Banks struggle over 'growing complaints'

More pressure on bank staff who struggle to handle increasing complaints after online frauds

(Continued from Page 1)

Staff at all commercial banks across the Kingdom now find it challenging to handle the rising number of complaints from customers after fraudulent online money transfers.

"It's not easy to handle the increasing number of complaints, and we feel embarrassed to face our customers as we don't have genuine answers to deal with them," a bank official told *The Daily Tribune*.

> **It's not easy to handle the increasing number of complaints, and we feel embarrassed to face our customers as we don't have genuine answers to deal with them**
>
> A BANK OFFICIAL

> **I don't understand how money is stolen even after deactivating many accounts. The disease has progressed, and no treatment seems to be working now**
>
> AN IT PROFESSIONAL AND CYBERSECURITY EXPERT

> **The hackers deploy their highest social engineering skills to get information, which is supposed to be kept secret, private and never shared, from their victims**
>
> ALI BESHARA, THE HEAD OF INFORMATION SECURITY AND RISK MANAGEMENT AT THE BENEFIT COMPANY

> **There is no automated system to de-link with the bank account upon installing or deactivating the app, which is worsening the situation, allowing scammers to steal more and more**
>
> IT PROFESSIONAL

Banks, money wallet apps should take more responsibility

On the other hand, an IT professional and cybersecurity expert said the Financial Institutions should collectively form a unit to tackle these online scammers. "In many developed countries, most banks and digital wallets compensate the customers for the lost amounts to scammers. And they have earmarked millions in this regard. In Bahrain also, I expect the banks to take more responsibility and at least share the risk along with the customers."

"I don't understand how money is stolen even after deactivating many accounts. The disease has progressed, and no treatment seems to be working now."

Hacking or buying accounts!

He said he had discussed the issue with many top bank officials. "What I could learn is that the scammers are either hacking the bank accounts or 'buying accounts from expatriates who are leaving the Kingdom'. The second one sounds quite strange, but I was told it's a reality, and 'these bought accounts' are used as the focal points to carry out scams."

"Many money wallets offer few procedural difficulties to make customers happy, which is not the right thing. Suppose a lengthy course of action ensures safety and keeps the scammers at bay. In that case, it must be adopted as the customers are now willing to bear procedural difficulties for keeping their money safe in the accounts."

He asked why the money wallets are permitting money transfers even after uninstalling and deactivating their apps. "There is no automated system to de-link with the bank account upon installing or deactivating the app, which is worsening the situation, allowing scammers to steal more and more."

Picture for representation only

> **The Central Bank of Bahrain, many a time, has carried out campaigns and circulated messages alerting over the possibility of falling victims to online fraudsters.**

The Daily Tribune spoke to many victims who have lost their money. And all of them said they haven't "got a fils back".

'Social engineering'

In an exclusive interview, Ali Beshara, the Head of Information Security and Risk Management at The BENEFIT Company, which owns the popular online money transfer app BenefitPay, attributed the rise in online fund transfer scams to lack of alertness from the part of users.

Mr Beshara also pointed out that this kind of cybercrime involves 'social engineering' - a term used by information security professionals to describe the action from the part of hackers.

"The hackers deploy their highest social engineering skills to get information, which is supposed to be kept secret, private and never shared, from their victims.

"It is in these situations, the hacker gets the password of the BenefitPay application and the OTP (One-Time Password), which is sent to the user in case of device change and money transfer," he had said.

Mr Beshara stressed that users are almost totally protected if they don't click on links sent by fraudsters or share passwords with strangers.

Target through calls

Scammers generally target victims by making calls to their mobile phones or sending SMSs. Upon receiving the call or SMS, data is leaked and money is either transferred to other accounts or used for purchasing various goods online through the payment app already installed on the mobile phone.

A few weeks ago, *The Daily Tribune* carried a report about fraudsters targeting the online banking and financial transaction network in the Kingdom.

The published article carried the plight of one Bangladeshi national, one Pakistani national, and an Indian businessman, who lost nearly BD1,500 to the scammers.

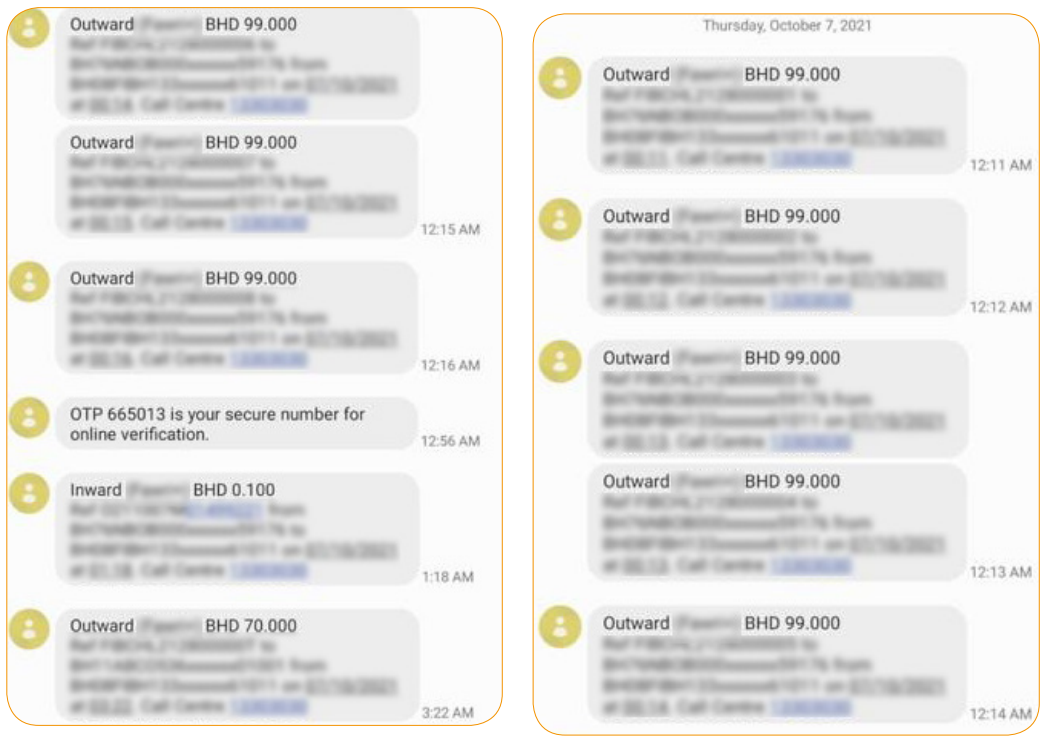
Stop responding to calls and text messages from strangers

Most victims have launched a complaint with the police department, pleading for an intense probe into the matter.

Cyber security experts have always highlighted the need to protect Unified Payment Interface (UPI) and online transactions from scammers in light of increasing online payments.

They include not responding to calls and text messages from strangers and putting up different passwords on different accounts and UPI apps.

The Central Bank of Bahrain, many a time, has carried out campaigns and circulated messages alerting over the possibility of falling victims to online fraudsters.



A mobile screenshot showing the flood of money transfers from Ajeesh's account. The scammer brilliantly chose the amount BD99 as OTP is required for transferring BD100 as well as higher amounts.

Court case

Drug peddler loses appeal, Court confirms 10-year jail term, BD5,000 fine

- **The accused was caught red handed with 210 grams of narcotic substances and 32 narcotic medical tablets**
- **Police set the trap by calling the suspect through a source offering to buy Shabu worth BD1000**
- **The accused, however, denied the charges levelled against him**

TDT | Manama

Representative picture

A 30-year-old drug peddler has had his 10-year prison term confirmed by the Court of Cassation, rejecting an appeal filed against the verdict.

The Court also confirmed a 5,000 dinar fine awarded to the appellant for selling Shabu, hashish and Marijuana in the Kingdom.

Court files say police confiscated the drugs from his home, following a court order.

The Public Prosecution charged the suspect with possessing psychoactive drugs such as hashish and methamphetamine to sell. The prosecution also charged him with abuse of hashish and methamphetamine.

Incidents leading to the case occurred with the security authorities receiving a tip-off that a person having prior convictions had obtained narcotic substances.

> **Incidents leading to the case occurred with the security authorities receiving a tip-off that a person having prior convictions had obtained narcotic substances.**

After confirming the information, the public prosecution issued a warrant to detain him and search his residence.

Investigators managed to arrest him red-handed with the help of a confidential source.

Police set the trap by calling the suspect through the source and offering to buy Shabu worth BD1000.

The source also offered to pay him in advance, to which the suspect agreed.

Unsuspecting the trap set, the suspect arrived in his car as agreed to the meeting place and called the undercover agent to meet him at the parking.

The suspect also handed out two bags of Shabu after taking the money, which the police photographed from another vehicle.

After completing the deal, the suspect drove off quickly. He was then tracked down by the police and arrested near his residence.

The police then searched his house and found a black bag with 210 grams of narcotic substances and 32 narcotic medical tablets.

The accused, however, denied the charges levelled against him and claimed that the drugs belonged to the confidential source.