

Se former au numérique

Sécurité sur Internet, smartphone et ordinateur

Des repères simples pour utiliser le numérique avec confiance

- Sécurité sur Internet
- Utiliser mon smartphone
- Utiliser mon ordinateur

Le numérique, un atout pour avancer sereinement !

www.nathalievanassche.be

UAW

Le Brabant wallon

Table des matières

La sécurité sur Internet 4
Les bons réflexes sur PC et smartphone 4
Avant de cliquer, je prends 5 secondes 5
Le phishing par e-mail 5
Les indices qui doivent m'alerter 6
Les appels frauduleux 6
Un numéro affiché à l'écran peut être trompeur 6
Et l'appel en absence ? 6
SMS, colis et QR codes 7
Le QR code : pratique, mais pas forcément sûr 7
Un SMS peut aussi être normal 7
Fausse facture et faux proche 8
Le faux support informatique 8
Ce que je fais 9
Le rançongiciel : reconnaître l'alerte 9
Les premiers réflexes 9
Signaux possibles d'un problème sérieux 10
J'ai mordu à l'escroquerie : que faire ? 10
Le mémo à garder près de l'ordinateur 10
Les mots de passe : la clé de vos comptes 11
Pourquoi les mots de passe simples sont-ils dangereux ? 11
Créer une phrase de passe 11
Retenir ses mots de passe sans les simplifier 12
Les habitudes à éviter 12
La double authentification (2FA) 12
Comment cela fonctionne ? 13
Le réflexe essentiel avec la 2FA 13
Quels comptes protéger en priorité ? 13

Mon smartphone Android 15
Les commandes essentielles : se repérer et comprendre ce que l'on voit 15
Se déplacer dans le smartphone 18
Retour, accueil, applications récentes et recherche d'une application 18
Notifications et réglages rapides 19
Accéder rapidement aux informations et aux commandes courantes 19
Les paramètres 21
Protéger l'accès au smartphone 22
Un bon verrouillage empêche une autre personne d'ouvrir facilement votre téléphone 22
Bien régler son écran verrouillé 22
Le téléphone doit se verrouiller seul et ne pas afficher trop d'informations sensibles 22
Code du téléphone et code PIN de la SIM 23
Deux protections différentes à ne pas confondre 23
Vérifier que le téléphone peut être retrouvé 24

Mon téléphone a disparu : que faire ? Localiser, faire sonner, sécuriser… puis effacer seulement en dernier recours ... 24
Sauvegarder mes données ... 25
Comprendre les connexions ... 25
Se connecter et se déconnecter ... 25
Partager sa connexion ... 26
Partager une photo depuis son smartphone ... 27

Mon ordinateur : fichiers, photos et sauvegardes ... 29
Se repérer sur l'écran ... 29
La souris : les actions de base ... 30
Les fenêtres : ouvrir, réduire, agrandir, fermer ... 30
Le clavier : quelques touches très utiles ... 31
Comprendre les fichiers et les dossiers ... 32
Fichier ou dossier : quelle différence ? ... 32
L'explorateur de fichiers ... 33
Actions de base sur un fichier ... 33
Sauvegarder sur un disque dur amovible ... 35
Quels dossiers sauvegarder ? ... 35
Les étapes d'une sauvegarde ... 35
Internet et navigateur ... 36
Comprendre le navigateur ... 36
La barre d'adresse : mon repère principal ... 36
Les commandes les plus utiles ... 37
Les onglets : garder plusieurs pages ouvertes ... 37
Retrouver facilement ce que j'ai consulté ... 37
Internet, comptes et démarches en ligne ... 38
Se connecter et se déconnecter ... 38
Reconnaître un site officiel belge ... 39
S'identifier sur les services publics avec CSAM ... 39
La carte d'identité électronique eID ... 40
Itsme et MyGov ... 40
Remplir un formulaire en ligne ... 41
Cases à cocher, newsletters et conditions générales ... 41

La sécurité sur Internet

Les bons réflexes sur PC et smartphone



Objectif de ce support

Retrouver facilement les réflexes vus pendant le Wooclap : reconnaître une situation suspecte, éviter de se faire piéger et savoir quoi faire si l'on a déjà cliqué, payé ou laissé quelqu'un accéder à son ordinateur.

À la fin de cette partie, je dois savoir :

- repérer les signaux qui doivent me rendre méfiant ;
- réagir face à un mail, un SMS, un QR code ou un appel inattendu ;
- vérifier une demande inhabituelle par un autre moyen ;
- agir rapidement si je pense avoir été victime d'une escroquerie.

Avant de cliquer, je prends 5 secondes

La plupart des arnaques cherchent d'abord à nous faire agir trop vite.

1. Je ralentis

Les mots « urgent », « dernier rappel », « compte bloqué » ou « aujourd'hui uniquement » doivent m'inciter à prendre du recul.

2. Je me demande si j'attendais ce message

Une facture, un colis, une aide ou un appel bancaire inattendu mérite une vérification.

3. Je vérifie par un autre chemin

Je vais moi-même vers le site, l'application ou le numéro que je connais déjà.

4. Argent ou données sensibles ?

Je redouble de prudence dès qu'on me demande de payer, de fournir des coordonnées bancaires ou de valider une opération.

5. Demande inhabituelle ?

Nouveau compte bancaire, changement de numéro, paiement urgent : je vérifie auprès de la personne concernée.

6. Un beau logo ne prouve rien

Un message peut être très bien écrit et parfaitement imiter une entreprise ou une administration.

7. En cas de doute, je demande

Mieux vaut perdre deux minutes pour vérifier que perdre de l'argent ou l'accès à ses données.

RÉFLEXE : urgence = je ralentis

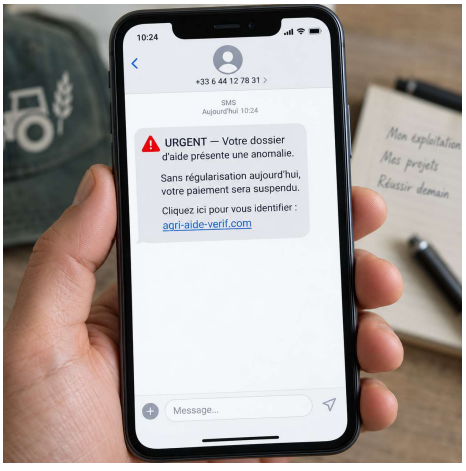
Un pirate essaie souvent de provoquer une émotion : peur, urgence, curiosité ou envie de profiter d'une bonne affaire. Le premier geste de sécurité est donc souvent très simple : ne rien faire dans la précipitation.

Le phishing par e-mail

Un faux message qui cherche à obtenir une action, des données ou un paiement.

Comment fonctionne le piège ?

- Le message semble venir d'une banque, d'un fournisseur, d'un magasin, d'une administration ou d'un proche.
- Il utilise une menace ou une récompense pour vous pousser à agir rapidement.
- Il contient souvent un lien, un formulaire ou une pièce jointe.
- Le but est de récupérer des informations, de vous faire payer ou de vous faire installer quelque chose.



Exemple : un message urgent concernant une aide agricole.

Les indices qui doivent m'alerter

- **Le message est inattendu.** Je ne suis pas en train de faire l'opération dont il parle.
- **Il crée de l'urgence.** On menace de bloquer un compte, de suspendre un paiement ou de réclamer des frais immédiatement.
- **On me demande une action inhabituelle.** Cliquer, payer, ouvrir une pièce jointe ou transmettre des données.
- **L'adresse de l'expéditeur paraît étrange.** C'est un indice à vérifier, mais ce n'est jamais une preuve suffisante à lui seul.
- **Le message semble pourtant parfait.** Ce n'est pas rassurant : les faux messages peuvent aujourd'hui être très bien rédigés et très bien présentés.

La bonne réaction

Je ne réponds pas au message pour vérifier. Je retrouve moi-même le site, l'application ou les coordonnées habituelles de l'organisme et je vérifie par ce chemin.

Les appels frauduleux

La personne au téléphone peut connaître votre nom, votre banque ou d'autres informations sur vous.

L'escroc se fait passer pour une personne de confiance : banque, Card Stop, Itsme, police, service public, entreprise ou technicien. Son objectif est de vous faire communiquer des informations, valider une opération ou effectuer vous-même un transfert.

Je refuse immédiatement si on me demande…

- de transférer mon argent vers un prétendu « compte sécurisé » ;
- de valider une opération que je n'ai pas moi-même commencée ;
- d'installer un logiciel de prise en main à distance ;
- de remettre ma carte bancaire ou un appareil à une personne qui vient à mon domicile ;
- de communiquer des coordonnées bancaires ou des codes reçus sur mon téléphone.

Je raccroche et je rappelle moi-même avec un numéro officiel que je connais.

Un numéro affiché à l'écran peut être trompeur

Le numéro présenté sur votre téléphone ne suffit pas à prouver l'identité de l'appelant. Le bon réflexe est de mettre fin à l'appel et de reprendre vous-même contact avec l'organisme concerné.

Et l'appel en absence ?

Le Wangiri

Certains fraudeurs laissent volontairement un appel en absence très bref pour vous pousser à rappeler un numéro fortement surtaxé, parfois avec un indicatif international inhabituel.

- Je ne rappelle pas précipitamment un numéro inconnu.
- Un correspondant légitime peut laisser un message ou rappeler.
- Si les appels se répètent, je peux en informer mon opérateur.

SMS, colis et QR codes

Un SMS ou un QR code peut cacher exactement le même type de piège qu'un e-mail.

Exemple : le faux problème de livraison

Situation

Vous attendez justement une pièce pour votre tracteur. Un SMS annonce : « Votre colis ne peut être livré. Payez 1,89 € pour reprogrammer la livraison. »

1. **Je ne clique pas automatiquement.** Le fait que j'attende réellement un colis ne prouve pas que le message est vrai.
2. **Je vérifie par moi-même.** J'utilise le site ou l'application du transporteur que je connais déjà, avec mon numéro de suivi.
3. **Je me méfie d'un petit paiement.** Une somme faible peut simplement servir à me faire introduire mes coordonnées bancaires.

Le QR code : pratique, mais pas forcément sûr

Un QR code peut masquer la destination réelle d'un lien. Lorsqu'un fraudeur utilise un QR code pour mener vers une page de phishing, on parle parfois de « quishing ».

- Je traite un QR code reçu par message avec la même prudence qu'un lien.
- Je vérifie qui me l'a envoyé et pourquoi.
- Avant d'ouvrir la page, je regarde l'adresse proposée si mon téléphone l'affiche.
- Je suis particulièrement prudent avec les QR codes ajoutés sur des affiches, cartes ou supports publics.

Un SMS peut aussi être normal

Un message d'information est moins suspect lorsqu'il correspond à une action que vous venez réellement d'effectuer et qu'il ne vous demande ni paiement, ni clic urgent, ni information sensible. Un message inattendu qui exige une action immédiate mérite au contraire une vérification.

Lien ou QR code : même prudence.

Fausse facture et faux proche

Le message peut provenir d'un nom que vous connaissez et sembler parfaitement crédible.





Cas 1 - « Nous avons changé de compte bancaire »

Un fournisseur habituel envoie une facture correcte, avec son logo, mais demande d'utiliser un nouvel IBAN. Je ne paie pas sur cette seule base et je ne me contente pas de répondre au mail.

Réflexe fournisseur

Je téléphone avec le numéro que j'utilise habituellement ou que je retrouve moi-même. Un changement de compte bancaire doit être vérifié par un autre canal.

Cas 2 - « J'ai changé de numéro, peux-tu payer pour moi ? »

Un employé, un proche ou un membre de la famille peut être imité. Le fait que le message connaisse votre prénom, contienne une photo ou même une note vocale ressemblante ne suffit pas à prouver l'identité de la personne.

Réflexe proche

Je contacte la personne avec un numéro ou un moyen de contact que j'utilisais déjà auparavant. Demande inhabituelle = vérification indépendante.

Le faux support informatique

Un grand écran alarmant ne signifie pas forcément que Microsoft, votre antivirus ou un technicien vous contacte réellement.

Situation typique

Un écran bleu ou une fenêtre annonce que l'ordinateur est infecté et affiche un numéro de téléphone à appeler immédiatement.

Ce que je fais

1. **Je ne clique sur rien.** Je ne téléphone pas au numéro affiché.
2. **Je ferme ou redémarre l'ordinateur.** Si l'écran bloque tout, je peux éteindre puis rallumer la machine.
3. **Je demande de l'aide si le problème revient.** Certaines situations nécessitent l'intervention d'une personne de confiance ou d'un professionnel.

Si quelqu'un me demande d'installer AnyDesk, TeamViewer ou un autre outil similaire

Ces logiciels peuvent être utilisés légitimement par un technicien, mais ils permettent aussi à une autre personne de voir ou de contrôler votre ordinateur. Je ne les installe pas à la demande d'un inconnu qui me contacte ou d'un numéro trouvé dans une alerte.

Si je l'ai déjà installé et que la personne a pris la main

- **Je coupe Internet.** Je désactive le Wi-Fi ou je débranche le câble réseau.
- **Je mets fin à l'accès.** Je ferme puis désinstalle le programme de prise en main à distance.
- **Je fais vérifier l'ordinateur.** Je demande de l'aide si je ne suis pas certain de ce qui a été fait.
- **Si des opérations bancaires ont été réalisées,** je contacte immédiatement ma banque depuis ses coordonnées officielles.

Une alerte qui affiche un numéro à appeler n'est pas une preuve de légitimité.

Le rançongiciel : reconnaître l'alerte

Parfois, l'attaque ne cherche pas à vous faire payer une fausse facture : elle bloque directement vos fichiers.

Situation

Vous ouvrez votre ordinateur : vos documents ont changé de nom ou ne s'ouvrent plus. Un message réclame une somme d'argent pour les récupérer.

Que s'est-il probablement passé ?

Il peut s'agir d'un rançongiciel (ransomware) : un programme malveillant chiffre ou bloque des fichiers et réclame ensuite une rançon.

Les premiers réflexes

1. **Je déconnecte l'ordinateur du réseau.** Je coupe le Wi-Fi ou le câble réseau afin de limiter la propagation possible.
2. **Je n'essaie pas tout au hasard.** Je ne multiplie pas les manipulations et je ne branche pas d'autres supports de stockage sur la machine infectée.
3. **Je demande rapidement de l'aide.** Je contacte une personne compétente pour évaluer la situation et les possibilités de récupération.
4. **Je garde les informations utiles.** Je peux photographier le message affiché et noter ce qui s'est passé juste avant l'incident.

À retenir

Le but de cette séance n'est pas d'apprendre à réparer un ordinateur infecté, mais de reconnaître la situation et d'éviter d'aggraver le problème.

Signaux possibles d’un problème sérieux

- documents soudainement illisibles ou renommés ;
- message demandant une somme d’argent pour récupérer les fichiers ;
- comportement inhabituel de plusieurs fichiers ou dossiers en même temps ;
- apparition d’une consigne de paiement ou d’un compte à rebours.

J’ai mordu à l’escroquerie : que faire ?

Agir vite, mais sans multiplier les gestes inutiles.

J’ai installé un logiciel de contrôle à distance

Je coupe immédiatement Internet. Je mets fin à l’accès, je désinstalle le programme et je fais vérifier l’ordinateur si nécessaire.

J’ai donné mes informations bancaires

Je contacte immédiatement ma banque avec ses coordonnées officielles, je fais opposition à la carte si nécessaire et je vérifie les opérations.

J’ai validé une opération bancaire ou Itsme

Je contacte immédiatement ma banque, j’explique exactement ce que j’ai validé et je vérifie les paiements et virements récents.

J’ai seulement cliqué sur un lien

Je ferme la page. Je ne télécharge rien. Si un fichier s’est téléchargé, je ne l’ouvre pas. Je surveille ensuite tout comportement inhabituel.

Je ne sais pas exactement ce que j’ai fait

Je demande rapidement de l’aide et j’évite d’utiliser l’appareil pour des opérations bancaires tant que la situation n’est pas clarifiée.

Quelqu’un a déjà pris de l’argent

Je contacte sans attendre la banque ou le service concerné et je conserve les éléments utiles : message, numéro, facture, capture d’écran, heure de l’appel.

Le réflexe : couper l’accès, prévenir le bon service, demander de l’aide.

Ne continuez pas à échanger avec l’escroc pour « arranger » la situation. Reprenez toujours contact avec la banque, l’entreprise ou le service concerné à partir de coordonnées que vous recherchez ou connaissez vous-même.

Le mémo à garder près de l’ordinateur

Huit règles simples suffisent à éviter une grande partie des pièges vus pendant la séance.

1. **Urgence = je ralentis.** Je ne prends pas une décision importante sous pression.
2. **Message inattendu = je vérifie.** Je me demande toujours si j’attendais vraiment ce contact.
3. **Je passe par un autre chemin.** Je retrouve moi-même le site, l’application ou le numéro habituel.
4. **Je ne donne pas d’informations sensibles à quelqu’un qui me contacte.** Banque, carte, identité ou validation : je garde le contrôle de l’opération.
5. **Nouveau compte bancaire ou demande de paiement inhabituelle = appel de vérification.** Je contacte la personne avec des coordonnées déjà connues.
6. **Lien, pièce jointe ou QR code inattendu = prudence.** Je n’ouvre pas simplement pour « voir ce que c’est ».
7. **Un nom, un logo, une photo ou une voix ne suffisent pas.** Une arnaque peut être très bien présentée.
8. **Si j’ai un doute, je demande de l’aide avant d’agir.** Deux minutes de vérification peuvent éviter beaucoup de problèmes.

Mon test en 3 questions

1. Est-ce que j'attendais ce message ou cet appel ?
2. Est-ce qu'on me pousse à agir vite, à payer ou à transmettre quelque chose ?
3. Puis-je vérifier la demande autrement, sans utiliser le lien, le numéro ou le QR code reçu ?

JE RALENTIS • JE VÉRIFIE • JE DEMANDE SI J'AI UN DOUTE

Ces réflexes valent aussi bien sur ordinateur que sur smartphone. Le support ne remplace pas l'aide d'un professionnel ou de votre banque lorsqu'une fraude est déjà en cours.

Les mots de passe : la clé de vos comptes

Un bon mot de passe doit surtout être long, unique et difficile à deviner.

La règle la plus importante

Un compte important = un mot de passe différent. Si le même mot de passe est utilisé partout et qu'il est volé sur un seul site, les fraudeurs peuvent essayer de l'utiliser sur votre messagerie, vos achats, vos réseaux sociaux ou d'autres services.

Pourquoi les mots de passe simples sont-ils dangereux ?

Les pirates peuvent tester automatiquement un très grand nombre de mots de passe. Cette technique est souvent appelée « force brute ». Ils essaient aussi en priorité les mots de passe très courants, les suites simples et les informations faciles à deviner.

À éviter

123456, azerty, password, prénom + année de naissance, nom de la ferme, numéro de téléphone…

À rechercher

Un mot de passe long, sans lien évident avec votre vie personnelle et différent pour chaque compte.

Plus long = plus solide

Pour un mot de passe que vous devez mémoriser, visez au moins 15 caractères.

Une phrase de passe

Plusieurs mots sans rapport entre eux peuvent être plus faciles à mémoriser tout en donnant un mot de passe très long.

Créer une phrase de passe

Choisissez au moins quatre mots qui n'ont pas de lien évident entre eux. Vous pouvez ajouter un chiffre ou un signe si le site le demande. Exemple pédagogique : Tulipe-Boussole7-Café-Nuage.

À RETENIR : LONG + UNIQUE + IMPOSSIBLE À DEVINER

Retenir ses mots de passe sans les simplifier

Le problème n'est pas de créer un seul bon mot de passe : c'est d'en gérer plusieurs.

Deux méthodes utiles

1. La phrase de passe

Pour les quelques mots de passe que vous devez réellement mémoriser, une phrase de passe longue est souvent plus facile à retenir qu'une suite de caractères au hasard.

2. Le gestionnaire de mots de passe

Il conserve vos identifiants et mots de passe dans un coffre-fort protégé. Il peut aussi générer des mots de passe longs et différents pour chaque site.

Important

Le gestionnaire de mots de passe ne signifie pas « utiliser le même mot de passe partout ». Au contraire : il permet d'avoir un mot de passe différent pour chaque compte sans devoir tous les mémoriser.

Les habitudes à éviter

- **Ne réutilisez pas** le même mot de passe sur plusieurs comptes.
- **N'utilisez pas une base identique** en changeant seulement deux lettres selon le site : si la logique est découverte, les autres mots de passe deviennent faciles à deviner.
- **Ne laissez pas vos mots de passe visibles** sur un post-it collé à l'écran ou dans un fichier intitulé « mots de passe » sur le bureau.
- **Ne communiquez jamais votre mot de passe** à une personne qui vous appelle, vous écrit ou vous demande de « vérifier votre compte ».

Si je pense qu'un mot de passe a été volé

1

Je le change

Je modifie immédiatement le mot de passe du compte concerné.

2

Je vérifie

Je regarde si le même mot de passe a été utilisé ailleurs.

3

Je sécurise

Je change aussi les comptes concernés et j'active la 2FA quand elle existe.

UN COMPTE IMPORTANT = UN MOT DE PASSE DIFFÉRENT

La double authentification (2FA)

Une deuxième protection lorsque le mot de passe ne suffit plus.

Pourquoi ajouter une deuxième étape ?

Même un excellent mot de passe peut être volé lors d'un phishing ou d'une fuite de données. Avec la double authentification, le mot de passe seul ne suffit plus pour entrer dans le compte.

Comment cela fonctionne ?

Pour prouver votre identité, un service peut combiner au moins deux éléments différents :

1	2	3
Ce que je sais	**Ce que je possède**	**Ce que je suis**
Un mot de passe ou un code PIN.	Mon téléphone, une application d'authentification ou une clé de sécurité.	Une empreinte digitale ou la reconnaissance du visage.

Exemple : je saisis mon mot de passe, puis je confirme la connexion sur mon smartphone. Un pirate qui possède seulement mon mot de passe reste bloqué.

Le réflexe essentiel avec la 2FA

Je n'ai rien demandé ? Je refuse.

Si vous recevez soudainement un code ou une demande de validation alors que vous n'êtes pas en train de vous connecter, ne validez pas. Ne communiquez jamais un code de vérification reçu par SMS ou dans une application à une personne qui vous le demande.

Quels comptes protéger en priorité ?

- **Votre boîte mail :** elle permet souvent de réinitialiser l'accès à vos autres comptes.
- **Vos services bancaires et administratifs :** ils donnent accès à des données et opérations sensibles.
- **Vos comptes importants :** réseaux sociaux, achats, stockage en ligne, outils professionnels...

MOT DE PASSE LONG ET UNIQUE + 2FA = DEUX BARRIÈRES



Objectif de ce support

Apprendre à utiliser son smartphone Android de manière plus autonome et plus sûre dans les situations du quotidien : se repérer dans l'appareil, le protéger, le retrouver en cas de perte et comprendre ses différentes connexions.

À la fin de cette partie, je dois savoir :

- me repérer sur l'écran d'accueil et retrouver une application ;
- utiliser les commandes essentielles de mon smartphone ;
- comprendre les notifications et les réglages rapides ;
- protéger l'accès à mon téléphone avec un verrouillage adapté ;
- distinguer le code de verrouillage du téléphone du code PIN de la carte SIM ;
- activer et utiliser la fonction permettant de retrouver mon téléphone ;
- comprendre la différence entre Wi-Fi, données mobiles, Bluetooth et mode avion ;
- connecter et déconnecter mon smartphone d'un réseau ;
- partager la connexion Internet de mon smartphone avec un autre appareil ;
- adopter quelques bons réflexes pour utiliser mon smartphone plus sereinement.

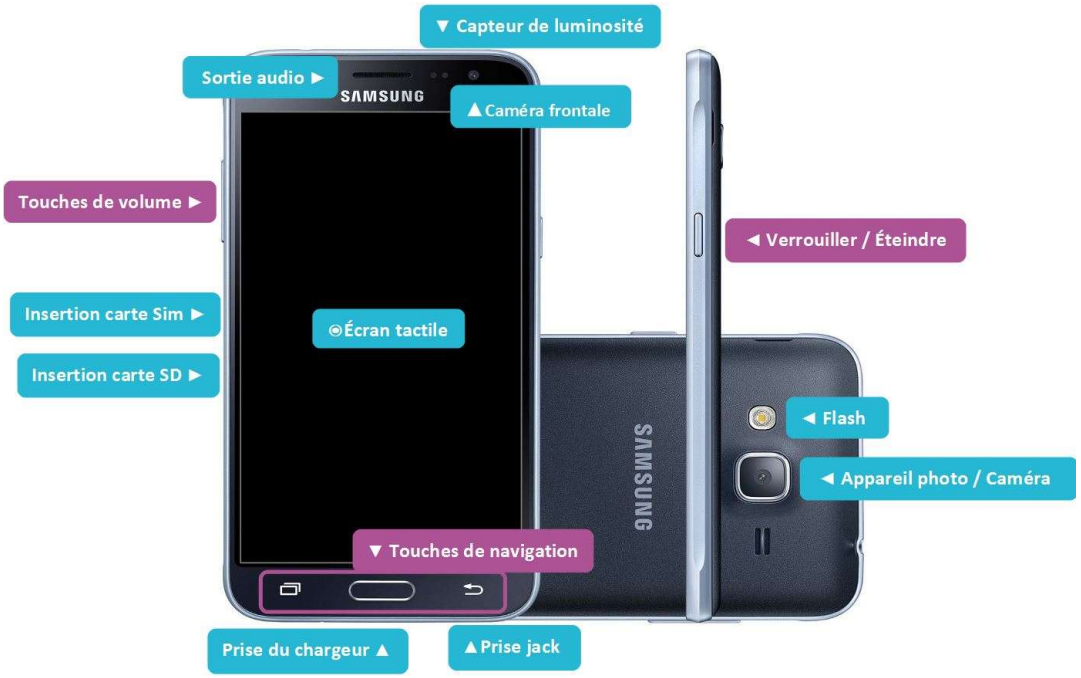
Mon smartphone Android

Les commandes essentielles : se repérer et comprendre ce que l'on voit

Important : tous les téléphones Android ne se présentent pas exactement de la même façon.

Samsung, Xiaomi, Motorola, Oppo, Google Pixel… les noms et les icônes peuvent varier. Les gestes et les principes présentés ici restent cependant très proches d'un appareil à l'autre.

Nous allons commencer par repérer les éléments externes de votre smartphone :



Lexique

La **carte SIM** est une petite carte à puce qui se place dans votre téléphone portable. Elle est unique, et c'est elle qui vous identifie en tant que numéro de téléphone. C'est votre opérateur téléphonique qui vous la fournit à la souscription d'un forfait mobile.

La **carte SD** est une mémoire supplémentaire à celle, interne, de votre smartphone. Elle permet de stocker davantage de données (photos, musiques, vidéos) et de ne pas saturer la mémoire de votre mobile.

La **prise jack**, comme sur une chaîne stéréo, votre smartphone dispose d'une prise jack vous permettant d'y brancher un casque ou des écouteurs.

Manipulations de base

ALLUMER – ETEINDRE – METTRE EN VEILLE UN SMARTPHONE / UNE TABLETTE

Le bouton de verrouillage est un bouton multi-usage.

- Une pression légère sort votre smartphone de sa veille. Il s'allume et vous indique l'écran de verrouillage. Une seconde pression le remet en veille.
- Une longue pression vous affiche plusieurs commandes. Vous pouvez ainsi choisir d'éteindre ou de redémarrer votre appareil, de faire une capture photo ou vidéo de votre écran.

- Une pression encore plus longue éteint complètement votre smartphone. Cette même pression vous permet de le rallumer lorsqu'il est éteint.

METTRE EN VEILLE

Lorsque votre appareil est éveillé, il suffit d'appuyer une fois sur le bouton d'allumage pour qu'il se mette en veille. L'écran devient noir mais le smartphone est encore allumé. Le mode veille permet d'économiser la batterie.

Rappuyer sur le bouton d'allumage sort votre mobile de sa veille mais vous dirige sur l'écran de verrouillage. Vous devez entrer votre code ou schéma pour accéder à la page d'accueil[1].

ÉTEINDRE/REDÉMARRER

Une pression de 3 à 5 secondes vous ouvre le menu de démarrage vous permettant d'éteindre ou redémarrer le mobile.

Une pression plus longue éteint complètement l'appareil.

L'écran d'accueil : point de départ

L'ÉCRAN D'ACCUEIL VERROUILLÉ

Quand vous appuyez légèrement sur votre bouton d'accueil, sans déverrouiller votre appareil, vous arrivez sur votre écran d'accueil, ce dernier comprend plusieurs informations : l'heure, la date, le pourcentage de batterie restant, l'indicateur de réseau disponible (3G, 4G, ou Wi-Fi) et pour les appareils disposants d'une carte SIM, votre réseau téléphonique…



Après le déverrouillage, le smartphone affiche généralement l'écran d'accueil. C'est l'endroit où l'on retrouve les applications les plus utilisées, l'heure, parfois la météo et différents raccourcis.

[1] Les différentes façons de sécuriser votre smartphone seront traitées plus tard.



Icônes d'applications

Une icône permet d'ouvrir une application : Téléphone, Messages, Appareil photo, Chrome, WhatsApp… Un simple appui suffit.

Barre d'état

Tout en haut : heure, niveau de batterie, réseau mobile, Wi-Fi et parfois d'autres petits symboles. Ils donnent des informations sur l'état du téléphone.

Écrans d'accueil

Il peut y avoir plusieurs pages. Faites glisser le doigt vers la gauche ou vers la droite pour passer de l'une à l'autre.

Zone des favoris

En bas de l'écran, certaines applications restent souvent visibles sur toutes les pages : téléphone, messages, appareil photo, navigateur…

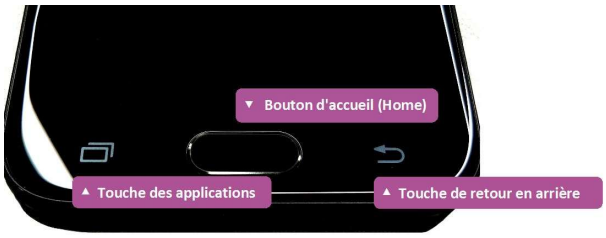


Se déplacer dans le smartphone

Retour, accueil, applications récentes et recherche d'une application

Navigation avec 3 boutons

Vous trouverez généralement trois commandes : Retour, Accueil et Applications récentes. L'ordre peut changer selon la marque du téléphone.

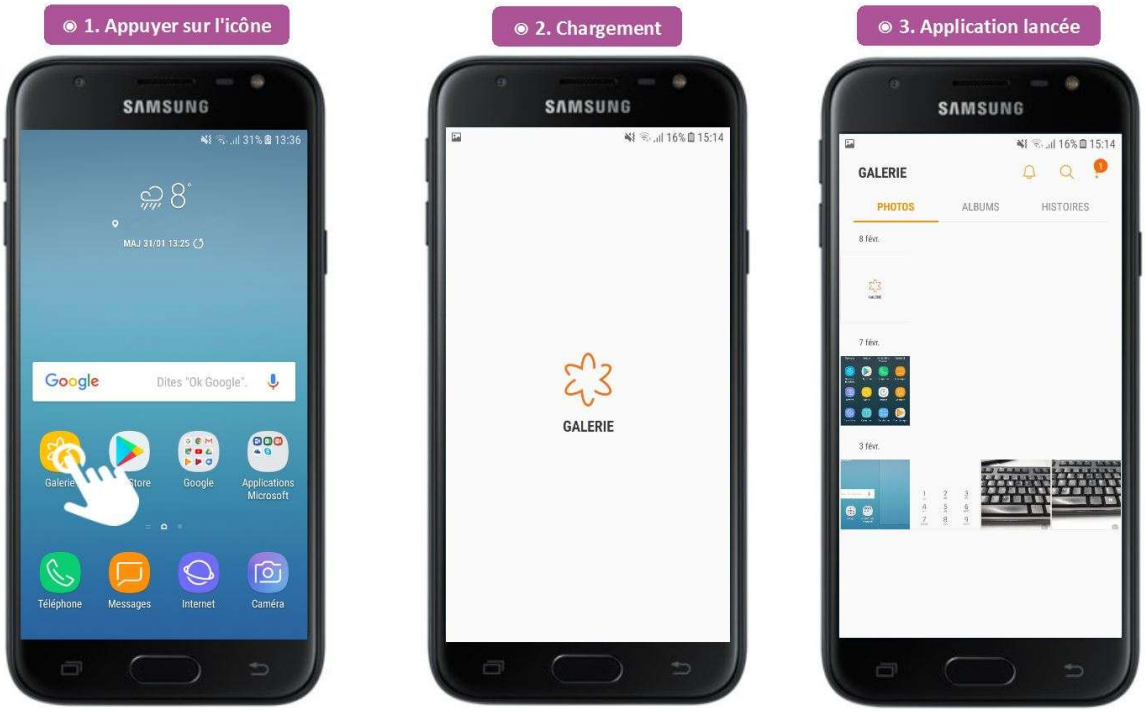


Le bon réflexe

Si vous êtes perdu dans une application, revenez à l'écran d'accueil. Vous ne cassez rien en revenant en arrière ou à l'accueil.

Ouvrir, quitter ou changer d'application

- Pour ouvrir une application : touchez simplement son icône.



- Pour revenir à l'accueil : utilisez le geste ou le bouton Accueil.
- Revenir à l'accueil ne ferme pas forcément l'application : elle peut rester ouverte en arrière-plan.
- Pour retrouver une application utilisée récemment : ouvrez l'écran des applications récentes, puis choisissez celle qui vous intéresse.
- Il n'est pas nécessaire de fermer toutes les applications après chaque utilisation. Android gère automatiquement la mémoire dans la plupart des cas.

Je ne retrouve plus une application

Selon le téléphone, faites glisser le doigt vers le haut depuis l'écran d'accueil pour afficher toutes les applications. Vous pouvez aussi utiliser la zone de recherche et taper quelques lettres du nom de l'application.

À faire sur votre smartphone

- Ouvrez l'application Appareil photo.
- Revenez à l'écran d'accueil.
- Affichez les applications récentes et retournez dans l'appareil photo.
- Retrouvez une application que vous utilisez peu en passant par la liste de toutes les applications ou la recherche.

Notifications et réglages rapides

Accéder rapidement aux informations et aux commandes courantes

Les notifications : ce que le téléphone veut me signaler



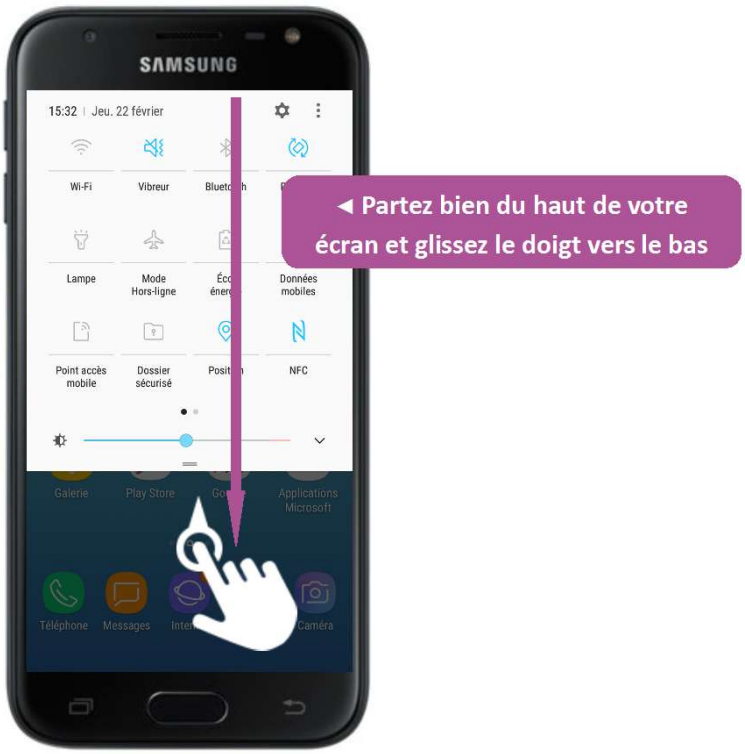
◀ Les notifications apparaissent au milieu de l'écran

Un message reçu, un appel manqué, une mise à jour ou un rappel peuvent apparaître sous forme de notification. Elles se trouvent généralement dans un panneau que l'on ouvre en faisant glisser le doigt du haut de l'écran vers le bas.

Lire une notification Glissez du haut vers le bas, puis touchez la notification pour ouvrir l'application concernée.	**Effacer une notification** Glissez-la sur le côté ou utilisez « Effacer ». Cela ne supprime pas forcément le message ou le contenu.
Trop de notifications ? Un appui prolongé permet souvent d'ouvrir les réglages de l'application et de choisir ce que l'on souhaite recevoir.	**Attention** Une notification peut être frauduleuse : les réflexes de la séance 1 restent valables.

Les réglages rapides

En glissant une ou deux fois du haut vers le bas, Android affiche des commandes rapides. Leur emplacement varie selon le modèle.



Luminosité

Réglez-la pour mieux lire l'écran et économiser la batterie.

Son / silencieux

Les boutons latéraux règlent généralement le volume. Le panneau rapide peut proposer silencieux ou vibration.

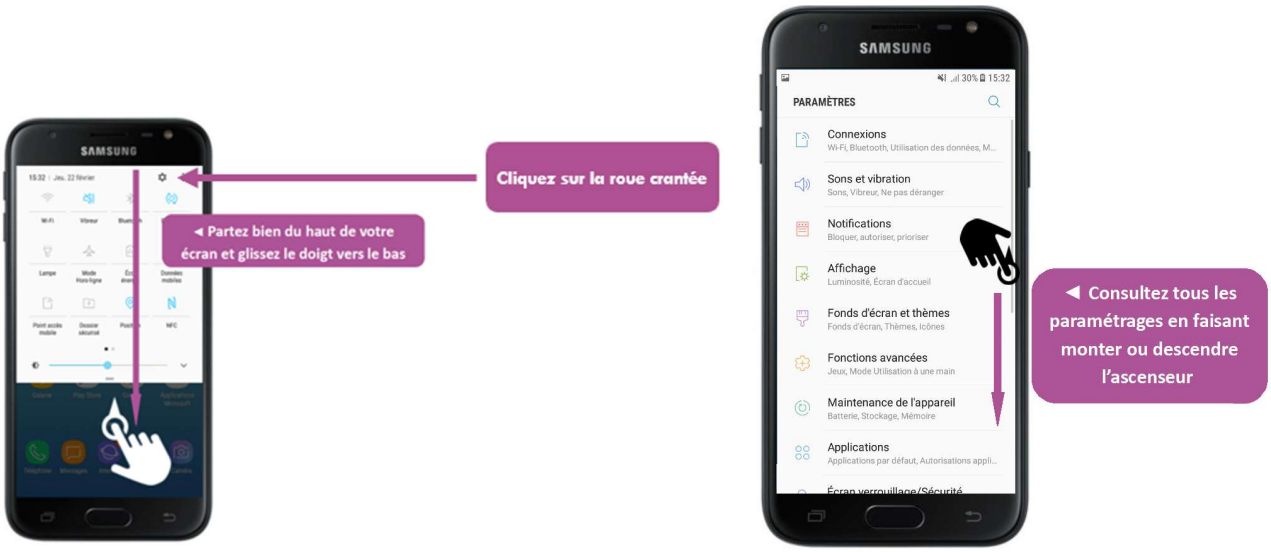
Rotation de l'écran

Activez-la si vous souhaitez que l'écran bascule lorsque vous tournez le téléphone.

Taille du texte

Dans Réglages > Affichage ou Accessibilité, augmentez le texte si nécessaire. Les noms exacts varient.

Les paramètres



À retenir

Si vous ne trouvez pas un réglage, ouvrez **Réglages** et utilisez la barre de recherche. Les noms et emplacements peuvent varier selon la marque.

Protéger l’accès au smartphone

Un bon verrouillage empêche une autre personne d’ouvrir facilement votre téléphone

Pourquoi verrouiller son smartphone ?

Votre téléphone contient souvent vos messages, photos, contacts, applications bancaires et accès à de nombreux services. Le verrouillage de l’écran constitue la première barrière en cas de perte, d’oubli ou de vol.

Choisir un verrouillage efficace

Aucun / Balayer Le téléphone s’ouvre sans véritable vérification. **À éviter : cela ne protège pas vos données**.	**Code PIN** Simple et pratique. Utilisez de préférence au moins 6 chiffres et évitez les suites évidentes ou les dates faciles à deviner.
Schéma Pratique, mais choisissez un dessin difficile à deviner. Évitez les formes très simples comme un L ou un carré.	**Mot de passe** Très protecteur s’il est suffisamment long, mais moins pratique à saisir plusieurs fois par jour.

Empreinte digitale ou reconnaissance faciale ?

La biométrie permet de déverrouiller rapidement le téléphone. Selon le modèle, vous pouvez utiliser une empreinte digitale, votre visage, ou les deux.

- La biométrie est pratique, mais un code, un schéma ou un mot de passe reste toujours nécessaire en secours.
- Après un redémarrage du téléphone, Android peut demander le code principal avant d’autoriser à nouveau l’empreinte ou le visage.
- La qualité de la reconnaissance faciale varie selon les appareils : suivez les indications de sécurité affichées par votre téléphone.

Bien régler son écran verrouillé

Le téléphone doit se verrouiller seul et ne pas afficher trop d’informations sensibles

Vérifier le verrouillage automatique

Un bon code ne sert à rien si le téléphone reste déverrouillé pendant plusieurs minutes après que vous l’avez posé. Cherchez dans les **Paramètres** les options liées à l’écran, au verrouillage automatique ou au **délai** avant verrouillage.

Réglage conseillé

Choisissez un délai assez court pour que le téléphone se verrouille rapidement lorsqu’il n’est plus utilisé, par exemple 30 secondes ou 1 minute. Adaptez-le à votre confort de travail.

Attention aux notifications sur l’écran verrouillé

Même verrouillé, un smartphone peut afficher le contenu de SMS, de mails ou de messages WhatsApp. Une personne qui trouve votre téléphone pourrait donc lire des informations sans connaître votre code.

À vérifier sur votre smartphone

- Repérez le délai de mise en veille ou de verrouillage automatique.

- Verrouillez votre téléphone avec le bouton Marche/Arrêt puis regardez ce qui reste visible à l'écran.
- Cherchez le réglage « Notifications sur l'écran de verrouillage » et vérifiez si le contenu sensible est masqué.
- Attendez le verrouillage automatique, puis vérifiez qu'un code ou la biométrie est demandé.

Code du téléphone et code PIN de la SIM

Deux protections différentes à ne pas confondre

Deux codes qui ne protègent pas la même chose

	CODE DU TÉLÉPHONE	CODE PIN DE LA SIM
Protège	L'accès au smartphone et à ses données.	L'utilisation de votre carte SIM et de votre numéro.
Demandé quand ?	Quand vous déverrouillez l'écran.	Après un redémarrage ou si la SIM est placée dans un autre appareil.
Où le régler ?	**Paramètres > Sécurité / Écran de verrouillage.**	**Paramètres > Sécurité / SIM**. Le nom varie selon le modèle.
En cas d'erreurs	Le téléphone impose généralement un délai entre les tentatives.	Après plusieurs erreurs (généralement 3), la SIM peut demander le code PUK fourni par l'opérateur.

Attention avant de modifier le PIN de la SIM

Ne testez pas plusieurs codes au hasard. Si vous ne connaissez pas le code PIN actuel ou le code PUK, consultez les documents de votre opérateur ou contactez-le avant de modifier ce réglage.

Mon smartphone est-il correctement protégé ?

- Mon téléphone demande un code, un schéma ou un mot de passe pour s'ouvrir.
- Si j'utilise un code PIN, il comporte au moins 6 chiffres et n'est pas facile à deviner.
- J'utilise l'empreinte ou le visage seulement en complément du code principal.
- Mon téléphone se verrouille automatiquement après une courte période d'inactivité.
- Le contenu sensible de mes notifications n'est pas visible par n'importe qui sur l'écran verrouillé.
- Je connais la différence entre le code de mon téléphone et le code PIN de ma carte SIM.

Retrouver mon téléphone

Préparer la localisation avant d'en avoir besoin

Le bon réflexe : préparer avant de perdre

La localisation à distance ne se configure pas au moment où le téléphone a déjà disparu. Vérifiez aujourd'hui que votre smartphone Android est bien prêt à être retrouvé.

Vérifier que le téléphone peut être retrouvé

Sur Android, le service de Google s'appelle actuellement « Localiser » (Find Hub). Les noms exacts des menus peuvent varier selon la marque et la version d'Android.

1. **Compte Google —** Vérifiez qu'un compte Google est bien connecté au smartphone.
2. **Localisation —** Dans Paramètres, cherchez « Localisation » et vérifiez qu'elle est activée.
3. **Service Localiser —** Dans Paramètres, recherchez « Localiser », « Find Hub » ou « appareil perdu » et vérifiez que l'appareil peut être localisé.
4. **Verrouillage de l'écran —** Conservez un code, un schéma ou un mot de passe de verrouillage. Il protège le téléphone et permet aussi certaines fonctions de localisation hors connexion.
5. **Localisation hors connexion —** Si cette option existe sur votre appareil, laissez-la activée : elle peut aider à retrouver un téléphone qui n'est plus connecté au Wi-Fi ou aux données mobiles.

Faire le test

Le meilleur moyen de savoir si tout fonctionne est de tester la localisation pendant que vous avez encore le téléphone en main.

1. Depuis un ordinateur ou un autre appareil, ouvrez le service Google Localiser / Find Hub.(**https://android.com/find**)
2. Connectez-vous avec le même compte Google que celui utilisé sur le smartphone.
3. Sélectionnez votre téléphone et vérifiez qu'il apparaît sur la carte.
4. Testez la fonction permettant de faire sonner le téléphone.

À retenir

Si votre téléphone n'apparaît pas aujourd'hui dans Localiser, il ne faudra pas compter sur cette fonction le jour où il sera réellement perdu.

Mon téléphone a disparu : que faire ?
Localiser, faire sonner, sécuriser… puis effacer seulement en dernier recours

LOCALISER Affiche la position connue du téléphone sur une carte. La position peut être approximative ou correspondre à une position récente.	**FAIRE SONNER** Utile si le téléphone est probablement à proximité : maison, voiture, hangar, prairie…
SIGNALER COMME ÉGARÉ Verrouille l'appareil et peut afficher un message ou des coordonnées pour permettre à une personne honnête de vous contacter.	**EFFACER LES DONNÉES** Dernier recours si vous pensez ne plus récupérer l'appareil. L'effacement est définitif et, après cela, le téléphone ne pourra plus être localisé avec le service.

S'il s'agit d'un vol

Notez les informations utiles et contactez la police si nécessaire.
Contactez votre opérateur mobile pour faire bloquer la carte SIM. L'opérateur peut aussi avoir besoin du numéro IMEI de l'appareil. **Astuce : prenez note de ces informations dans un carnet (en dehors de votre téléphone)**

Et si le téléphone est éteint ou hors connexion ?

La localisation immédiate peut être impossible. Selon le modèle, les réglages activés et la version d'Android, Google peut néanmoins afficher une localisation récente ou utiliser le réseau Localiser pour aider à retrouver certains appareils hors connexion.

Sauvegarder mes données

Via les paramètres de votre téléphone (section **Google** > **Sauvegarde**), vous pouvez enregistrer :

- **Vos applications** et leurs données (pour retrouver vos applications déjà installées sur un nouveau téléphone).
- **L'historique de vos appels** et vos **SMS/MMS**.
- **Les paramètres de l'appareil** (mots de passe Wi-Fi, fonds d'écran, langues, disposition de l'écran d'accueil).
- **Vos alarmes** et préférences de l'horloge.

Comprendre les connexions

Wi-Fi, données mobiles et Bluetooth : ce n'est pas la même chose

Un smartphone peut communiquer de plusieurs façons. Le Wi-Fi et les données mobiles donnent accès à Internet. Le Bluetooth sert surtout à relier des appareils proches entre eux.

Les trois connexions à reconnaître

Connexion	À quoi ça sert ?	Ce qu'il faut	À retenir
Wi-Fi	Accéder à Internet via une box, un routeur ou un point d'accès.	Être à portée du réseau et, souvent, connaître son mot de passe.	Ne consomme pas votre forfait de données mobiles.
4G / 5G	Accéder à Internet via le réseau de votre opérateur.	Une carte SIM/eSIM, du réseau et un forfait de données.	Peut consommer votre volume de données mobiles.
Bluetooth	Relier des appareils proches : voiture, casque, enceinte, montre…	Activer Bluetooth et associer les appareils.	Ce n'est généralement pas une connexion à Internet.

Comment savoir quelle connexion est utilisée ?

- Le symbole Wi-Fi en haut de l'écran indique généralement que le téléphone utilise un réseau Wi-Fi.
- Les indications 4G, 5G, LTE ou similaires signalent une connexion au réseau mobile.
- L'icône Bluetooth peut apparaître lorsqu'un accessoire est connecté ou que Bluetooth est actif, selon le modèle.

Se connecter et se déconnecter

Choisir un réseau, l'oublier et utiliser les réglages rapides

Se connecter à un réseau Wi-Fi

1. **Ouvrir le Wi-Fi —** Faites glisser le haut de l'écran vers le bas puis touchez Wi-Fi, ou ouvrez Paramètres > Réseau et Internet / Connexions.
2. **Choisir le réseau —** Touchez le nom du réseau auquel vous voulez vous connecter.
3. **Entrer le mot de passe —** Si un cadenas apparaît, le réseau demande un mot de passe.
4. **Vérifier —** Une fois connecté, le nom du réseau ou le symbole Wi-Fi apparaît dans les réglages ou la barre d'état.

Se déconnecter… ou oublier le réseau ?

DÉSACTIVER LE WI-FI
Coupe temporairement le Wi-Fi. Le téléphone pourra se reconnecter lorsque vous le réactiverez.

CHANGER DE RÉSEAU
Sélectionnez simplement un autre réseau disponible.

OUBLIER UN RÉSEAU
Supprime le réseau enregistré. Le mot de passe devra être saisi à nouveau pour s'y reconnecter.

Données mobiles : activer ou couper

Dans les **réglages rapides** ou dans **Paramètres** > **Réseau et Internet / Connexions** > **Réseau mobile**, vous pouvez activer ou désactiver les données mobiles.

Si le Wi-Fi fonctionne, Android utilise généralement le Wi-Fi plutôt que les données mobiles.

Et le mode avion ?

Le mode avion coupe les connexions radio principales. Selon le téléphone, il est ensuite possible de réactiver manuellement le Wi-Fi ou le Bluetooth. C'est utile en avion, mais aussi parfois pour relancer rapidement une connexion qui fonctionne mal.

Partager sa connexion

Utiliser le smartphone pour connecter un ordinateur à Internet

Le partage de connexion

Votre smartphone peut transformer sa connexion mobile en petit point d'accès Wi-Fi pour un ordinateur ou un autre appareil. On parle aussi de « point d'accès », « hotspot » ou « modem ».

Partager Internet avec son ordinateur

Activer les données mobiles — Le téléphone doit lui-même avoir accès à Internet via le réseau mobile.

Activer le point d'accès — Dans les **réglages rapides** ou **Paramètres**, recherchez « **Point d'accès** », « **Partage de connexion** » ou « **Hotspot** ».

Connecter l'ordinateur — Repérez le nom et le mot de passe du point d'accès. Sur le PC, choisissez ce réseau Wi-Fi puis entrez le mot de passe.

Couper après usage — Désactivez le point d'accès lorsque vous avez terminé pour économiser batterie et données mobiles.

Les précautions utiles

- Le partage de connexion utilise votre forfait mobile et davantage de batterie : surveillez les gros téléchargements et branchez le téléphone si nécessaire.
- Gardez un mot de passe sur votre point d'accès. Ne laissez pas un hotspot ouvert à tout le monde.
- Sur un Wi-Fi public ou inconnu, évitez les opérations sensibles si vous avez un doute sur le réseau.

Les réflexes à retenir

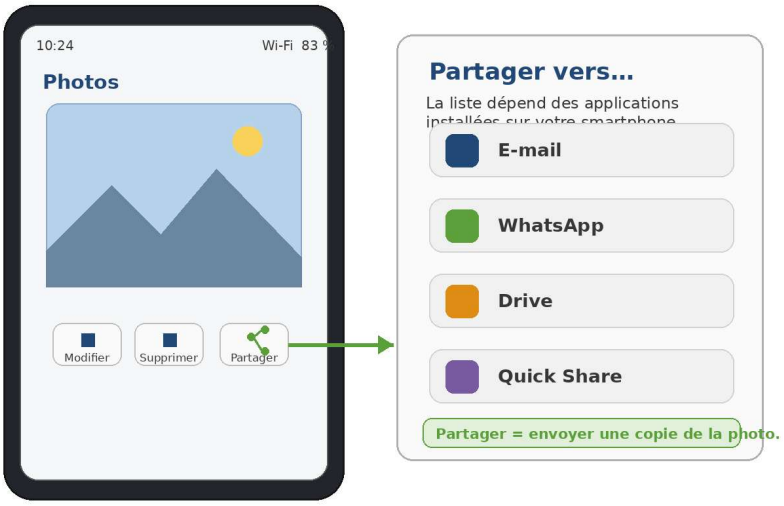
Wi-Fi, 4G/5G, Bluetooth
Wi-Fi = un réseau connu quand il est disponible. 4G/5G = Internet via mon forfait mobile. Bluetooth = relier des appareils proches.

Partager une photo depuis son smartphone

Sur la plupart des smartphones Android, la méthode est la même : ouvrir la photo, toucher Partager, puis choisir la destination.

Idée simple à retenir

Le bouton Partager permet d'envoyer une copie d'une photo vers une autre application ou une autre personne. La photo d'origine reste dans le smartphone.



Les étapes

1. Ouvrez Photos ou Galerie.
2. Touchez la photo à envoyer.
3. Touchez Partager.
4. Choisissez la destination : e-mail, WhatsApp, Drive, partage à proximité…
5. Vérifiez le destinataire avant d'envoyer.

À savoir

La liste proposée dépend des applications installées. Si l'application souhaitée n'apparaît pas, faites défiler ou choisissez "Plus".



Objectif de ce support

Apprendre à mieux organiser les fichiers et les photos de son ordinateur, à les retrouver facilement et à en conserver une copie de sécurité sur un support externe.

À la fin de cette partie, je dois savoir :

- me repérer sur le bureau et dans l'explorateur de fichiers ;
- comprendre la différence entre un fichier et un dossier ;
- reconnaître quelques types de fichiers courants : photo, PDF, document, tableau ;
- ouvrir, renommer, copier, déplacer et supprimer un fichier ;
- retrouver mes documents dans Documents, Images ou Téléchargements ;
- créer des dossiers et donner des noms clairs à mes fichiers ;
- partager ou exporter une photo depuis mon smartphone ;
- brancher un disque dur externe à mon ordinateur ;
- copier mes dossiers importants sur ce disque ;
- vérifier que la sauvegarde a bien été réalisée ;
- comprendre qu'une sauvegarde est une copie supplémentaire et ne remplace pas les fichiers présents sur l'ordinateur.

Mon ordinateur : fichiers, photos et sauvegardes

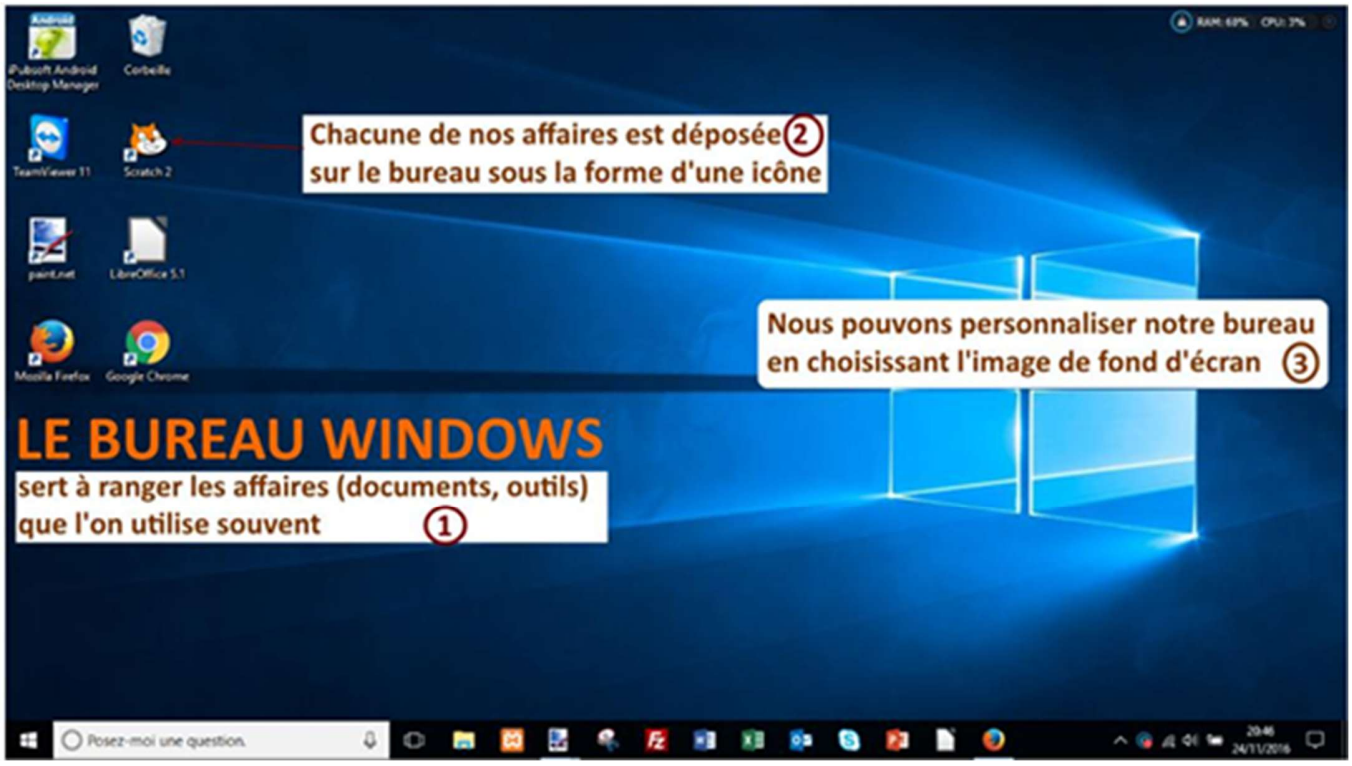
Selon l'ordinateur, l'écran peut varier un peu. Les repères et les gestes restent toutefois très proches d'un appareil à l'autre.

Se repérer sur l'écran

Quand l'ordinateur est allumé, on arrive le plus souvent sur le bureau. On y retrouve des icônes, la barre des tâches, le bouton Démarrer et l'heure.

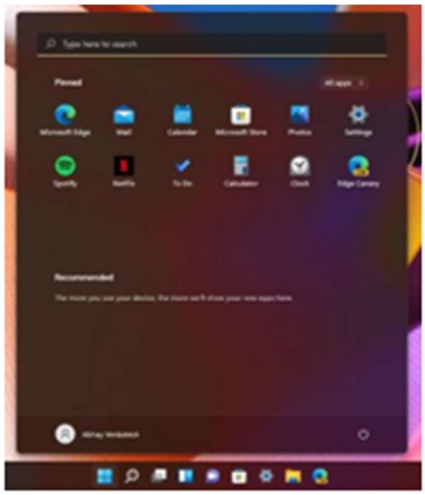


- Le bureau : l'écran principal avec des icônes.

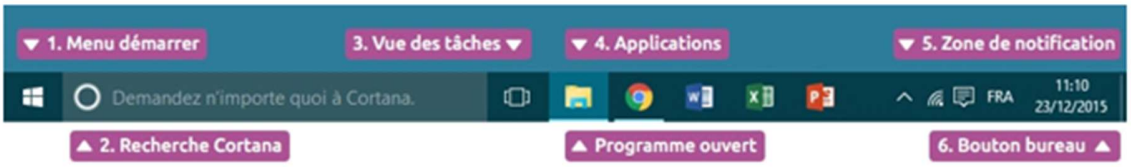


- Le bouton Démarrer : ouvrir des programmes, rechercher et éteindre.



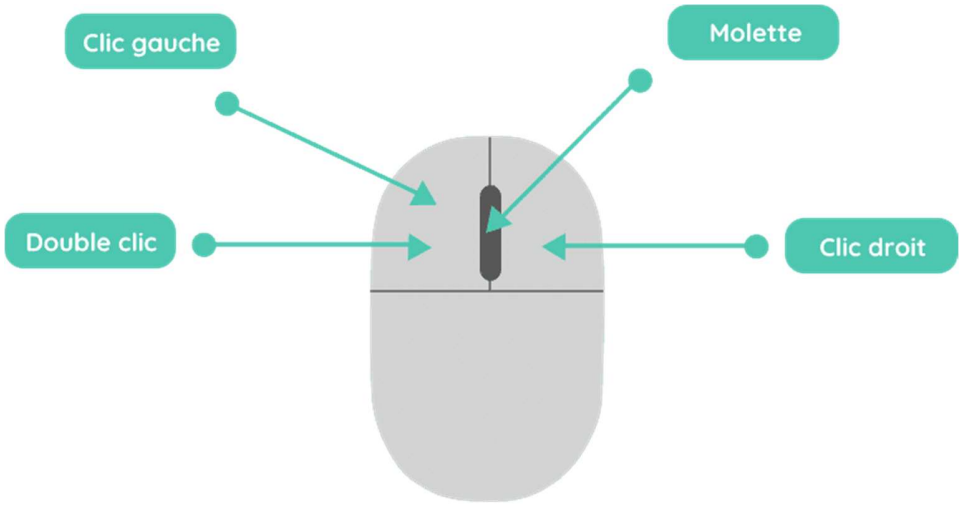


- La barre des tâches : voir les programmes ouverts - À droite : heure, son et réseau.



La souris : les actions de base

La souris permet de pointer, cliquer, ouvrir un élément et se déplacer dans une page.



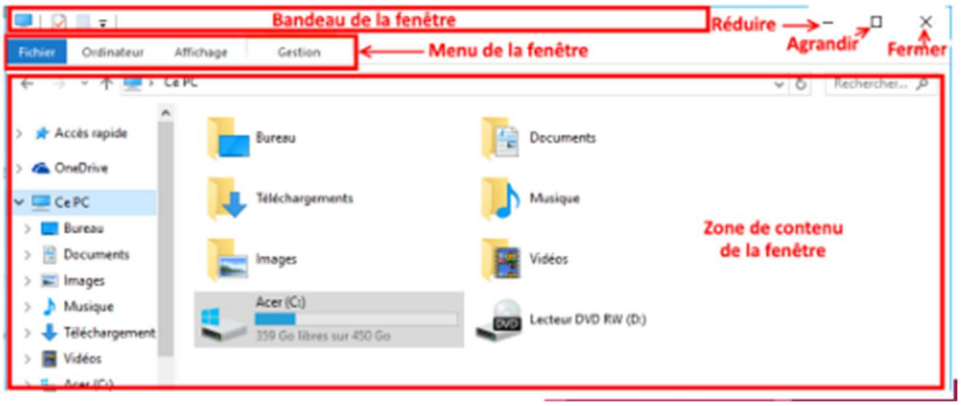
Les gestes à retenir

- Clic gauche : sélectionner ou cliquer sur un bouton.
- Double-clic : ouvrir un dossier, un fichier ou un programme.
- Clic droit : faire apparaître un menu d'options.
- Molette : faire défiler vers le haut ou vers le bas.

Glisser-déposer : maintenir le clic et déplacer un élément.

Les fenêtres : ouvrir, réduire, agrandir, fermer

Quand on ouvre un programme, il s'affiche dans une fenêtre. En haut à droite, trois boutons sont très utiles : réduire, agrandir et fermer.

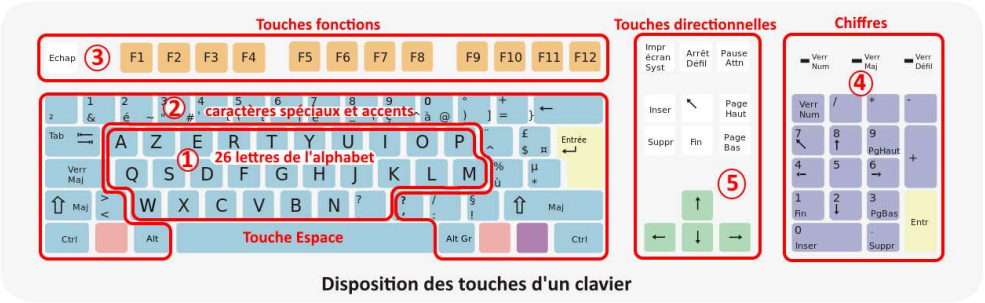


À retenir

- Réduire : la fenêtre descend dans la barre des tâches sans se fermer.
- Agrandir : la fenêtre prend presque tout l'écran.
- Fermer : la fenêtre se ferme complètement.

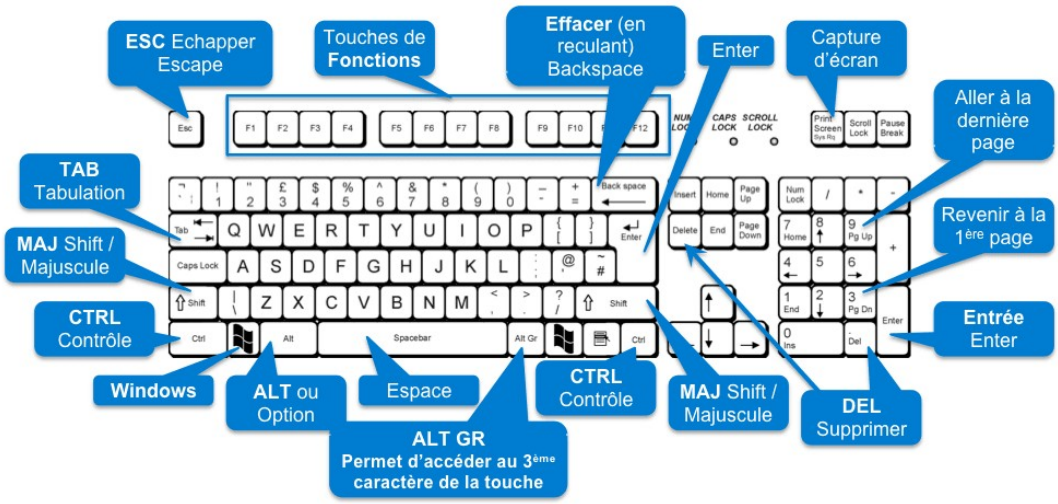
Le clavier : quelques touches très utiles

Le clavier permet d'écrire du texte, mais aussi de valider une action, effacer un caractère ou mettre une lettre en majuscule.



Les touches à retenir

- Entrée : valider une action ou aller à la ligne.
- Retour arrière : effacer le caractère situé à gauche du curseur.
- Espace : laisser un espace entre deux mots.
- Maj : écrire une majuscule temporaire.

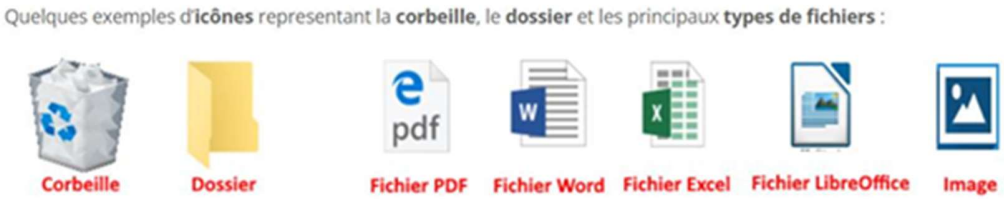


Premiers bons réflexes

- Un simple clic suffit souvent.
- Fermez la fenêtre avec la croix quand vous avez terminé.
- Si quelque chose ne fonctionne pas, prenez le temps de lire l'écran.

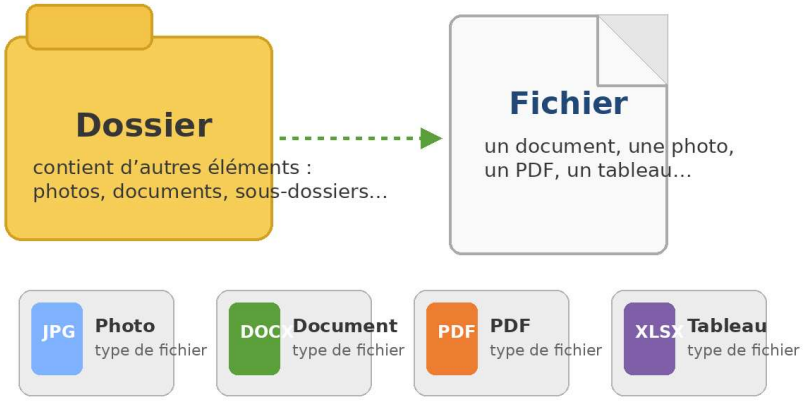
Comprendre les fichiers et les dossiers

Un **fichier** est un élément enregistré dans l'ordinateur : une photo, un document, un PDF… Un **dossier** sert à ranger plusieurs fichiers ensemble, comme une chemise de classement.



Fichier ou dossier : quelle différence ?

Le fichier contient l'information. Le dossier sert à la classer et à mieux la retrouver.



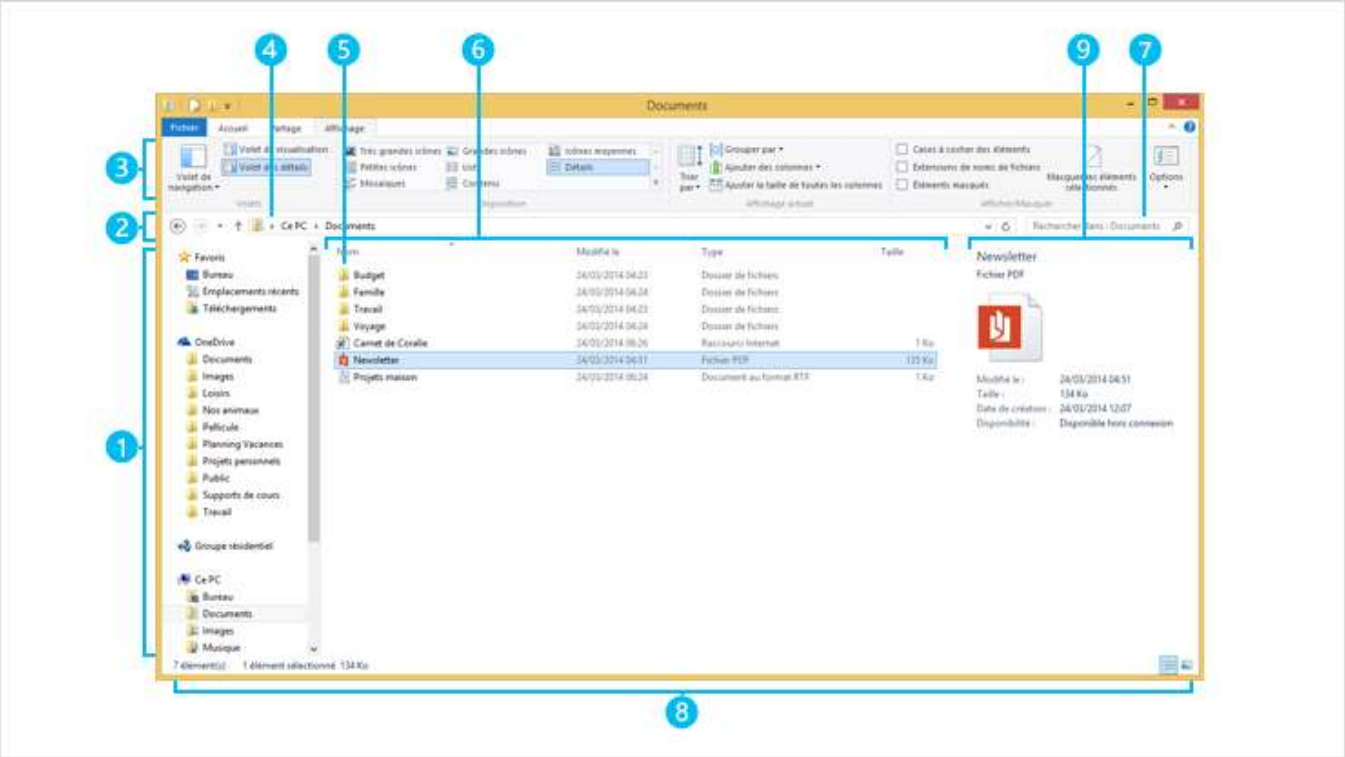
À retenir

- Un fichier peut être une photo, une lettre, un PDF ou un tableau.

- Un dossier peut contenir des fichiers et d'autres dossiers.
- Le nom et parfois l'extension aident à reconnaître le type de fichier : .jpg, .pdf, .docx, .xlsx…

L'explorateur de fichiers

L'explorateur de fichiers permet de voir où sont enregistrés les dossiers et les fichiers.

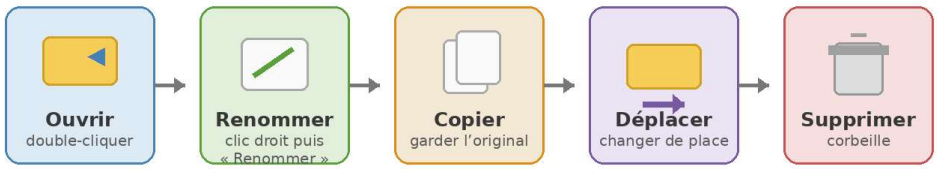


Repères utiles

- À gauche : les emplacements importants comme Documents, Images et Téléchargements.
- Au centre : la liste des fichiers et des dossiers.
- En haut : le chemin qui indique l'endroit où l'on se trouve.

Actions de base sur un fichier

Les gestes les plus courants sont : ouvrir, renommer, copier, déplacer et supprimer.



Astuce : prenez le temps de lire ce qui est proposé à l'écran.
Sur beaucoup d'ordinateurs, un clic droit donne accès aux actions utiles.

Les gestes simples

- Ouvrir : on double-clique souvent sur le fichier ou le dossier.
- Renommer : un clic droit permet de donner un nom plus clair.
- Supprimer : on clique sur le fichier et on appuie sur la touche Suppr (ou Del), ou clic droit et supprimer > .le fichier part d'abord dans la corbeille.

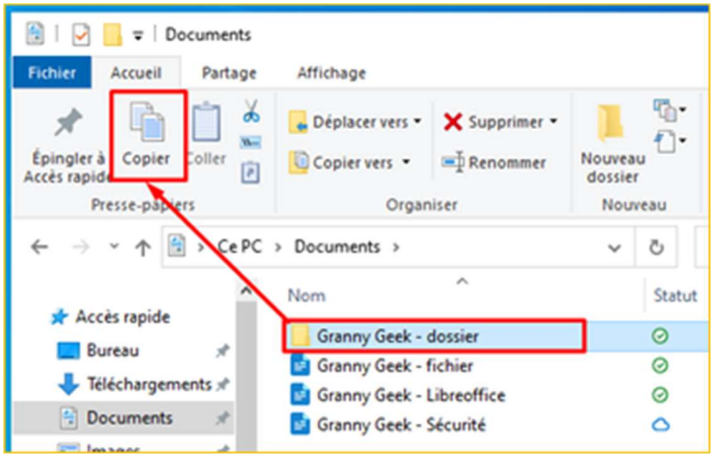
Bon réflexe

Avant de déplacer ou de supprimer un document important, vérifiez bien son nom et l'endroit où il est rangé.

Dupliquer un fichier

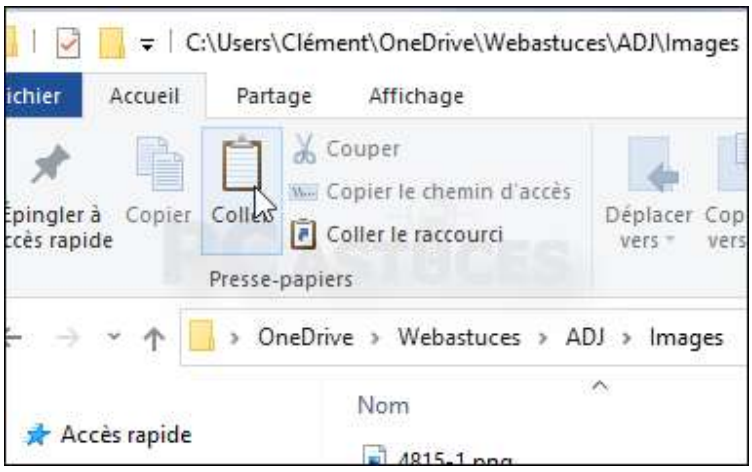
Pour dupliquer rapidement un fichier dans le même dossier sous Windows, sélectionnez le fichier puis appuyez sur les touches Ctrl + C (copier) puis Ctrl + V (coller). Windows créera une copie intitulée « - Copie ».

1. Copier un fichier



ou **CTRL + C**

2. Allez à l'emplacement où copier les fichiers.
3. Coller un fichier



ou **CTRL + V**

Où retrouver ses fichiers ?

On perd souvent un document parce qu'on ne sait plus où il a été enregistré. Quelques habitudes simples aident à le retrouver.



Les emplacements fréquents

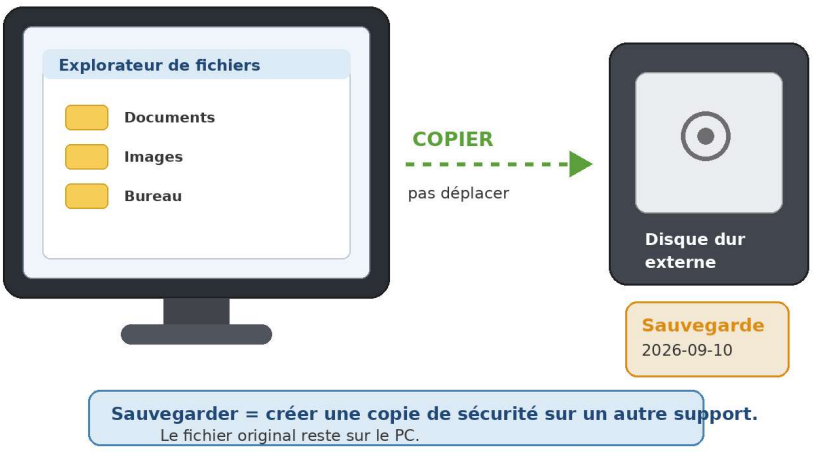
- Documents : pour les lettres, PDF, formulaires et autres papiers numériques.
- Images : pour les photos et les captures d'écran.
- Téléchargements : pour les fichiers récupérés depuis internet.

Bons réflexes

- Donnez un nom clair à vos fichiers.
- Rangez vos fichiers dans des dossiers logiques.
- Après un téléchargement, regardez où le fichier a été enregistré.

Sauvegarder sur un disque dur amovible

Une sauvegarde est une copie de sécurité de vos fichiers importants. Elle permet de les récupérer si le PC tombe en panne ou si un fichier est supprimé par erreur.



Quels dossiers sauvegarder ?

- Documents : factures, courriers, formulaires, tableaux…
- Images : photos de l'exploitation, du matériel, des documents…
- Bureau : seulement si vous y conservez des fichiers importants.
- Tout autre dossier contenant des données que vous ne voulez pas perdre.

Les étapes d'une sauvegarde



À ne pas oublier

- Gardez l'original sur le PC : ne le déplacez pas vers le disque.
- Ne laissez pas le disque de sauvegarde branché en permanence.
- Refaites une sauvegarde régulièrement.

1. Branchez le disque externe et attendez qu'il apparaisse dans l'explorateur.
2. Créez sur le disque **un dossier au nom clair**, par exemple "Sauvegarde 2026-09-10".
3. Sur le PC, sélectionnez les dossiers importants et choisissez **Copier**.
4. Ouvrez le dossier de sauvegarde sur le disque et choisissez **Coller**.
5. Attendez la fin de la copie, puis ouvrez quelques fichiers pour vérifier.
6. **Éjectez correctement le disque** avant de le débrancher.

Les réflexes à retenir

- Refaites une sauvegarde régulièrement.
- Ne laissez pas le disque branché en permanence au PC.
- Vérifiez de temps en temps que les fichiers sauvegardés s'ouvrent.

Internet et navigateur

Comprendre le navigateur

Internet, Google et Chrome ne sont pas la même chose. Apprendre à les distinguer permet de mieux comprendre ce qui se passe à l'écran et de retrouver plus facilement un site.

Internet, navigateur, moteur de recherche, site web

Ces quatre mots sont souvent mélangés. Pourtant, ils désignent des choses différentes.

Mot	Ce que c'est	Exemple / image mentale
Internet	Le réseau qui relie des ordinateurs et des services dans le monde.	La "route" qui permet d'accéder aux services en ligne.
Navigateur	Le programme utilisé pour afficher les sites web.	Chrome, Edge, Firefox…
Moteur de recherche	Un service qui aide à trouver des pages sur le web.	Google, Bing…
Site web	Un ensemble de pages accessibles à une adresse précise.	Le site d'une banque, d'une administration, d'un fournisseur…

Une comparaison simple

- Internet = le réseau, comme un ensemble de routes.
- Le navigateur = le véhicule qui permet de circuler sur ces routes.
- Le moteur de recherche = l'annuaire qui aide à trouver une destination.
- Le site web = la destination que l'on veut atteindre.

La barre d'adresse : mon repère principal

La barre d'adresse se trouve en haut du navigateur. Elle sert à voir l'adresse du site sur lequel on se trouve. On peut aussi y taper directement une adresse ou des mots pour effectuer une recherche.



Un bon réflexe de sécurité

Pour un site important, par exemple une administration, votre banque ou un fournisseur, regardez toujours l'adresse affichée dans la barre d'adresse. Si vous avez reçu un lien douteux, mieux vaut ouvrir vous-même le navigateur et rechercher le site officiel.

Les commandes les plus utiles

Commande	À quoi elle sert
← **Retour**	Revenir à la page précédente.
→ **Suivant**	Retourner vers une page quittée après avoir utilisé Retour.
⟳ **Actualiser**	Recharger la page si elle s'affiche mal ou si elle doit être mise à jour.
Barre d'adresse	Écrire ou lire l'adresse d'un site. Elle peut aussi servir à lancer une recherche.
Onglet	Ouvrir plusieurs pages dans la même fenêtre sans perdre la page actuelle.
× **Fermer un onglet**	Fermer seulement la page concernée, pas nécessairement tout le navigateur.

Les onglets : garder plusieurs pages ouvertes

Un onglet est une page ouverte dans le navigateur. Plusieurs onglets permettent de consulter plusieurs sites sans fermer les pages déjà ouvertes.

- Un nouvel onglet s'ouvre généralement avec le bouton +.
- Cliquez sur un onglet pour revenir à la page correspondante.
- Fermez l'onglet avec sa petite croix lorsque vous n'en avez plus besoin.
- Si vous ouvrez trop d'onglets, il devient plus difficile de vous repérer.

Retrouver facilement ce que j'ai consulté

Le navigateur garde plusieurs repères qui peuvent éviter de tout rechercher à nouveau.

Les favoris / marque-pages

Ils servent à enregistrer l'adresse d'un site que l'on consulte souvent. C'est pratique pour revenir rapidement sur un site officiel ou un service utilisé régulièrement.

L'historique
L'historique permet de retrouver les pages consultées auparavant. Il est utile lorsque l'on se souvient du site, mais plus de son adresse exacte.

Les téléchargements
Quand on télécharge un PDF, une facture ou un autre document depuis Internet, le navigateur garde généralement une liste des fichiers téléchargés. Le fichier se trouve souvent dans le dossier "Téléchargements" de l'ordinateur.

Internet, comptes et démarches en ligne

Se connecter et se déconnecter

Se connecter à un compte
Se connecter signifie indiquer au site ou au service qui vous êtes afin d'accéder à votre espace personnel. Vous entrez généralement un identifiant et un mot de passe.

Pourquoi se connecter ?
Pour retrouver vos informations personnelles, vos documents ou des services réservés à votre compte.

Se déconnecter
Se déconnecter signifie fermer l'accès à votre compte sur l'appareil que vous utilisez. C'est particulièrement important sur un ordinateur qui ne vous appartient pas.

Fermer un onglet ≠ se déconnecter
Fermer la page du navigateur ne signifie pas forcément que votre compte est fermé. Si vous rouvrez le site, vous pouvez parfois être encore connecté.

À faire sur votre ordinateur ou smartphone
- Connectez-vous à un compte que vous utilisez pendant la formation.
- Fermez simplement l'onglet puis rouvrez le site : observez si vous êtes encore connecté.
- Repérez ensuite le bouton ou le menu « Se déconnecter ».

« Mon mot de passe est enregistré… mais où ? »
Le navigateur peut proposer d'enregistrer un mot de passe lorsque vous vous connectez à un site. Cela permet de le retrouver et parfois de le remplir automatiquement lors d'une prochaine visite.

- Le navigateur peut proposer d'enregistrer un nouveau mot de passe.
- Vous pouvez retrouver les mots de passe déjà enregistrés.
- Vous pouvez supprimer un ancien mot de passe qui ne doit plus être utilisé.
- Le navigateur peut aussi proposer de générer un mot de passe.
- Lorsque la synchronisation est activée, les informations liées au compte peuvent être retrouvées sur plusieurs appareils.

À retenir
Un mot de passe enregistré n'est pas « perdu dans l'ordinateur » : il se trouve dans l'espace de gestion des mots de passe du navigateur ou du compte associé.

À faire sur votre ordinateur ou smartphone
- Ouvrez les paramètres de votre navigateur.

- Repérez la partie consacrée aux mots de passe enregistrés.
- Cherchez si certains sites y apparaissent déjà.

Reconnaître un site officiel belge

Vérifier l'adresse du site

Les sites des administrations utilisent des adresses web qui permettent de vérifier où l'on se trouve. Le Wooclap insiste particulièrement sur la lecture de l'adresse du site.

- L'extension .be est un repère important pour les sites officiels belges.
- Pour l'État fédéral, on rencontre notamment des adresses contenant .fgov.be ou .fed.be.
- L'élément officiel doit se trouver juste avant le .be.
- Exemple présenté comme correct dans le cours : safeonweb.be.
- Exemples présentés comme frauduleux : safeonweb-be.com ou safeonweb.com.
- Le cours rappelle aussi la présence du cadenas à gauche de l'adresse, indiquant que la connexion est chiffrée.

Quelques portails officiels à connaître

- Belgium.be : portail d'information officiel de l'État fédéral.
- MyGov.be : application et portefeuille digital pour accéder à des documents officiels.
- Mon Dossier : accès aux données du Registre national.
- Wallonie.be : guichet officiel pour les démarches régionales en Wallonie.

À faire sur votre ordinateur ou smartphone

- Tapez vous-même le nom d'un portail officiel dans votre navigateur.
- Repérez l'adresse affichée en haut de la page avant de poursuivre.

S'identifier sur les services publics avec CSAM

À quoi sert CSAM ?

CSAM est présenté dans le cours comme le point d'identification central permettant d'accéder à de nombreux services en ligne de l'administration belge avec un niveau de sécurité élevé.

Important

Pour vous connecter à une administration, le cours rappelle qu'on ne vous demandera pas vos codes bancaires.

Exemples de services accessibles via CSAM

- Administration fédérale : par exemple Tax-on-web ou Student@Work.
- Administrations régionales : par exemple IRISbox.
- Communes : e-guichets de nombreuses communes.
- Institutions auxiliaires : par exemple certaines mutualités.
- Dans le Wooclap, Mon espace citoyen, eBox, MaSanté, MyPension et MyMinFin sont associés à une connexion via CSAM.
- Facebook et la SNCB sont associés à un autre moyen de connexion.

Moyens d'identification présentés dans le cours

- L'application itsme.
- L'application MyGov.be.

- La carte d'identité électronique eID avec un lecteur de carte et son code PIN.

La carte d’identité électronique eID

La carte eID et le lecteur de carte

La carte d'identité ou carte de résident belge eID contient des informations personnelles. Sa puce électronique permet aussi de vous identifier en ligne.

- Elle peut servir à vous identifier auprès de différentes instances.
- Elle peut être utilisée pour signer des documents électroniques.
- Elle permet une connexion sécurisée à des services publics en ligne.
- Pour lire les informations de la puce sur un ordinateur, le cours présente l'utilisation d'un lecteur de carte eID.
- La carte eID est associée à un code PIN à 4 chiffres.

Où retrouver le code PIN ?

Le cours indique que les codes figurent sur la lettre reçue lors du renouvellement ou de la délivrance d'une nouvelle eID.

Code oublié ou carte bloquée ?

Le Wooclap indique qu'après trois tentatives avec un mauvais code, ou si le code PIN est perdu ou oublié, un nouveau code PIN doit être obtenu auprès de l'administration communale.

À faire sur votre ordinateur ou smartphone

- Repérez le lecteur de carte eID utilisé pendant la formation.
- Identifiez l’endroit où insérer la carte.
- Rappelez à quoi sert le code PIN de l’eID.

Itsme et MyGov

À quoi servent ces applications ?

Itsme et MyGov sont présentés comme des applications permettant de justifier votre identité en ligne et de vous connecter à différents services administratifs depuis un PC ou un smartphone.

Différence présentée dans le cours

Itsme est une application privée agréée par l'État. MyGov.be est l'application publique officielle de l'État belge.

De quoi avez-vous besoin ?

- Un smartphone avec une carte SIM.
- L'application installée sur le smartphone.
- Un code personnel choisi lors de la configuration.
- Un lecteur de carte eID est nécessaire lors de la création du compte, mais pas à chaque utilisation ensuite.

Que peut-on faire ?

- S’identifier sur des services en ligne.
- Signer certains contrats.
- Confirmer certains paiements.

Remplir un formulaire en ligne

Reconnaître les différents champs

Un formulaire en ligne peut contenir différents types de champs : zones de texte, listes, cases à cocher ou choix obligatoires. Certaines zones demandent aussi de respecter des contraintes avant de pouvoir envoyer le formulaire.

Pourquoi voit-on parfois un CAPTCHA ?

Empêcher des programmes automatisés d'introduire de fausses informations dans un formulaire.

- Il peut demander de recopier un texte déformé.
- Il peut demander de sélectionner certaines images selon un critère.
- Le but est de vérifier que l'utilisateur est bien une personne et non un programme automatisé.

Cases à cocher, newsletters et conditions générales

Toutes les cases ne sont pas obligatoires

Le cours distingue les cases facultatives, souvent liées à des services supplémentaires, et les cases indispensables pour utiliser le service demandé.

Newsletter et partage d'informations

- Une newsletter correspond à des e-mails envoyés régulièrement, souvent avec des offres promotionnelles.
- Si le site propose un service supplémentaire ou l'envoi d'une newsletter, le cours indique que vous n'êtes pas obligé d'accepter.
- Certains sites peuvent demander la permission de communiquer vos informations à des tiers.
- Si ces cases sont décochées, le site ne peut normalement pas utiliser vos données pour ces finalités supplémentaires.

Conditions générales d'utilisation ou de vente

Les conditions générales sont les règles qui encadrent l'utilisation du service, ce que le site peut faire avec vos informations et les engagements liés au service.

- Pour certains formulaires, accepter les conditions générales est nécessaire pour poursuivre.
- Si vous refusez les conditions, le formulaire peut ne pas pouvoir être envoyé.
- On rencontre notamment les termes CGU (conditions générales d'utilisation) et CGV (conditions générales de vente).

Le réflexe à retenir

Avant de cocher, lisez ce qui est demandé : une case peut être nécessaire au service, ou seulement servir à recevoir des offres ou à autoriser un autre usage de vos informations.

À faire sur votre ordinateur ou smartphone

- Sur un formulaire d'exercice, repérez une case facultative et une case nécessaire pour poursuivre.
- Expliquez avec vos mots ce que vous acceptez en cochant chacune d'elles.