactez votre centre de services en TI pour signaler une fraude ou un incident réel ou suspecté.

[ulaval.ca/cybersecurite](http://ulaval.ca/cybersecurite)