
## ATTENTION AUX SMARTPHONES ANDROID : COMMENT SE PROTÉGER DU MALWARE[1] DROIDBOT ?

Un nouveau logiciel malveillant cible les applications bancaires sur les smartphones Android. Pour vous protéger, nous vous recommandons de suivre quelques gestes simples.

### COMMENT FONCTIONNE LE MALWARE DROIDBOT ?

Le malware DroidBot se fait passer pour une application légitime (navigateur web, application de sécurité, jeu...). Une fois téléchargé et après vous avoir demandé la **permission d'accéder aux services d'accessibilité de votre appareil**, le malware peut ensuite collecter vos informations confidentielles (y compris vos identifiants bancaires).

### COMMENT SE PROTÉGER DU MALWARE DROIDBOT ?

Pour vous protéger, il est recommandé de suivre ces quelques gestes simples lorsque vous téléchargez une application :

- **Téléchargez uniquement des applications depuis le Google Play Store.**
- **Examinez attentivement les demandes d'autorisation lors de l'installation d'une application** (par exemple, a-t-elle vraiment besoin d'accéder à vos droits d'administration, de lire vos sms ou de prendre une copie d'écran ?).
- Portez une attention particulière aux applications demandant l'accès aux services d'accessibilité et ne l'activez que si nécessaire.

Enfin, nous vous recommandons également d'**effectuer régulièrement les mises à jour** de sécurité de votre appareil et de votre application bancaire.

### LES BONNES PRATIQUES POUR SÉCURISER VOTRE SMARTPHONE

Découvrez **10 bonnes pratiques** à adopter pour la sécurité de votre appareil mobile.