

**Discipline :** Transversal

**Classe ou niveau :** Collège-Lycée

**Domaines :** 5. Environnement numérique

**Compétences :** 5.1 Résoudre des problèmes techniques

**Niveau du cadre de référence des compétences numérique :** Niveau 2

---



## DESCRIPTION DE L'ACTIVITE

Les élèves sont face à un problème technique : leur souris ne fonctionne plus. Ils doivent trouver des solutions (raccourcis clavier) pour palier cette défaillance technique.

---



## OUTILS UTILISÉS DOMAINE(S)

Traitement de texte

---



## LES ETAPES DE L'ACTIVITE

1. Rechercher les raccourcis clavier pour :

- sélectionner une partie du texte, tout le texte
  - copier, coller, couper la sélection
  - annuler la dernière opération
  - modifier le style : gras, italique, souligné...
  - centrer, justifier un paragraphe
-

## 2. Présenter les raccourcis dans un tableau

## 3. Utiliser ces raccourcis pour modifier le texte donné en respectant les consignes suivantes :

- Le titre sera en gras et centré
- les sous-titres seront en italique gras
- les paragraphes seront justifiés
- les expressions en rouge seront soulignées
- les mots en vert seront supprimés (3 mots dans le § 1.)
- Le texte entier sera écrit dans la police Arial

---

## CONSIGNES DONNÉES AUX ÉLÈVES

Votre souris ne fonctionne plus (piles usagées, fil défectueux...)

On trouvera les différents raccourcis pour LibreOffice sur ce site :

[https://help.libreoffice.org/Writer/Shortcut\\_Keys\\_for\\_Writer/fr#Raccourcis\\_clavier\\_dans\\_LibreOffice\\_Writer](https://help.libreoffice.org/Writer/Shortcut_Keys_for_Writer/fr#Raccourcis_clavier_dans_LibreOffice_Writer)

*Rq : à moins de retirer les souris, ou de surveiller très attentivement les élèves, rien ne permet de savoir sur la production finale si les raccourcis clavier ont bien été utilisés.*

Texte à modifier

## Sécuriser son Smartphone sous Android en 8 étapes

Android représente environ 70% de part du marché des systèmes d'exploitation pour smartphone contre 15 à 20% pour iOS. C'est un OS moderne qui permet non seulement l'envoi de SMS/MMS mais aussi d'installer toutes sortes d'applications pour nous localiser, traiter des données médicales et bien d'autres.

Tout le monde peut, à l'aide d'un tutoriel, créer une application Android. Et ensuite tout le monde peut la télécharger **facilement et gratuitement**. Cette facilité de création combinée à une utilisation massive par des personnes non sensibilisées est un point d'entrée idéal pour les pirates informatiques.

Voici donc les 8 étapes pour sécuriser son mobile sous Android

### 1. Choisir un verrouillage complexe

Le verrouillage est la première barrière de sécurité contre **contre** une utilisation frauduleuse de **de** notre smartphone. Il peut s'agir d'un code de verrouillage, d'un modèle à tracer, d'une lecture d'empreintes digitales ou même d'une lecture de l'iris. Ces méthodes ont leurs avantages et leurs inconvénients. Chaque option possède également des failles, plus **plus** ou moins patchées. Lorsqu'il ne s'agit pas de failles, il s'agit d'un problème de complexité permettant de débloquent le téléphone en devinant par exemple le modèle ou le mot de passe.

L'un des problèmes typiques de sécurité informatique se pose : **Sécurité ou facilité d'utilisation ?**

Ces deux critères sont souvent opposés. Faut-il utiliser un mot de passe long et compliqué qui protège bien le smartphone en contre partie de prendre 30 secondes à débloquent le téléphone, ou un modèle simple à tracer mais facile à deviner ?

L'idéal est donc de bien doser. Concernant l'option de verrouillage à choisir, on conseille habituellement **le mot de passe ou l'empreinte**.

### 2. Installer un antivirus

Installer un antivirus pour smartphone : Pour ou contre ? Cette question est souvent au centre des débats.

Certaines choses sont à savoir concernant les antivirus pour smartphones :

- Oui ils n'arrêtent pas toutes les applications malveillantes, tout comme l'ordinateur avec les malwares.
- Oui ils demandent un peu plus de consommation RAM/Processeur sur votre smartphone, comme d'autres applications.

Un antivirus est tout de même une sécurité supplémentaire et recommandée.

À noter qu'il est inutile et contre-productif d'en installer plusieurs à la fois.

### 3. Bloquer les sources non sûres

Le vecteur d'infection numéro 1 des appareils mobiles est l'installation d'applications venant de **sources non sûres**.

Les applications Android terminent typiquement par l'extension « .apk » et rien n'empêche de partager une telle application via un site web donné hors du *Play Store*.

Le blocage est habituellement mis en place par défaut sur la plupart des appareils. Vous pouvez tout de même vérifier sur le vôtre.

Votre smartphone peut également se connecter automatiquement à un réseau Wi-Fi non sûr, mais aussi via Bluetooth ou encore NFC.

Garder ces options activées en permanence n'est pas recommandé. Vous pouvez donc les activer au besoin via les paramètres du smartphone **et non pas en permanence**.

*D'après le blog du Hacker :*

<https://www.leblogduhacker.fr/securiser-son-smartphone-android/>

**Production de l'élève :**

Production de l'élève :	
Fonction	Raccourcis clavier
sélectionner une partie de texte	Shift + flèche droite
sélectionner tout le texte	Ctrl + A
copier	Ctrl + C
coller	Ctrl + V
couper la sélection	Ctrl + X ou <u>Suppr</u>
annuler la dernière opération	Ctrl + Z
mettre en gras	Ctrl + G
mettre en italique	Ctrl + I
souligner	Ctrl + U
centrer	Ctrl + E
justifier	Ctrl + J