|  |  |
| --- | --- |
| The International Teleocmmunication Union - Connecting the World. | **Union internationale des télécommunications****Bureau de la Normalisation des Télécommunications** |
|  |  | Genève, le 10 mars 2025 |
| **Réf.:** | **Circulaire TSB 31**Manifestations du TSB/VM | – Aux Administrations des États Membres de l'Union;– À l'État de Palestine (Résolution 99 (Rév. Dubaï, 2018));– Aux Membres du Secteur de l'UIT-T;– Aux Associés de l'UIT-T;– Aux Établissements universitaires participant aux travaux de l'UIT**Copie:**– Aux Présidents et Vice-Présidents des Commissions d'études;– Au Directeur du Bureau de développement des télécommunications;– Au Directeur du Bureau des radiocommunications |
| Tél.: | +41 22 730 6356 |
| Télécopie: | +41 22 730 5853 |
| Courriel: | tsbevents@itu.int |
| **Objet:** | **Webinaire sur les services financiers numériques, épisode 2 – "*Sécuriser les applications de paiement sur mobile – Partie 1*" (entièrement virtuel, 26 mars 2025)** |

Madame, Monsieur,

1 J'ai l'honneur de vous inviter au webinaire en direct sur le thème "***Sécuriser les applications de paiement sur mobile – Partie 1***", qui se déroulera **en ligne** le **26 mars 2025 de 14 h 00 à 15 h 00 CET**. Ce webinaire, le deuxième d'une série consacrée à la sécurité des services financiers numériques, est organisé dans le cadre des activités du [laboratoire de sécurité des services financiers numériques (DFS) de l'UIT](https://www.itu.int/en/ITU-T/dfs/seclab/Pages/default.aspx#/fr).

2 La croissance rapide des services financiers numériques (DFS) a fait des applications de paiement sur mobile une cible de choix pour les cyberattaques. Les applications DFS sur mobile, qui fonctionnent sur diverses plates-formes, sont confrontées à des problèmes particuliers en matière de sécurité, tels que l'authentification non sécurisée, les fuites de données et les attaques de logiciels malveillants. Il est essentiel de remédier à ces risques potentiels pour maintenir la confiance des utilisateurs et assurer la sécurité globale de l'écosystème des services DFS.

3 La première partie de ce webinaire en deux parties porte sur des conseils techniques et sur les bonnes pratiques en matière d'exigences minimales de sécurité pour les applications DFS sous Android. Les participants découvriront un modèle de bonnes pratiques en matière de sécurité des applications, issu de la Recommandation [UIT-T X.1150](https://itu.int/rec/T-REC-X.1150-202403-I/en) intitulée "*Cadre d'assurance de la sécurité pour les services financiers numériques*", et conçu pour être intégré par les régulateurs des services DFS dans leurs politiques de sécurité relatives aux applications. Cette approche permet également de donner des orientations utiles aux fournisseurs de services DFS dans le cadre de leurs processus de développement. Au cours de cette session, les participants se familiariseront avec les bonnes pratiques en matière d'exigences minimales de sécurité des applications sur mobile et recevront des conseils techniques en vue d'améliorer la résilience des applications de paiement sur mobile et de protéger les utilisateurs contre les nouvelles menaces.

À partir de ces connaissances de base, la première partie de cet atelier sera consacrée à la présentation de la méthodologie du [laboratoire de sécurité des services DFS de l'UIT](https://www.itu.int/en/ITU-T/dfs/seclab/Pages/default.aspx#/fr), fondée sur le projet ouvert concernant la sécurité des applications web (OWASP) 2024, en particulier pour valider la conformité des applications DFS sur mobile sous Android aux bonnes pratiques établies en matière d'exigences minimales de sécurité pour les applications DFS. La méthodologie comprend des tests en laboratoire et des stratégies d'atténuation pour garantir une sécurité robuste. Les principales normes et bonnes pratiques du secteur seront présentées tout au long de la session, ce qui donnera aux participants un aperçu complet des tests de sécurité pour les applications DFS sous Android.

4 Les participants approfondiront leurs connaissances sur les points suivants:

– Risques de sécurité pouvant menacer les applications de paiement sur mobile sous Android.

– Bonnes pratiques en matière d'exigences minimales de sécurité pour les applications DFS adaptées de la Recommandation [UIT-T X.1150](https://itu.int/rec/T-REC-X.1150-202403-I/en).

– Méthode du laboratoire de sécurité des services DFS de l'UIT visant à valider la conformité des applications DFS sous Android aux bonnes pratiques en matière d'exigences minimales de sécurité pour les applications DFS.

5 Le webinaire s'adresse aux spécialistes des télécommunications, des services financiers, des technologies financières, de la cybersécurité et des organismes de réglementation qui sont directement concernés ou touchés par la sécurité des services DFS.

6 Afin de faciliter les discussions collaboratives avec les régulateurs, les fournisseurs de services DFS et les fournisseurs de télécommunications, et de contribuer à la poursuite de l'élaboration des bonnes pratiques en matière de sécurité des services DFS avant et après le webinaire, les participants sont invités à rejoindre les [plates-formes d'échange des connaissances de l'UIT en matière de sécurité des services DFS](https://www.itu.int/en/ITU-T/dfs/Pages/share-platform.aspx) sur Slack et GitBook.

7 Vous trouverez des informations détaillées sur le webinaire à l'adresse suivante: [https://itu.int/en/ITU-T/webinars/dfs/20250326](https://www.itu.int/en/ITU-T/webinars/dfs/20250326/Pages/default.aspx#/fr).

8 Afin de permettre aux organisateurs de prendre les dispositions nécessaires concernant l'organisation de l'atelier, je vous saurais gré de bien vouloir vous inscrire dès que possible à l'adresse suivante: <https://itu.zoom.us/webinar/register/WN_UIov8n3hRNC9A5X1j9Hw4w#/registration>.

Veuillez agréer, Madame, Monsieur, l'assurance de ma considération distinguée.

Seizo Onoe
Directeur du Bureau de la normalisation
des télécommunications