FAÇONNEUR D'Avenir

WEBINAIRE :

« La digitalisation et la sécurisation de vos moyens de paiement »

Intervenants

Benoît MERCEY : Chargé Partenariats & Filières
Nurten KARAKOL : Conseillère Développement des Flux

FILIÈRE TOURISME by CA CHAMPAGNE BOURGOGNE

Côte-d'Or ATTRACTIVITÉ

Pour le bon déroulé de cette présentation,
pensez à **couper vos micros**.

N'hésitez pas à poser **vos questions sur le chat**,
nous y reviendrons plus tard.

Sommaire

1) La règlementation encadrant les moyens de paiement

2) La digitalisation croissante des moyens de paiement

La digitalisation des moyens de paiement : une solution d'avenir

81%

des entreprises reconnaissent la contribution du multicanal dans la sauvegarde de l'activité

79%

considèrent que le multicanal maintient la relation client

78%

considèrent que le multicanal permet une amélioration en termes de satisfaction & de fidélité client

Les bénéfices de l'omnicanalité incontestés

D'après le Baromètre de Croissance & Digital 2021 – étude réalisée sur 701 entreprises (toutes entreprises)

La digitalisation des moyens de paiement : une solution d'avenir

La digitalisation des moyens de paiement

BOUTIQUE EN LIGNE, BOUTIQUE PHYSIQUE : NÉCESSITÉ et COMPLÉMENTARITÉ

Journée d'Inès, une future cliente de Salomé

Le soir Inès voit ses macarons préférés sur la page facebook de la boutique de Salomé qui se trouve près de son travail

Inès se rend dans la boutique de Salomé sur sa pause déjeuner pour récupérer son achat.

La spécialité n'est plus disponible mais Salomé lui propose de la commander et de lui envoyer à son domicile. Inès paie sa commande sur le TPE de Salomé et s'enrôle sur le programme de fidélité de Salomé (**UP2PAY Fidélité**)

Chez elle, Inès partage son avis sur la boutique de Salomé sur les réseaux sociaux de celle-ci.

Lors de sa pause au bureau, Inès commande ses macarons et paie avec le lien sms (UP2PAY par lien) et demande un retrait en Click & collect

Inès jette un œil dans la boutique et voit une spécialité locale qui l'intéresse

3) Etre visible et vendre sur Internet

Comment développer votre activité ?

- ÉLARGIR SA ZONE DE CHALANDISE
- ÊTRE PRÉSENT ET VISIBLE SUR INTERNET
- ETRE CAPABLE DE VENDRE SUR PLUSIEURS CANAUX ET AVEC TOUS MOYENS DE PAIEMENT
- OFFRIR UN PARCOURS SIMPLE ET RAPIDE A SON CLIENT

- CONNAITRE ET COMMUNIQUER AVEC SES CLIENTS
- CONSTRUIRE UNE BASE CLIENTS ET UN PROGRAMME DE FIDELITE
- SECURISER SES ENCAISSEMENTS
- ENCAISSER EN CLICK & COLLECT

Comment être visible et vendre sur Internet ?

D'après le Baromètre de Croissance & Digital 2021 – étude réalisée sur 701 entreprises (toutes entreprises)

FAÇONNEUR D'Avenir

61% ont une page PRO

63% ont un site vitrine

VISIBILITÉ

Réseaux sociaux

Google My Business

Paiement à distance

up2pay

Par lien

VISIBILITÉ / VENTE à DISTANCE

Site Vitrine

Simplébo

Paiement à distance

up2pay

Par lien

SITE MARCHAND

Site Marchand simple

(clé en main, plateforme saas)

+

Paiement à distance

up2pay

Par lien

Paiement en ligne

up2pay

e-Transactions

SITE MARCHAND / ENCAISSEMENT OMNICANAL

Site Marchand complexe développé par une agence web

PrestaShop

WOO COMMERCE

+ Paiement à distance

up2pay

Par lien

+ Paiement en ligne

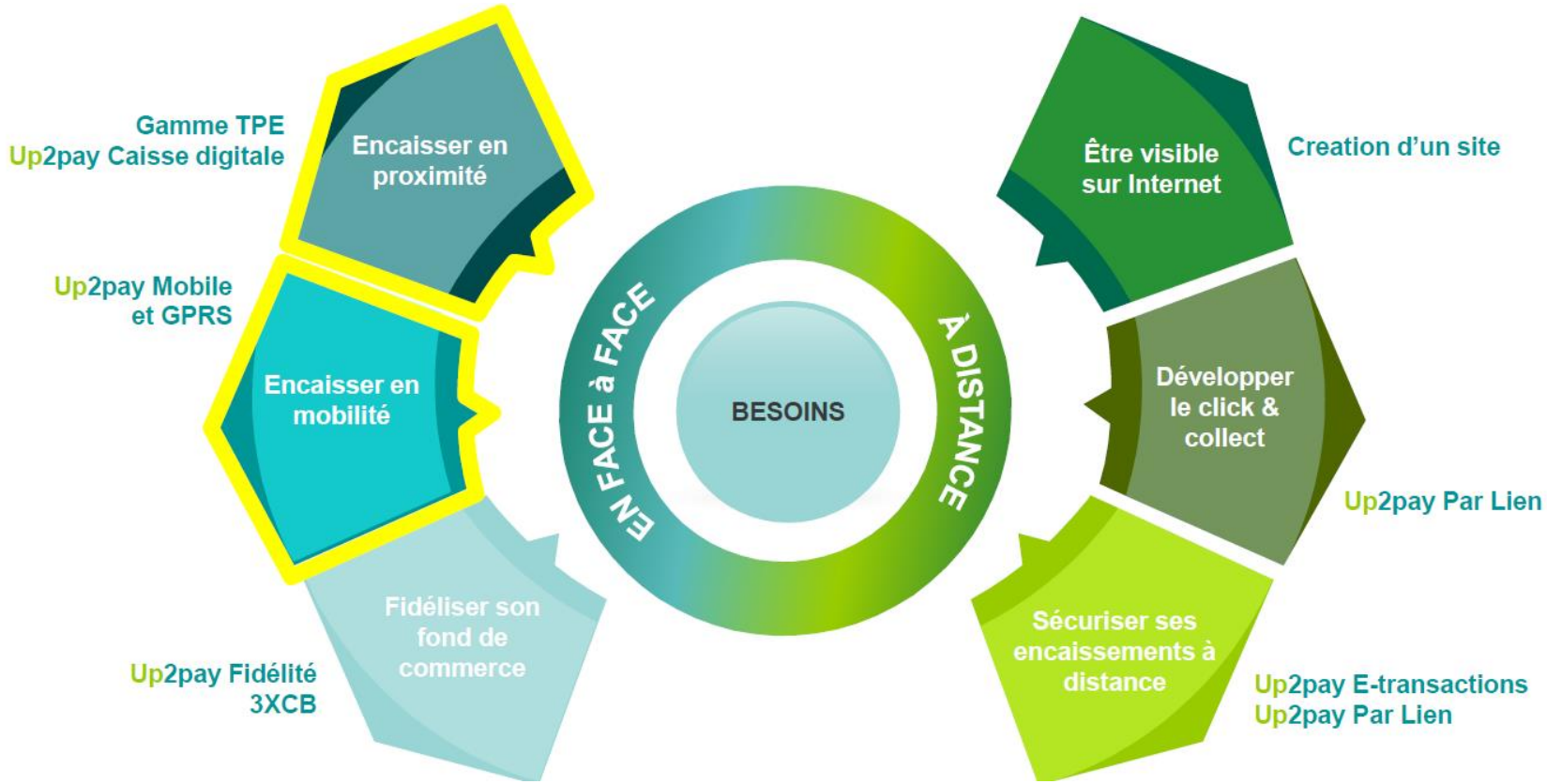
up2pay

e-Transactions

CHAMPAGNE BOURGOGNE

4) Les solutions d’encaissement à votre disposition

Quelles solutions pour quels besoins d'encaissement ?



Comment encaisser en mobilité avec up2pay mobile ?

FAÇONNEUR D'Avenir

Accès au service	**10€**	29€ (TPE inclus)	39€ (TPE inclus + accès Soft POS sur 3 smartphones)

Formule au choix

Usage : 1,75% de frais par transaction

ou

Abonnement (sans engagement de durée) : 15,50 €/mois + taux commission standard

- CB, Visa, Mastercard, AMEX* et CONECS*
- Catalogue produits
- Logiciel de caisse certifié NF525
- Matériel garanti 12 mois
- Un interlocuteur unique pour vous répondre
- Encaissements crédités à J+1

*disponible sur l'encaissement avec lecteur uniquement

CA CHAMPAGNE BOURGOGNE

Comment développer le Click & Collect/sécuriser vos paiements à distance avec up2pay par Lien ?

Façonneur d'Avenir

Le paiement à distance, simple et sécurisé, ***sans site internet ni Tpe*** , via l'envoi d'un lien de paiement sécurisé par email ou sms

1

Vous vous **connectez au portail** de l'offre **sur ordinateur ou portable** et entrez les données de la transaction
et les coordonnées de votre client pour envoi du lien

2

Votre client reçoit un **SMS avec le lien de paiement** sécurisé

3

Votre client clique sur le lien et entre ses coordonnées bancaires sur la page de paiement

4

Vous pouvez suivre votre activité et l'avancé du paiement en temps réel.

Sans abonnement — up2pay Par lien

Des frais s'appliquent pour la mise en service et pour chaque opération (voir détail ci-dessous)

Offre Access
Une solution simple sans frais d'abonnement

10€ / mois(3) — up2pay Par lien

Des frais s'appliquent pour la mise en service et pour chaque opération (voir détail ci-dessous)

Offre Standard
Une solution enrichie de services à valeur ajoutée

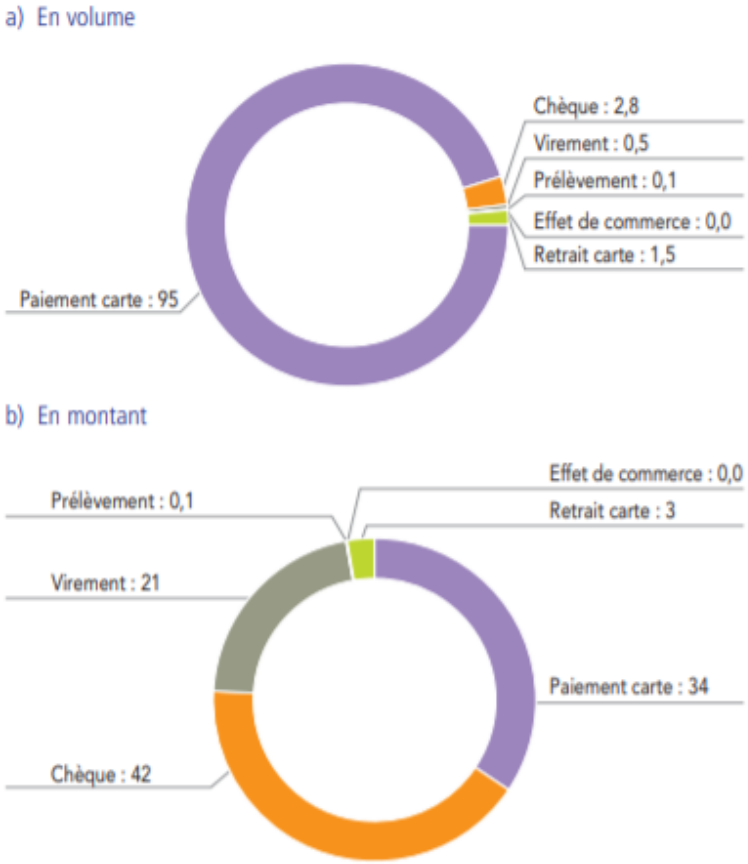
5) Les risques de fraudes

Les risques de fraude liés au paiement

« La fraude est l'utilisation illégitime d'un moyen de paiement ou des données qui lui sont attachées, ainsi que tout acte concourant à la préparation ou la réalisation d'une telle utilisation ayant pour conséquence un préjudice financier. »

Définition de l'Observation de la Sécurité des Moyens de Paiement.

L'état de la fraude aux moyens de paiement



Rapport annuel de l'Observatoire de la sécurité des moyens de paiement 2020

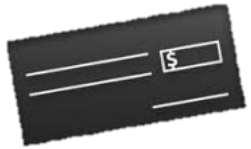
La fraude sur les transactions par carte reste maitrisée en montant mais le nombre des opérations cartes représente la majorité des transactions frauduleuses

La fraude sur les virements progresse en 2020 de manière importante du, pour l'essentiel, des fraudes par ingénierie sociale

La fraude sur le chèque se développe à un rythme soutenu alors que ce moyen de paiement est de moins en moins utilisé

La fraude aux prélèvements reste au niveau le plus faible

Les fraudes aux moyens de paiement



CHEQUES

- **Faux chèque** (perdu ou volé, fausse signature, …)
- **Chèque falsifié** (altération volontaire)
- **Chèque détourné**

Les fraudeurs « jouent » sur les délais d'encaissement et réalisent des retraits avant le retour
impayé des chèques (max 60 J).

VIREMENT

- **Escroquerie** (démarchage par internet ou autre **:** fraude à l'emploi, fraude dans le cadre d'un achat, …)
- **Détournement des coordonnées bancaires** (vol RIB, piratage, …)

CARTE

- Carte **perdue** ou volée
- Carte **non parvenue**
- Carte **falsifiée** ou contrefaite
- Numéro de carte **usurpé**
- Numéro de carte **non affecté**

Les fraudes par ingénierie sociale

Consiste à manipuler une personne en lui faisant croire qu'elle a affaire à un interlocuteur légitime, en vue d'obtenir des informations ou de lui faire réaliser une action ou une opération (exemple : un virement bancaire).

FRAUDE AU PRÉSIDENT :

Usurpation d'identité d'un des dirigeants de l'entreprise afin de convaincre un collaborateur d'effectuer un virement urgent et confidentiel vers un compte le plus souvent domicilié à l'étranger.

Indices pouvant alerter :

Email évoquant un rachat de société, contrôle fiscal… urgence de la situation, secret et confidentialité mentionné dans la conversation, flatterie ou intimidation, appel d'un tiers usurpant l'identité d'un cabinet comptable, conseiller juridique…

FRAUDE AU CHANGEMENT DE COORDONNÉES BANCAIRES :

Usurpation d'identité d'un fournisseur, du bailleur ou de tout autre créancier pour demander un changement de coordonnées bancaires afin de détourner les prochains règlements de loyers ou de factures, paiement des salaires.

Indices pouvant alerter :

Email avec les nouvelles coordonnées bancaires avec des caractéristiques de messagerie très proches de celles de l'interlocuteur habituel.

FRAUDE AU TEST INFORMATIQUE :

Usurpation d'identité d'un prestataire informatique de l'entreprise, voire de la banque, afin de demander l'exécution d'un « virement test » vers un compte domicilié à l'étranger.

Indices pouvant alerter :

Un interlocuteur propose une assistance sur les outils de paiement, demande de connexion par l'intermédiaire d'un hyperlien, demande de virement de test.

Les fraudes par Internet

PHISHING

Récupération de vos informations confidentielles grâce à un courrier reprenant la charte graphique d'une société

SPAM

Courrier support pouvant être utilisé :

- Canular
- Escroquerie
- Logiciel malveillant
- Phishing

MALWARES

Logiciel qui a été installé à votre insu sur votre ordinateur.
But : vente / vol d'informations / chantage / …

ESCROQUERIE

Courriel indésirable qui va **chercher à abuser de votre crédulité ou de votre compassion** pour vous soutirer de l'argent

6) Les techniques permettant de s’en prémunir

Les techniques permettant de s'en prémunir

SOYEZ RESPONSABLES

- **Soyez attentifs** à vos relevés de compte
- Consultez régulièrement les **consignes de sécurité** communiquées par votre banque
- **Assurez-vous que votre banque dispose de vos coordonnées** afin de vous contacter rapidement en cas d'opérations douteuses
- **Sensibilisez** vos collaborateurs et fournisseurs

SOYEZ ATTENTIFS

- Lors d'un paiement à distance vérifiez la **cohérence des informations fournies**
- **Méfiez-vous du contenu des courriers reçus et des demandes d'informations personnelles**

SACHEZ REAGIR

- **Instrument de paiement perdu ou volé :**

Faîtes immédiatement opposition

- **Activités suspectes sur vos moyens de paiement :**

Contactez nous

- **Anomalies sur votre relevé de compte :**

N'hésitez pas à faire opposition afin de vous prémunir contre toute nouvelle tentative

SACHEZ VOUS PREMUNIR

- Assurez-vous de votre enrôlement pour bénéficier de **l'authentification forte**
- **Assurez-vous afin de vous prémunir en cas de fraude**
- **Mettez en place des doubles signatures, des plafonds, des listes fermées pour vos opérations via EDI**

Rapport annuel de l'Observatoire de la sécurité des moyens de paiement 2019

Les techniques permettant de s'en prémunir

SACHEZ VOUS PREMUNIR

Authentification forte

3D SECURE

3D-Secure est un dispositif permettant **d'authentifier le porteur d'une carte de paiement de manière renforcée**.

SÉCURIPASS

Cliquez ici

C'est la **solution d'Authentification Forte du Crédit Agricole** disponible dans l'application Ma Banque qui permet de **garantir que le client est bien à l'origine d'une opération**

SECURICODE

Le SécuriCode (ou SMS Renforcé) **est une alternative à SécuriPass, pour authentifier les achats en ligne** et qui permet de **garantir que le client est bien à l'origine d'une opération**

Assurances

CYBERPROTECTION

Avec l'assurance Cyber Protection vous bénéficiez d'une **assistance à la gestion de crise en cas de cyber-attaque.**

- Assistance à la gestion de crise en cas de cyber-attaque
- Indemnisation des dommages subis par votre entreprise
- Responsabilité civile en cas de dommages causés aux tiers

Sécurité des données

RGPD

- Renforcer le **droit des personnes**
- **Responsabiliser les acteurs** traitant des données
- Créer une vrai synergie

ALERTES BANQUE

En cas de doute votre banque vous contacte pour vérification via un contre appel du signataire déclaré dans notre système d'information

Merci pour votre écoute.

A vos questions !

Nurten KARAKOL
nurten.karakol@ca-cb.fr
06.78.24.99.15