Afin de garantir la sécurité de votre PC, il y a plusieurs gestes préventifs à réaliser régulièrement. Que ce soit le verrouillage du PC quand vous ne l'utilisez pas, les mots de passe, les mises à jour et d'autres bons réflexes, la protection de l'ordinateur commence avec vous.

1. Verrouillage de l'ordinateur

Comme pour un smartphone, il est possible de verrouiller le PC lorsque vous ne l'utilisez pas, sans l'éteindre, pour éviter que d'autres personnes y accèdent.
Quand vous verrouillez le PC, il est mis en veille : les programmes et fichiers restent ouverts et vous pouvez reprendre là où vous en étiez.

Le verrouillage peut se faire avec un mot de passe aux différentes formes :

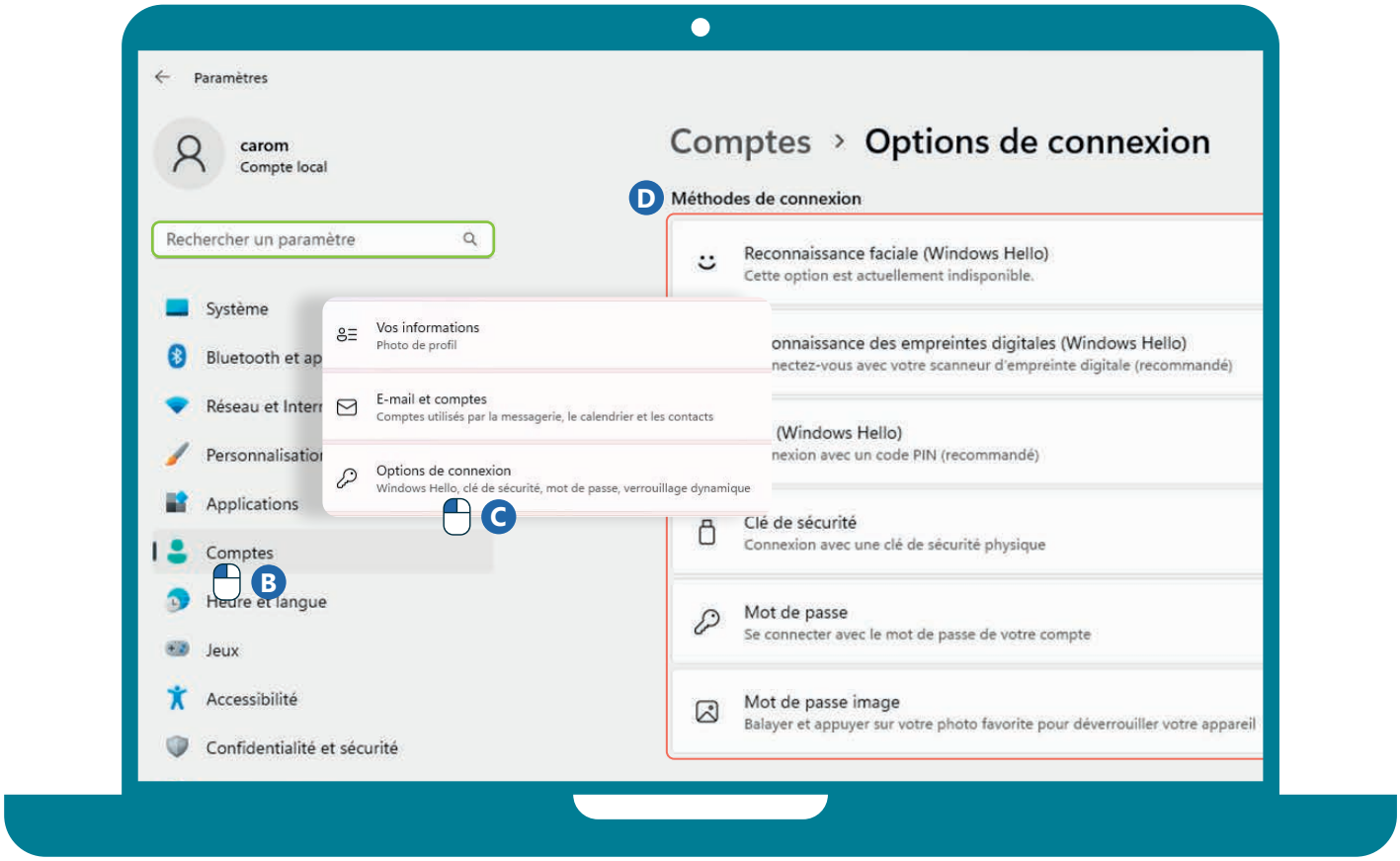
- **mot de passe**
- **code PIN**
- **reconnaissance faciale**
- **reconnaissance des empreintes**
- **image favorite**
- **clé de sécurité**

Les possibilités sont différentes selon la version de Windows installée sur la machine.
Vous pouvez aussi en configurer plusieurs, comme sur un smartphone.

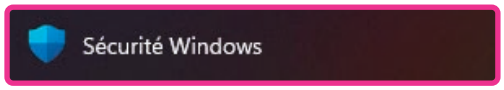
Pour changer le mot de passe, **appuyez en même temps** sur les touches **Ctrl + Alt + Suppr(Delete)** et choisissez « **Modifier un mot de passe** ».

Ctrl + Alt + Del

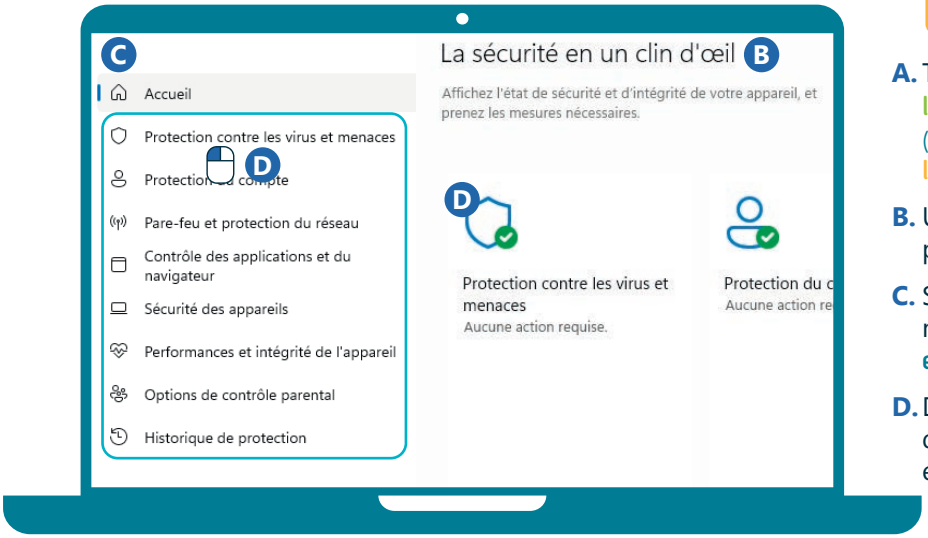
A. Allez dans les **paramètres** (voir fiche 9.3.).
B. Sélectionnez « **Comptes** ».
C. Dans ce menu, cliquez sur « **Options de connexion** ».
D. Vous pouvez désormais définir les différents modes de connexion.

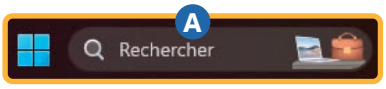


2. Entretien de base



Sur Internet, vous entendrez beaucoup parler de **virus**, **d'anti-virus**, de **protection contre les malwares**...
On peut vite s'y perdre. Mais saviez-vous que Windows a de base une protection pré-installée sur le PC ?





A. Tapez « **Sécurité Windows** » dans **la barre de recherche des paramètres** (voir recto) ou celle présente dans **la barre des tâches** (voir fiche 1.3.).

B. Un aperçu de l'état de sécurité se présente à vous.

C. Sur la gauche, **différents sous-menus**, notamment « **Protection contre les virus et menaces** ».

D. Dans ce sous-menu, apparaissent la date de la dernière analyse de sécurité et les paramètres de protection.

Vous pouvez aussi lancer des analyses :

- avec le bouton d'analyse rapide dans le menu de protection.
- via un logiciel à installer tel que **CCleaner** ou **Malwarebytes** (voir fiche 1.14.).

CCleaner et Malwarebytes sont des **freemium**, c'est-à-dire qu'ils proposent **une version de base gratuite** et des avantages payants (premium).

CCleaner

CCleaner permet de faire un nettoyage rapide du pc mais aussi de vos navigateurs, notamment l'historique de navigation et les cookies.

Malwarebytes permet de faire une analyse plus poussée pour voir s'il existe des malwares et autres logiciels malveillants.

3. Bons réflexes

Aucune protection logicielle n'étant infaillible, il est **important** en tant qu'utilisateur·trice de faire preuve de **vigilance.**

- **Vérifier la clé USB :** Ne branchez pas **n'importe quelle** clé USB donnée par **n'importe qui** sur le PC.
- **Attention aux sites visités :** Sur les sites de téléchargements illégaux (films, musique...), **le risque est grand de télécharger aussi des fichiers malveillants.**
- **Ne cliquez pas sur tous les liens dans les mails :** Assurez-vous que l'adresse du site est sécurisée et légitime. Ou rendez-vous sur le site **sans cliquer sur le lien dans l'email**.
- **Si c'est trop beau pour être vrai... :** En naviguant sur le Web, vous verrez des publicités pour des anti-virus miracles. Comme les crèmes de beauté, c'est souvent un mensonge déguisé. **Évitez de cliquer sur ces publicités et renseignez-vous sur les logiciels mentionnés avant de prendre une décision.** Une simple recherche pourra identifier si l'anti-virus miracle est un piège ou non.

interface3 namur
www.interface3namur.be/box-numerique

Projet réalisé avec le soutien du Fonds "ING Fund for a more Digital Society", géré par la Fondation Roi Baudouin