PROTÉGER SON SMARTPHONE

(ET SE PROTÉGER D'INTERNET)

WWW.NATHALIEVANASSCHE.BE

De plus en plus de personnes utilisent leurs smartphones pour faire du shopping, accéder à son compte bancaire ou rester connecté avec ses amis…

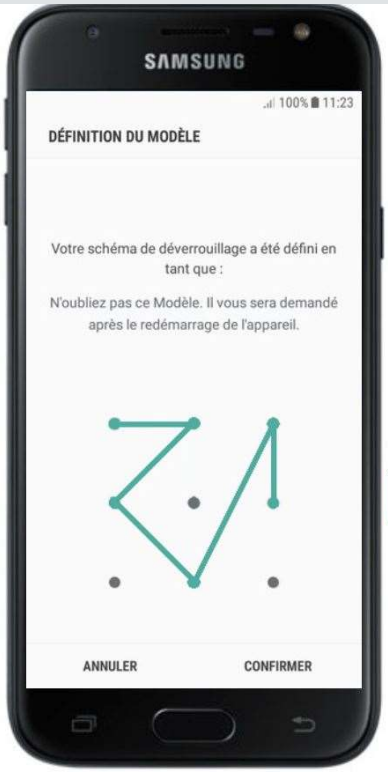
Tout comme son ordinateur, il est important de protéger son smartphone contre les pirates et les menaces en ligne !

RÈGLES À SUIVRE POUR BIEN SÉCURISER SON SMARTPHONE

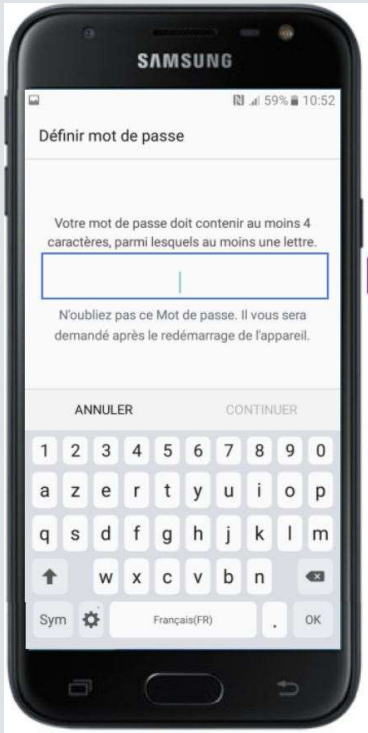
1. DÉFINIR UN MOT DE PASSE

- ✓ Définir un mot de passe fort pour votre téléphone
- ✓ Activer le verrouillage automatique de l'écran au bout de 5 minutes
  - ➢ Sont les meilleurs moyens de préserver la confidentialité de vos informations personnelles.

MODIFIER LE TYPE DE VERROUILLAGE/DÉVERROUILLAGE



◄ Sélectionnez au moins 4 points



◄ Évitez les mots de passe du type 12345 ou date de naissance

2. TÉLÉCHARGER LES MISES À JOUR DE SON TÉLÉPHONE

- ✓ Consacrez toujours du temps au téléchargement des mises à jour du logiciel.
- ✓ Souvent, elles incluent des corrections pour les failles de sécurité trouvées récemment dans le logiciel.
  - ➢ Tout comme pour un ordinateur de bureau ou portable, rester à jour est votre première ligne de défense contre les hackers et virus.

3. ÊTRE PRUDENTS EN TÉLÉCHARGEANT DES APPLICATIONS

- ✓ L'une des choses les plus amusantes à faire avec un nouveau smartphone est d'explorer toutes les formidables applications que vous pouvez télécharger.
  - ➢ En commençant à explorer, assurez-vous de télécharger responsablement.
  - ➢ Téléchargez seulement les applications à partir de sites de confiance,
  - ➢ Vérifiez l'évaluation de l'application et lisez les commentaires pour vous assurer qu'elle soit largement utilisée et respectée.

4. PRÊTER ATTENTION AUX DONNÉES PRIVÉES AUXQUELLES ACCÈDENT LES APPLICATIONS

- ✓ Les applications ont la capacité d'accéder à beaucoup d'informations à votre sujet.
- ✓ En installant l'application, prenez le temps de lire les données et informations personnelles auxquelles elle a besoin d'accéder.
  - ➢ Que ce soit un accès à votre localisation, vos informations personnelles ou vos SMS, il devrait être logique que l'application ait réellement besoin d'accéder à ces capacités pour fonctionner.

5. ATTENTION AUX LIENS DANS LES SMS

- ✓ On parle de **Smishing**, ou la combinaison des SMS et du phishing, quand un arnaqueur vous envoie un message vous redirigeant vers un site frauduleux ou vous demandant d'entrer des informations sensibles.
- ✓ Ne cliquez pas sur des liens dans les SMS ou emails si vous ne connaissez pas l'expéditeur ou s'il parait suspect. Faites confiance à votre instinct.

6. EN WI-FI PUBLIC, LIMITER L'ENVOI D'EMAILS ET LES RÉSEAUX SOCIAUX

- ✓ Les réseaux Wi-Fi publics sont devenus omniprésents, mais malheureusement la protection des sites internet auxquels vous pourrez accéder ne l'est pas.
- ✓ Beaucoup de sites web, de programmes d'email et de messagerie instantanée et les sites de réseaux sociaux ne sont pas complètement sans danger lorsque vous naviguez ou y accédez à partir d'un réseau Wi-Fi public.
- ✓ Essayez aussi de limiter votre shopping en ligne à du « lèche-vitrine » sur un réseau public.

7. NE JAMAIS ENTRER SES INFORMATIONS DE CARTE DE CRÉDIT

- ✓ Si un site vous demande d'entrer vos informations de carte de crédit, vous devriez automatiquement regardez si l'adresse web commence par « https ».
- ✓ Sur les réseaux non sécurisés, (ceux qui ont seulement http://), cela veut dire qu'un hacker pourrait facilement voler vos informations comme les identifiants, mots de passe et numéros de carte de crédit, ce qui pourrait mener au vol d'identité.

8. TRAITER SON SMARTPHONE COMME SON PC

- ✓ A mesure que les téléphones deviennent de plus en plus puissants et que les consommateurs font de plus en plus avec, ils deviennent des cibles plus intéressantes pour les attaques malveillantes.
  - ➢ Protégez-vous ainsi que vos données personnelles contre les logiciels malveillants, logiciels espions et applications malveillantes en téléchargeant une application de sécurité

9. TÉLÉCHARGER UNE APPLICATION « LOCALISER MON TÉLÉPHONE »

- ✓ Google (avec un compte Android) permet de localiser votre téléphone, verrouiller votre appareil, et effacer ses données.
  - ➢ https://support.google.com/accounts/answer/6160491?hl=fr

OU

- ✓ Téléchargez une application qui aide à localiser votre téléphone en cas de perte ou de vol. Assurez-vous de pouvoir verrouillez votre téléphone à distance s'il est volé ou perdu.

10. ACTIVER LA FONCTION « EFFACER » SUR VOTRE TÉLÉPHONE

- ✓ Si vous (ou votre téléphone) vous retrouvez dans une situation difficile, et vous ne pourrez pas récupérer votre téléphone, téléchargez une application pour effacer les données de votre téléphone pour ne pas que vos informations personnelles tombent entre de mauvaises mains.
- ✓ Si vous le pouvez, essayez de télécharger une application qui peut également effacer votre carte SD.

J'AI PERDU MON SMARTPHONE/MA TABLETTE, QUE FAIRE ?

Que pouvez-vous faire ?

1. Changez immédiatement tous les mots de passe des comptes qui étaient installés sur votre appareil (e-mail, Facebook, etc.) et choisissez un nouveau mot de passe unique par compte.
2. Si vos coordonnées bancaires ou vos données de paiement se trouvaient sur votre appareil, avertissez votre banque et surveillez bien vos comptes. Faites éventuellement bloquer vos cartes de banque et vos comptes.
3. En cas de vol de données professionnelles, prévenez au plus vite votre employeur.
4. En cas de vol, faites une déclaration à la police.