|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| The International Teleocmmunication Union - Connecting the World. | | **International telecommunication union**  **Telecommunication Standardization Bureau** | |  | |
|  | | | Geneva, 30 October 2020 | | |
| **Ref:** | | | **TSB Circular 278** | | **To:**  - Administrations of Member States of the Union;  - ITU-T Sector Members;  - ITU-T Associates;  - ITU Academia  **Copy to:**  - The Chairmen and Vice-Chairmen of Study Groups;  - The Director of the Telecommunication Development Bureau;  - The Director of the Radiocommunication Bureau;  - The Directors of ITU Regional Offices | | |
| **Contact:** | | | Vijay Mauree | |
| **Tel:** | | | +41 22 730 5591 | |
| **Fax:**  **E-mail:** | | | +41 22 730 5853  [tsbevents@itu.int](mailto:tsbevents@itu.int) | |
| **Subject: Insights on Digital Financial Services during COVID-19 Webinar Series   (Episode 12: Fully Virtual Meeting,** **10 November 2020)** | | | | | |

Dear Sir/Madam,

1 The International Telecommunication (ITU) is organizing the twelfth episode of the webinar series on [Insights on Digital Financial Services (DFS) during COVID-19](https://www.itu.int/en/ITU-T/webinars/Pages/dfs.aspx) on **10 November 2020 from 15h00 - 16h30 CEST.** This episode will discuss the topic **mitigating infrastructure vulnerabilities for digital finance**.

2 The session will focus on the vulnerabilities in the underlying telecom infrastructure such as SS7 as well as SIM cards and their potential threat on digital financial services and best practices for mitigating them. The world of digital finance is hugely dependent on telecommunications infrastructure and services. Due to the dominance of feature phones among users in developing economies, which comprise the majority of digital finance end-users, the channels that the end‑user communicates with the digital financial services provider are mostly Unstructured Supplementary Service Data (USSD), Short Messaging Service (SMS) and Sim Tool Kit (STK). USSD and SMS as means of communication have long been known as susceptible to attack and have many published vulnerabilities. The SIM card of the phone is another security vulnerability point that needs special attention as well. For instance, SIMs which are vulnerable to Simjacker could be vulnerable to an attack that contains a series of SIM Toolkit (STK) instructions specifically designed to be passed on to the SIM Card within the device. Exploiting these vulnerabilities enables attackers to commit fraud and steal funds from unsuspecting victims, who in in most cases are unaware their account is being compromised or hacked.

4 Participation in the webinar is open to ITU Member States, Sector Members, Associates and Academic Institutions and to any individual from a country that is a member of ITU who wishes to contribute to the work. This includes individuals who are also members of international, regional and national organizations.

5 All relevant information pertaining to the webinar (speakers, registration link, remote connection details) will be made available here: <https://www.itu.int/en/ITU-T/webinars/20201110/Pages/default.aspx> . The website will be regularly updated as new or modified information becomes available. Participants are requested to check periodically the webpage for new updates. You may also check out the previous episodes on the main landing page found [here](https://www.itu.int/en/ITU-T/webinars/Pages/dfs.aspx).

Yours faithfully,

Chaesub Lee  
Director of the Telecommunication  
Standardization Bureau