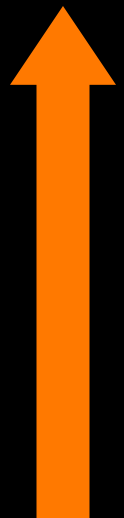
Eviter les arnaques en ligne

Un Atelier Numérique Orange

Christophe Ferrier



1 – Mots de passe

2 – Phishing / Hameçonnage

3 – Appels indésirables

4 – Questions / réponses

1 – Mots de passe

2 – Phishing / Hameçonnage

3 – Appels indésirables

4 – Questions / réponses

Pourquoi de plus en plus de sites nous imposent des contraintes dans la création de nos mots de passe ?

Parce que la complexité de notre mot de passe va déterminer le temps mis par les pirates pour le retrouver en essayant toutes les combinaisons possibles.

Le temps qu'il faut aux pirates pour retrouver nos mots de passe.

Nombre de caractères	Nombres seulement	Lettres minuscules	Lettres majuscules et minuscules	Nombres, lettres majuscules et minuscules	Nombres, lettres majuscules et minuscules, symboles
4	Immédiat	Immédiat	Immédiat	Immédiat	Immédiat
5	Immédiat	Immédiat	Immédiat	Immédiat	Immédiat
6	Immédiat	Immédiat	Immédiat	Immédiat	Immédiat
7	Immédiat	Immédiat	1 seconde	2 secondes	4 secondes
8	Immédiat	Immédiat	28 secondes	2 minutes	5 minutes
9	Immédiat	3 secondes	24 minutes	2 heures	6 heures
10	Immédiat	1 minute	21 heures	5 jours	2 semaines
11	Immédiat	32 minutes	1 mois	10 mois	3 ans
12	1 seconde	14 heures	6 ans	53 ans	226 ans
13	5 secondes	2 semaines	332 années	3 000 années	15 000 ans
14	52 secondes	1 an	17 000 ans	202 000 ans	1 million d'années
15	9 minutes	27 ans	898 000 ans	12 millions d'années	77 millions d'années
16	1 heure	713 ans	46 millions d'années	779 millions d'années	5 milliards d'années
17	14 heures	18 000 ans	2 milliards d'années	48 milliards d'années	380 milliards d'années
18	6 jours	481 000 ans	126 milliards d'années	1 trillion d'années	26 trillions d'années

Source : Hive Systems 2023

Un mot de passe unique pour chaque compte

En cas de perte ou de vol d'un de vos mots de passe, seul le service concerné sera vulnérable.

Dans le cas contraire, tous les services pour lesquels vous utilisez le même mot de passe compromis seraient piratables.

Votre mot de passe de messagerie est l'un des plus importants à protéger.

Un mot de passe impossible à deviner

- Ne pas employer dans vos mots de passe des informations personnelles qui pourraient être faciles à retrouver comme votre nom, prénom, date anniversaire, lieu de résidence.

- Ne pas employer les suites simples ou connues comme 123456, azerty, abcdef…

Un mot de passe à renouveler régulièrement et à changer au moindre soupçon.

Les mots de passe

Les mots de passe sont le premier rempart de protection pour vos équipements informatiques et comptes en ligne

Trop souvent encore les mots de passe sont vus comme quelque chose de compliqué et de difficile à gérer

En adoptant quelques bonnes pratiques et bons outils, vous ferez des mots de passe vos alliés pour protéger efficacement votre mobile et vos comptes en ligne

Comment créer un mot de passe facile à mémoriser ?

- Construire un mot de passe d'au minimum 12 caractères
- Choisir le titre d'un livre/film/chanson/slogan/phrase :
  Exemple : Lepetitprince
- Ajouter au moins un chiffre et un caractère spécial (* ! $...) : 24*
- Choisir les deux premières lettres en majuscule du compte

  OR pour Orange => mot de passe : Lepetitprince24*OR
  EN pour Engie => mot de passe : Lepetitprince24*EN

La méthode des premières lettres peut aussi être utilisée
Exemple : le proverbe « On n'est jamais mieux servi que par soi même » donnera : On'ejmsqpsm24

Créer un mot de passe robuste mais facile à mémoriser

Un mot de passe robuste c'est

1. **12 caractères minimum**

+

2. **Un mélange de lettres minuscules, majuscules, chiffres et caractères spéciaux (! , @ ; * $ …)**

La méthode des premières lettres

Composer une suite de mots que vous retiendrez facilement

1 Lapin + 2 poules = 3 bestioles dans la basse-cour !

Puis, « compacter » cette phrase en prenant les premières lettres de chaque mot, garder les nombres et la ponctuation

1L+2p=3bdlbc!

La méthode phonétique

Composer une phrase / suite de mots que vous retiendrez facilement

j'ai acheté 8 Cédérom pour 100 euros cet après-midi !

Puis, « compacter » cette phrase en l'écrivant phonétiquement en gardant les nombres et la ponctuation

ght8CDp%E7am!

Protéger l'accès à ses équipements et comptes

	Code de la carte SIM	Code de déverrouillage du mobile	Codes d'accès aux services en ligne
			
À faire	Personnaliser le code Utiliser un code non trivial (ex: 4387)	Définir un code d'accès numérique de 6 à 8 chiffres Activer l'accès biométrique	Un mot de passe robuste et unique pour chaque service Activer l'authentification renforcée
À ne pas faire	Laisser le code par défaut Désactiver le code PIN de la carte SIM	Désactiver le verrouillage Utiliser un code trop simple	Mots de passe trop simples ou faciles à deviner Utiliser le même mot de passe sur plusieurs sites

Les gestionnaires de mots de passe

Ce sont des logiciels conçus pour stocker de façon sécurisée des mots de passe. Ils intègrent des fonctions de génération de mots de passe très robustes et une fonction de saisie automatique.

Gestionnaires intégrés dans les services associés au mobile

Trousseau iCloud Apple

Gestionnaire de mots de passe Google

Gestionnaires basés sur des solutions gratuites ou payantes

KeePass

KeePass : un gestionnaire de mots de passe sécurisé et gratuit

Ce petit logiciel libre et en français, certifié par l'ANSSI, permet de stocker en sécurité vos mots de passe pour les utiliser dans vos applications.

Bitwarden **… etc**

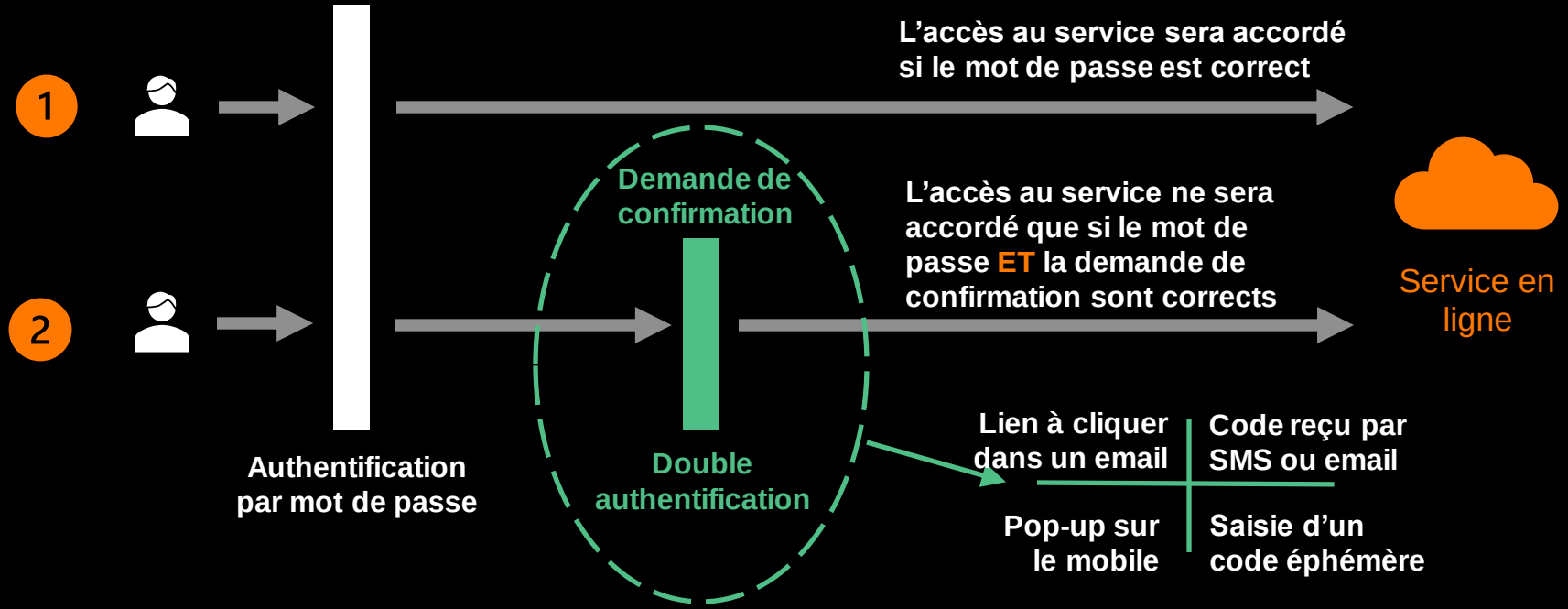
1Password **Dashlane**

L'utilisation d'un gestionnaire permettra d'avoir à retenir uniquement un seul mot de passe : celui pour ouvrir l'accès du gestionnaire.

La double authentification ou « authentification renforcée »

- La double authentification, c'est permettre l'accès à un service avec un mot de passe ET une demande de confirmation additionnelle
- La demande de confirmation peut être un pop-up à cliquer sur le mobile
- La demande de confirmation peut être un code reçu par SMS ou email
- La demande de confirmation peut être un code généré par une application qu'il faudra saisir dans la page web
- La double authentification permet de bloquer l'accès à un service dans le cas où le mot de passe aurait été découvert ou compromis

La double authentification ou « authentification renforcée »



La double authentification permet de bloquer l'accès à un service dans le cas où le mot de passe aurait été découvert ou compromis

Il est recommandé de l'activer dès que proposée par le service

En résumé, les bonnes pratiques pour ses mots de passe

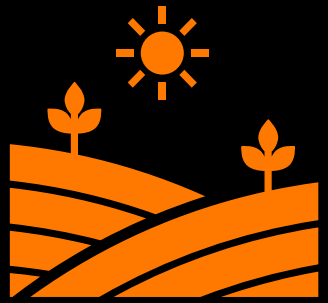
Je protège l'accès à mon smartphone avec un code PIN et un code d'accès robustes.
J'utilise la reconnaissance biométrique

J'active la double authentification pour protéger l'accès à mes comptes : un second verrou c'est mieux qu'un seul !

J'utilise des mots de passe complexes/robustes et uniques pour protéger l'accès à chaque service

J'utilise un gestionnaire de mots de passe pour qu'ils soient tous robustes et uniques pour chaque site

Et vous ?



1 – Mots de passe

2 – Phishing / Hameçonnage

3 – Appels indésirables

4 – Questions / réponses

Pourquoi faut-il faire attention aux sms/mails que l'on reçoit ?

Le phishing (ou hameçonnage) est une technique de manipulation utilisée par des fraudeurs.

- Usurpation d'identité : elle consiste à se faire passer pour un organisme qui vous est familier (banque, CAF, opérateur de téléphonie, impôts) en utilisant son logo, son nom.
- Fins frauduleuses : elle permet notamment de dérober des informations personnelles et/ou financières.

Mail ou SMS ?

répondre | transférer | traiter comme indésirable | déplacer vers

de	"Direction Générales des Finances publiques" <kqjkas@oapemsl.com>
à	
date	07/11/17 10:11
objet	IMPÔT SUR LE REVENU : DÉCLARATION DE VOS REVENU EN LIGNE

DIRECTION GÉNÉRALE DES
FINANCES PUBLIQUES

Remarque !

L'absence de contestation vaudra acceptation des dites modifications de votre part.

Madame / Monsieur,

Vous avez déclaré vos revenus en ligne e

La Direction Générale des Finances Publique
d'administration fiscale d'impôt sur le revenu.
recevoir un remboursement de notre part d'u
facturation effectuée par nos services.

Pour éviter tout incident , nous vous invitons

Orange F 10:37 39 %

+33 6 50 49 86

Message
jeu. 28 avr. à 10:54

Votre colis a été envoyé. Veuillez le vérifier et le recevoir. http://irxvj.yvqsr.com

Orange F 10:37 39 %

+33 7 80 06

Message
jeu. 28 avr. à 14:19

Votre solde CPF est arrivé a échéance. Veuillez remplir le formulaire ci-dessous sous 24h, pour convertir vos droits acquis en 2021 https://cutt.ly/nGvEwj9

Message

Orange F 10:36 39 %

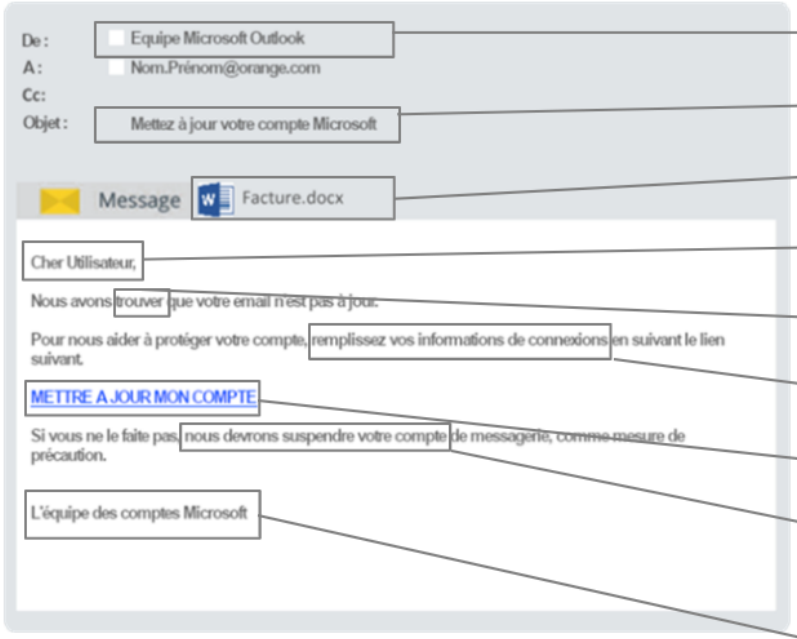
+33 7 49 32 99

Message
mer. 4 mai à 13:37

[ASSURANCE-MLD]: Après les calculs de l'analyse de votre dossier d'Assurance Maladie, nous vous informons que vous allez recevoir un remboursement de 776,99 euros. Veuillez le valider via le lien ci-joint: https://cpam-indemnite-r.com/social

Message

Comment reconnaître un mail de phishing ?



Expéditeur suspect

Sujet inhabituel ou sans interaction préalable

Pièce jointe suspecte ou inattendue

Mauvaise personnalisation

Erreurs de syntaxe ou d'orthographe

Demande d'informations personnelles / sensibles

Lien suspect

Ton urgent / menaçant ou offre de cadeaux / argent, ou jouant sur l'aspect sentimental (proche en difficulté)

Esthétique suspecte

Comment réagir en cas de doute ?

- Ne jamais répondre aux mails ou SMS vous demandant des informations confidentielles.
- Ne jamais cliquer sur les liens/pièces jointes d'un message suspect provenant d'un interlocuteur que vous ne connaissez pas.

En cas de tentative de phishing, vous pouvez le signaler :

- Signal Spam : signalement des mails et des adresses de sites frauduleux https://www.signal-spam.fr/
- Fédération Française des télécoms : signalement de contenus numériques illicites https://signalement.fftelecoms.org/

Si vous êtes victime de Spam téléphonique

- Demandez à votre interlocuteur à ce que vos données soient retirées des fichiers de coordonnées de l'appelant.
- Pour bloquer un SMS ou MMS indésirables, envoyer le mot « STOP » à l'expéditeur.
- Signalez-le sur la plateforme 33700 (www.33700.fr) ou par SMS au 33700.
- Bloquer les SMS ou appels indésirables directement sur votre téléphone mobile.
- En cas de sollicitations abusives, faites une réclamation depuis le site Bloctel.
- Si les appels persistent, déposez plainte auprès de la CNIL ou d'un commissariat de police.

Pour lever tous vos doutes

- Aller sur le site Internet de l'expéditeur en s'assurant que l'on est bien sur son adresse précise.

- Se connecter à votre compte client avec vos identifiants et mots de passe habituels.

- Prendre connaissance des éventuelles demandes en attente et y répondre.

Oups, vous avez cliqué ?

- Mais vous n'avez saisi aucune donnée sur le site pointé et réalisé aucune action, le risque est faible (attention, le risque 0 n'existe pas).

- Vous avez communiqué un mot de passe que vous utilisez pour d'autres sites, modifiez-le immédiatement sur tous ces sites.

- Vous avez communiqué vos coordonnées bancaires ou celles de votre carte de crédit, prévenez sans délai votre banque.

1 – Mots de passe

2 – Phishing / Hameçonnage

3 – Appels indésirables

4 – Questions / réponses

Se préserver des appels indésirables et démarchage illégal

Reprenez le contrôle sur vos appels en identifiant et bloquant les appels indésirables sur votre mobile

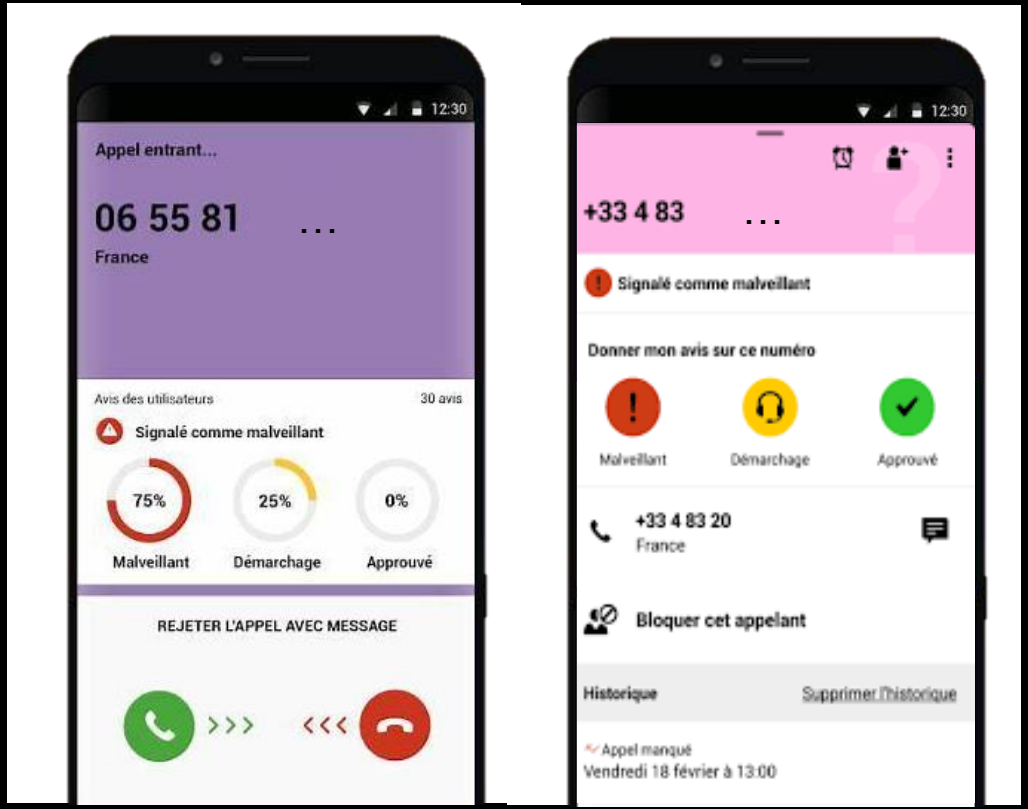
- Des applications téléchargeables sous Android et iPhone
- Gratuites et sans publicités
- Accessibles à tous*

Orange et moi

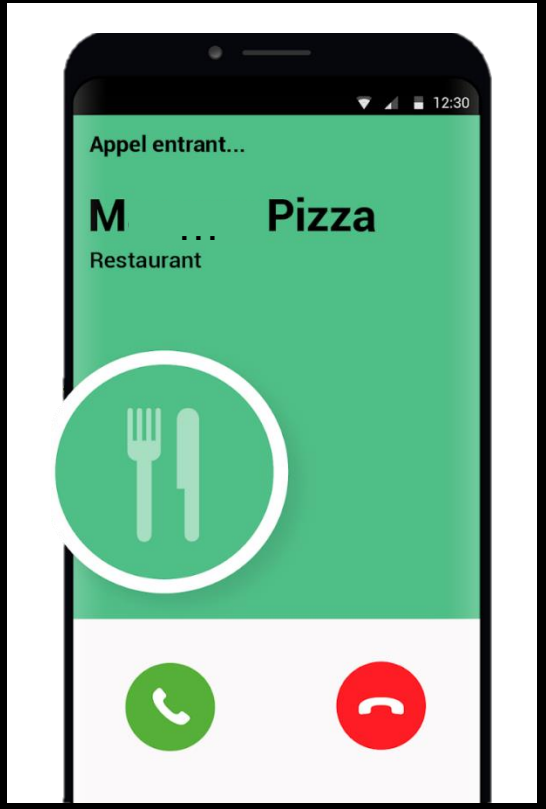
Orange téléphone

*hors coût de connexion internet mobile selon l'offre souscrite
**Orange et moi fonctionne uniquement pour les clients particuliers Orange disposant d'une offre mobile ou internet. En revanche, Orange Téléphone est accessible à tous.

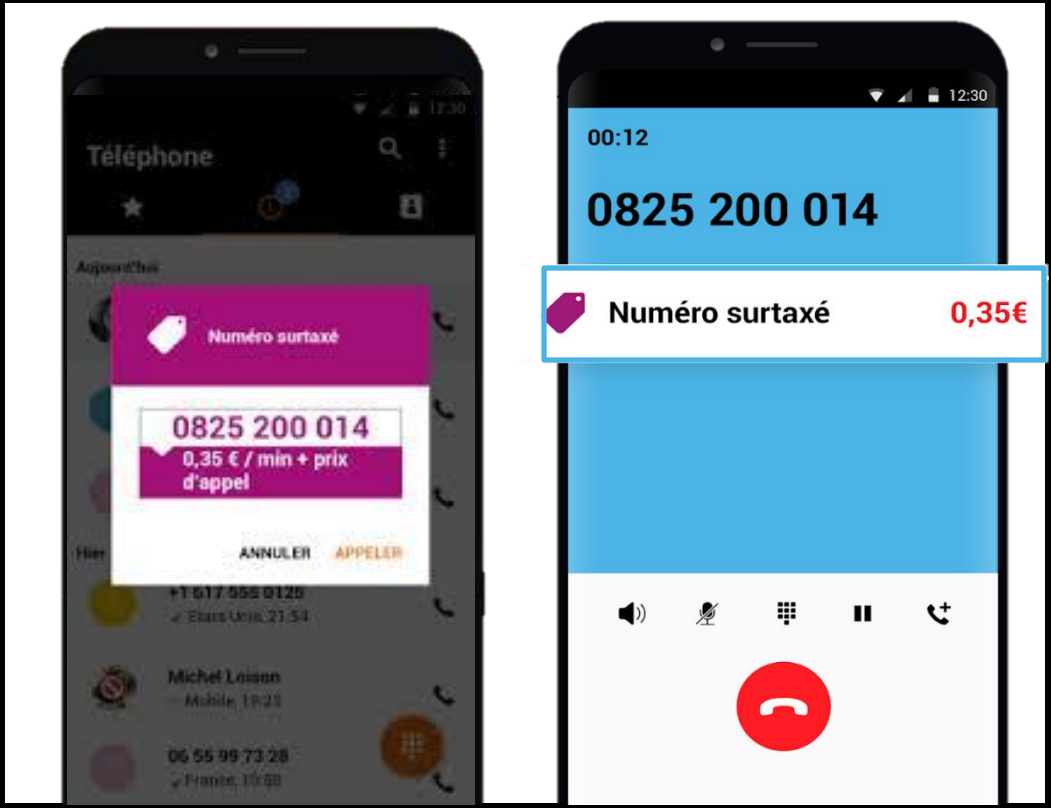
Anti-spam : appels indésirables



Annuaire inversé

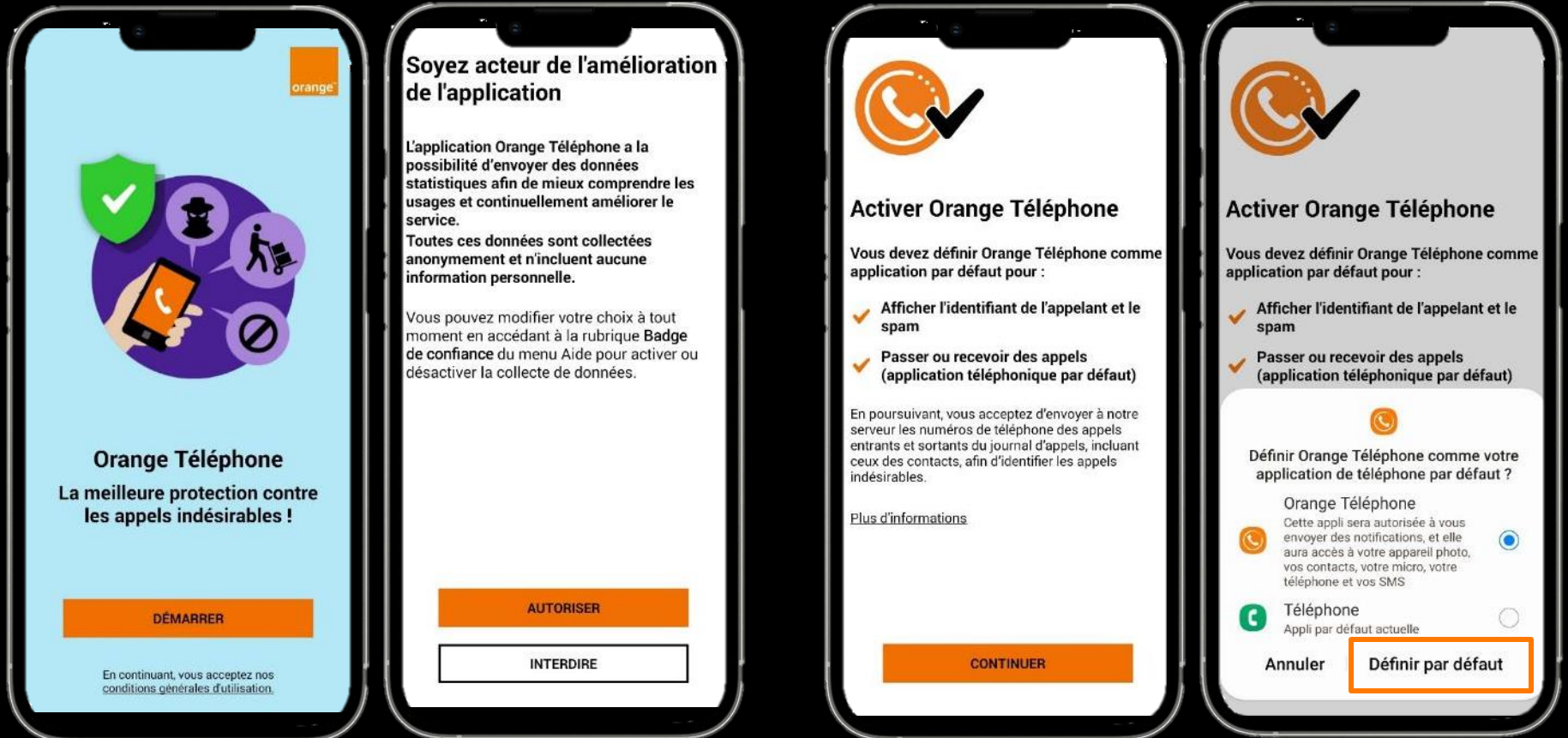


Anti-escroquerie : Numéros surtaxés



Numéros d'urgence

Ouvrir l'application Orange Téléphone



1 – Mots de passe

2 – Phishing / Hameçonnage

3 – Appels indésirables

4 – Questions / réponses

Découvrez des articles, des conseils et des vidéos conçus pour vous aider à vous familiariser avec le monde numérique et l'utiliser en toute tranquillité **sur** Bien vivre le digital (orange.fr)

Rejoignez-nous pour un nouvel Atelier Numérique Orange !

Découvrez un large catalogue de thématiques conçu pour développer vos compétences numériques.
Les Ateliers Numériques Orange sont gratuits et ouverts à tous.

Ne tardez pas, inscrivez-vous dès maintenant et retrouvez-nous pour un atelier enrichissant et convivial.

Réserver dès maintenant votre place sur
https://inscription.orange.fr/ateliersnumeriques

ou en appelant le numéro d'appel gratuit 0800 06 15 46 du lundi au samedi de 8 heures à 20 heures

Votre avis nous intéresse !

Répondez à ce court sondage

Cliquer ici pour répondre au sondage

OU

Munissez-vous de votre smartphone Android ou iPhone.

- Ouvrez l'application « appareil photo »
- Placez le téléphone sur le QR Code
- Cliquez sur le lien qui apparaît

Valorisez l'acquisition de vos nouvelles compétences

En récupérant votre badge de compétences numérique

Cliquez ici pour récupérer votre badge de compétences

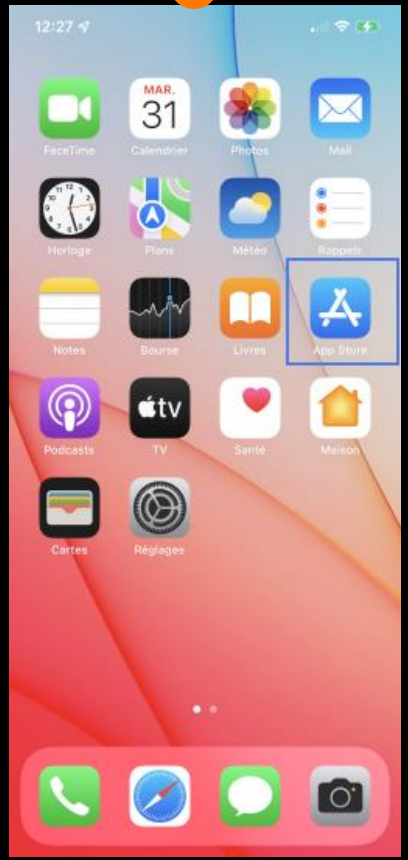
OU

Munissez-vous de votre smartphone Android ou iPhone.

- Ouvrez l'application « appareil photo »
- Placez le téléphone sur le QR Code
- Cliquez sur le lien qui apparaît

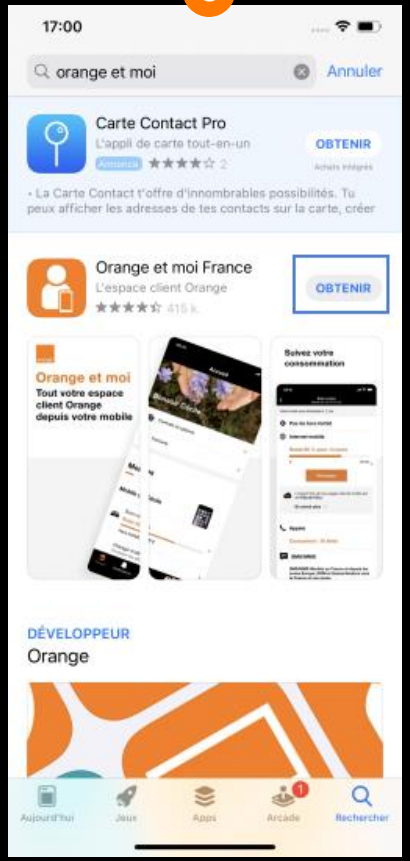
Télécharger et installer une application

1



2

3



4

Télécharger et installer une application

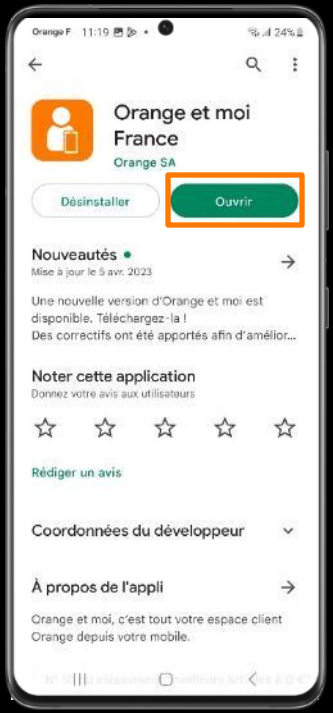
1

Cherchez l'application désirée en entrant son nom dans le champ de recherche.

2

Appuyez sur Installer pour installer votre application sur le smartphone.

3



L'application est installée. Appuyez sur Ouvrir pour la lancer. L'application s'affichera ensuite automatiquement sur le menu d'accueil du smartphone.

Les applications sont téléchargeables dans la boutique en ligne : le Play Store*.

N'hésitez pas à lire la description et les avis pour juger de la qualité d'une application.

*Compte Google indispensable

Merci