|  |  |  |
| --- | --- | --- |
| The International Teleocmmunication Union - Connecting the World. | **国 际 电 信 联 盟****电信标准化局** |  |
|  | 2020年10月30日，日内瓦 |
| **文号：** | **电信标准化局第278号通函** | **致：**- 国际电联各成员国主管部门；- ITU-T部门成员；- ITU-T部门准成员；- 国际电联学术成员 |
| **联系人**： | Vijay Mauree |
| **电话：****传真：** | +41 22 730 5591+41 22 730 5853 |
| **电子邮件：** | tsbevents@itu.int | **抄送：**- 各研究组正副主席；- 电信发展局主任；- 无线电通信局主任；- 国际电联各区域代表处主任 |
| **事由：** | **在新冠肺炎大流行期间举办的“数字金融服务见解”系列网络研讨会（第12期：完全虚拟式会议，2020年11月10日）** |

尊敬的先生/女士：

1 国际电信联盟（ITU）正在组织于**2020年11月10日（中欧时间）15时 — 16时30分**举办 [**新冠肺炎大流行期间的“数字金融服务（DFS）见解”**](https://www.itu.int/en/ITU-T/webinars/Pages/dfs.aspx)系列网络研讨会第十二期。此期将讨论**缓解数字金融基础设施漏洞**的议题。

2 会议将重点讨论诸如7号信令（SS7）和SIM卡之类的基础电信基础设施中的漏洞，及其对数字金融服务的潜在威胁和缓解这些风险的最佳做法。数字金融世界极大地依赖于电信基础设施和服务。由于发展中经济体的用户大多使用功能手机，而在那里又有大多数数字金融终端用户，因此终端用户与数字金融服务提供商进行通信的渠道主要是非结构化补充服务数据（USSD）、短消息服务（SMS）和芯片卡工具包（STK）。长期以来，USSD和SMS作为一种通信手段一直很容易受到攻击，并且存在许多已公布的漏洞。手机的SIM卡是另一个安全漏洞点，也需要特别注意。例如，容易受到SIM卡攻击（Simjacker）的SIM卡可能会受到由包含一系列专门设计为传到设备内SIM卡上的芯片卡工具包（STK）指令的攻击。攻击者可以利用这些漏洞进行欺诈，并且从毫无戒心的受害者那里窃取资金，而这些受害者在大多数情况下都不知道自己的账户受到了攻击或者已经被黑。

4 国际电联成员国、部门成员、部门准成员和学术机构以及有意参加此工作的来自国际电联成员国的任何个人均可参加这些网络研讨会。在此包括作为国际、区域和国家组织成员的个人。

5 与网络研讨会有关的所有相关信息（演讲人、注册链接、远程连接细节等）均将在此处提供：<https://www.itu.int/en/ITU-T/webinars/20201110/Pages/default.aspx>。随着新信息或修改信息的提供，此网站将定期更新。请参会者定期查看网页上是否有新的更新。您也可以在[此处](https://www.itu.int/en/ITU-T/webinars/Pages/dfs.aspx)的主要登录页面上查看以往各期。

顺致敬意！

电信标准化局主任
李在摄