- Computer crimes / Internet shopping

Always put your alert status on a high

A simple, yet effective, way to survive everyday cybercrimes

Manila Bulletin · 28 Dec 2021 · B-10 · (Art Samaniego, Jr.)*

The popularity of digital payments helped many Filipinos to access goods and services while in quarantines, isolations, and on-and-off lockdowns during the pandemic. It also made many businesses continue to function even with the global slowdown due to fear of the virus. Work-from-home has become much easier for parents, and online learning is more comfortable for students because of the safety digital payment offers. Also, with online payments, users can pay bills for credit cards, electricity, water, and more. Online shopping, grocery shopping, and paying for food deliveries have become convenient because of digital payment solutions. This technology also answers the consumers' concern about health risks associated with handling paper bills and coins when paying for goods and services.

With people seeing the beneΣts of digital payments, users have grown exponentially. The increase of usage and transactions across all spectrums of the society attracted legitimate users but also got the attention of opportunists and scammers who are creatively ramping up their methods to trick users into giving up their money via money transfer or taking over accounts via phishing.

I've been a long-time e-wallet user and I always get attempts from cybercriminals to scam me. The attempts are, however, not exclusive to any digital payments platform. Majority regularly get scam and phishing attacks from the internet bad guys.

Based on my experience, two types of scams are commonly done which every user needs to know about.

Swindling

Just recently, fake job offers flooded the SMS inbox of many users. The purpose of the scam is not to get your bank details but to make you willingly send money to a bank account the cybercriminals provided. Believing that they are investing in legitimate part-time job opportunities, victims unknowingly send thousands of pesos to the scammers. Other forms of swindling include fake sellers who ask you to pay via digital payment methods and then disappear without any trace, ghosting you on social media. Fake donation drives and hacked friends' accounts where scammers would take advantage of your goodness by asking for money is also a form of swindling.

Account takeover

This scam happens when cybercriminals gain access to your username and password. Once you log in via a fake website, the fraudsters will record and use your credentials. They could then steal all your money once they have your login details. While there are many ways the scammers get our details, phishing is the most common reason why account take over happens. Cybercriminals would send emails, SMS, and private messages with fake landing pages pretending to be from GCash. Sometimes, these criminals would also use fake social media proΣles and pretend to be from payment platforms.

If you got scammed because of these methods, it's time to reevaluate your priority list and put a focus on your security. Truth be told, it is beyond your payment platform's control if you share your private account details with scammers. Having a lack of awareness is the Σrst thing we need to address and break in order to stop these cybercrimes.

Even as a cybersecurity advocate, I still get a lot of scamming and fraud attempts myself. These criminals obviously have no idea that I spend most of my time exposing them and encouraging other people to take their security seriously. I've been using GCash now for a long time, the most popular digital payment platform in the country,

and aside from making their platforms secured, they are calling to all users like you and me to #GCheckMuna and fight the fraudulent activities by following the easy-to-remember GChecklist reminders:

01

Never share MPIN or OTP - Scammers often pose as a GCash representative or a friend to trick you into giving your OTP. Remember your MPIN and OTP are only for you. In some situations, scammers try to look over their target's shoulder to get their MPIN or OTP. To avoid this, GCash has a feature that allows you to login using your Σnge-rprint or face. Enable your biometrics login so that you can keep your MPIN safe even when you're in a public space.

02

Only do actions via the app - When asked to verify or login, only do it with the GCash app. Some scammers use similar-looking phishing sites to trick you into giving your information. Always keep tabs on all your transactions, GCash now has real time transaction history, so you can Σnd discrepancies or unauthorized transactions and report it right away.

03

Be careful of who you transact with - Always read seller reviews and research the product you are buying and who you are buying it from. There are cases when fraudsters would pretend to be your friends in need. Don't send any-thing yet, be sure that you know the person who sent the message. A simple call to verify is all it takes to save you from the scam.

04

Go to GCash Channels For all concerns, go to the GCash Help Center. Do not post your inquiries on social media, and GCash will never send a personal message to you to address concerns.

Remember that being a victim of cybercrime not only puts us in danger but also the people we have engaged with on social media, including our families and friends. Be more mindful of our own account safety while using the internet. Follow the tips on securing digital payments and social media accounts for all of us to have a safe online experience.