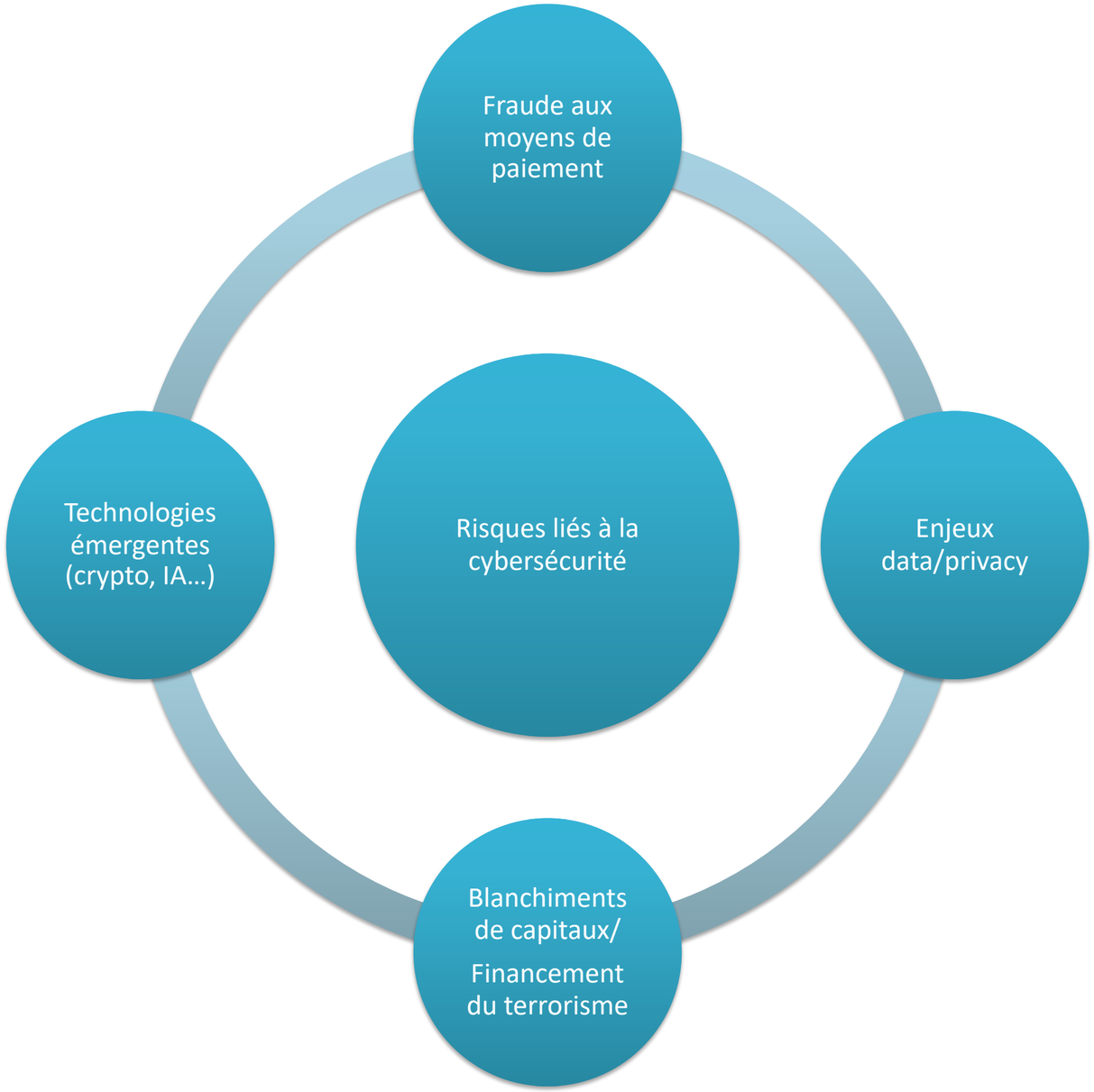
Partelya CONSULTING

Mercatel
Pour le Commerce et la Distribution

Sécurité des paiements :
Focus sur les nouveaux modes opératoires des fraudeurs

WEBINAR 18 juin 2024

Les enjeux de la sécurité des paiements



Sécurité des paiements : quel cadre réglementaire ?

- MiCA (Markets in Crypto-Assets)
- AI Act (intelligence artificielle)
- Evolutions en termes de cybersécurité

- Authentification forte
- Sécurité instant payment
- Evolution de la lutte contre la fraude

- Evolution vers une approche « par les risques »
- Vigilance sur les moyens de paiement considérés comme « à risque » (espèces, prépayé)

- Notion de consentement
- Notion « d'intérêt légitime »
- Enjeux de la localisation des données

Les réalités de la sécurité des paiements : quelques chiffres clés en France

- En France, l'Observatoire de la sécurité des moyens de paiement (OSMP) a relevé dans son rapport 2022 une baisse de 20% de la fraude sur le paiement sur Internet du fait du passage à l'authentification forte
- Ce constat positif est confirmé dans le rapport 2023 de l'OSMP : baisse générale de la fraude de 4% en volume et en valeur et une contraction du taux de fraude sur la carte de paiement à 0,053%, soit « le niveau le plus bas jamais enregistré »
- Néanmoins, des marges de progression existent, comme « un usage plus ciblé et parfois plus conforme des exemptions à l'authentification forte »

- **… mais une vigilance accrue des régulateurs face aux nouvelles formes de fraude**
- L'exemple du virement : hausse annuelle des montants de fraude (+9%) selon le rapport 2023 de l'OSMP et près de 70% du préjudice financier résultant d'attaques sur les virements initiés par les particuliers et les entreprises => travaux pour identifier les mesures complémentaires de lutte contre la fraude au virement initiés en septembre 2023 par l'OSMP

- *Source : www.banque-france.fr*

Nouveaux modes opératoires des fraudeurs : quelles pratiques?

Fraude au « faux conseiller »

Fraude « triangulaire »

Fraude « au retour »

Usurpation d ’identité

Fausses offres d’investissement/d’emploi

Nouveaux modes opératoires des fraudeurs : quelles pratiques?

Focus sur la situation en France* :

- En 2023, 3,7 millions visiteurs ont pu découvrir les 500 contenus disponibles sur Cybermalveillance.gouv.fr dont la fréquentation se stabilise.
- En parallèle, 280 000 demandes d'assistance ont été enregistrées via l'outil de diagnostic en ligne, avec une augmentation de +13 % pour les particuliers et +17 % de la part des collectivités », indique l'organisation.
- **Le hameçonnage ou « phishing »** reste la principale menace pour toutes les catégories de publics en 2023, avec près de 1,5 million de consultations des contenus sur les principales formes de hameçonnage (plus de 50 000 particuliers et professionnels ont recherché une assistance sur cette menace qui se diversifie et se sophistique.
- Déjà identifiées en 2022, **les escroqueries au faux conseiller bancaire** sont le phénomène de 2023 (+78% vs 2022) avec 80 000 consultations de l'article en ligne.
- Autre menace majeure : **le piratage de compte**, qui prend la deuxième place toutes catégories de publics confondus.
- En outre, avec 2 782 demandes d'assistance, **les attaques par rançongiciel** ont atteint un niveau record depuis quatre ans, tous publics confondus (+12%).
- **L'arnaque au faux support technique**, quant à elle, repose sur un mode opératoire toujours plus agressif et suscite 140 000 consultations de l'article sur le sujet.
- Enfin, **les programmes malveillants (virus)** font un retour en force et se positionnent à la quatrième place des causes principales de demandes d'assistance chez les particuliers.

** Rapport Cybermalveillance.gouv.fr, présenté en mars 2024*

Nouveaux modes opératoires des fraudeurs : pistes d'action des acteurs en place

Exemples : biométrie, identité numérique, IA

Travail collaboratif

Solutions technologiques

Information et pédagogie

Exemple : Travaux de l'OSMP (recommandations sur le remboursement des clients, GT en cours sur la fraude au virement, GT veille en cours sur les scoring de fraude)

Exemples : En France, campagnes de la FBF sur la protection des données et recommandations de Cybermalveillance.gouv.fr sur un usage Web sécurisé + actions de sensibilisation menées au Portugal via les médias grand public sur les nouveaux cas de fraude au paiement

Nouveaux modes opératoires des fraudeurs : pistes d'action des acteurs en place

En France, CharteCyber signée fin 2023 par 83 entités*

- ✓ Faire de la cybersécurité une priorité stratégiques adaptée aux risques pouvant peser sur les activités
- ✓ Nommer un « référent cybersécurité » en charge de porter le sujet en interne
- ✓ Sensibiliser l'ensemble des collaborateurs aux risques cyber et aux enjeux pour l'organisation
- ✓ Former ses collaborateurs aux bonnes pratiques et réflexes de cybersécurité
- ✓ Anticiper les cyberattaques en élaborant des plans de secours adaptés et à en vérifier périodiquement la pertinence par des exercices
- ✓ Evaluer régulièrement le niveau d'exposition aux risques cyber des différentes composantes de son système d'information afin d'en décliner les mesures correctrices nécessaires
- ✓ S'appuyer, autant que de besoin, sur des fournisseurs et prestataires de cybersécurité à la compétence reconnue et attestée par des labels et certifications
- ✓ Promouvoir autant que possible auprès de l'ensemble de ses parties prenantes (clients, administrés, fournisseurs, partenaires…) les enjeux liés à la cybersécurité et les bonnes pratiques à observer

*Cybermoi/s 2023 : 83 entités s'engagent à travers la signature de la « CharteCyber » et lancent un appel à mobilisation générale - Assistance aux victimes de cybermalveillance

Nouveaux modes opératoires des fraudeurs : pistes d'action des acteurs en place

Au Portugal, deux solutions dédiées à la sécurité des paiements lancées par Banco de Portugal en mai/juin 2024*

- Solution de confirmation de l'identité du bénéficiaire lors de virements classiques, instantanés ou de prélèvements, avant l'opération (disponible depuis le 20 mai 2024) :

- La solution inclut ainsi deux fonctionnalités : la confirmation d'un bénéficiaire unique, qui sera proposée aux utilisateurs de services de paiement ; et la confirmation d'un bénéficiaire groupé, soit la confirmation d'un ou plusieurs compte(s) de paiement via la validation de pairs NIF (ou numéro d'identification fiscale)/IBAN ou NIPC (ou numéro d'identification de personne collective)/IBAN, qui sera utilisable par les entreprises lors des versements de salaires, du paiement des fournisseurs ou du processing de prélèvements.

- Solution « SPIN », disponible à partir du 24 juin 2024, visant à permettre aux clients particuliers l'utilisation du numéro de téléphone mobile, et aux clients entreprises du numéro d'identification de personne collective (NIPC), au lieu de l'IBAN, dans le cadre de virements instantanés.

Ces services seront proposés via l'ensemble des canaux (homebanking, applications bancaires, agences...) aux prestataires de services de paiement participant au Système de Compensation Interbancaire (SICOI), qui assure le processing pour la totalité des opérations de paiement réalisées par les particuliers et les entreprises au Portugal.

**www.bportugal.pt*

Sécurité des paiements : focus sur les nouveaux modes opératoires des fraudeurs

- Comment évolue la fraude en matière de paiement en France et en Europe? Quelles sont les nouvelles pratiques en termes de fraude?
- Quelles sont les actions des acteurs en place (en termes de recommandations, initiatives…)?
- Comment vont évoluer les dispositions relatives à la lutte contre la fraude dans le nouveau cadre réglementaire européen?
- Quelle place pour les technologies émergentes dans cette politique en matière de sécurité des paiements?
- Quelles évolutions sectorielles des travaux, et quelle place pour les acteurs « connexes » (retailers, telcos…)?

Débat

Présentation des panélistes

Julien LASALLE

Directeur de la surveillance des moyens de paiement scripturaux
BANQUE DE FRANCE

Bertrand PINEAU

Délégué Général
MERCATEL

Olivier SCHERSCHEL

Directeur des filières flux, échanges, et sécurité des paiements
CREDIT AGRICOLE PAYMENT SERVICES

Modératrice

Andréa TOUCINHO

Directrice Etudes, Prospective et Formations
PARTELYA CONSULTING

Keynote : Focus sur un exemple européen => Le Portugal

Vinay Pranjivan

Senior Economist, Advisor in consumer protection for financial services

DECO – Associação portuguesa para a defesa do consumidor

Partelya Consulting en quelques mots

Fondé en 2008, Partelya Consulting est un cabinet de conseil innovant spécialisé en Monétique, Moyens de Paiement et Systèmes d'Informations associés, qui a contribué sur plusieurs projets d'envergure à la mise en œuvre de nouvelles solutions monétiques, auprès d'entreprises et de grandes institutions financières et industrielles.

Andréa TOUCINHO

Directrice Études, Prospective & Formations
andrea.toucinho@partelya.com | 06 17 19 55 21