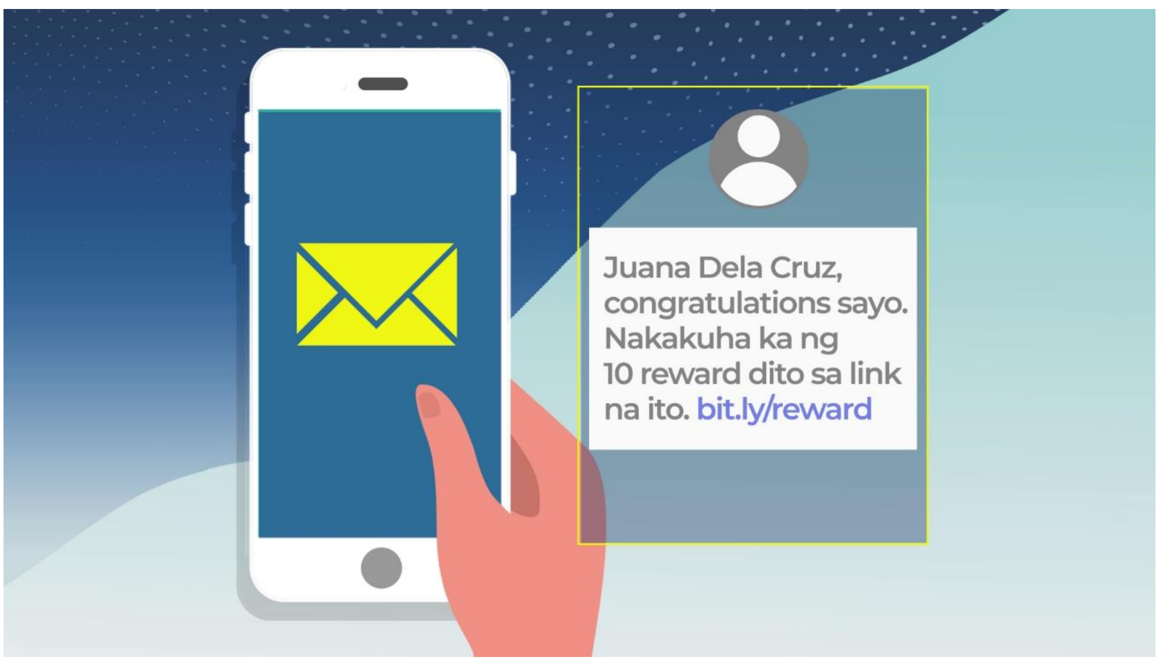
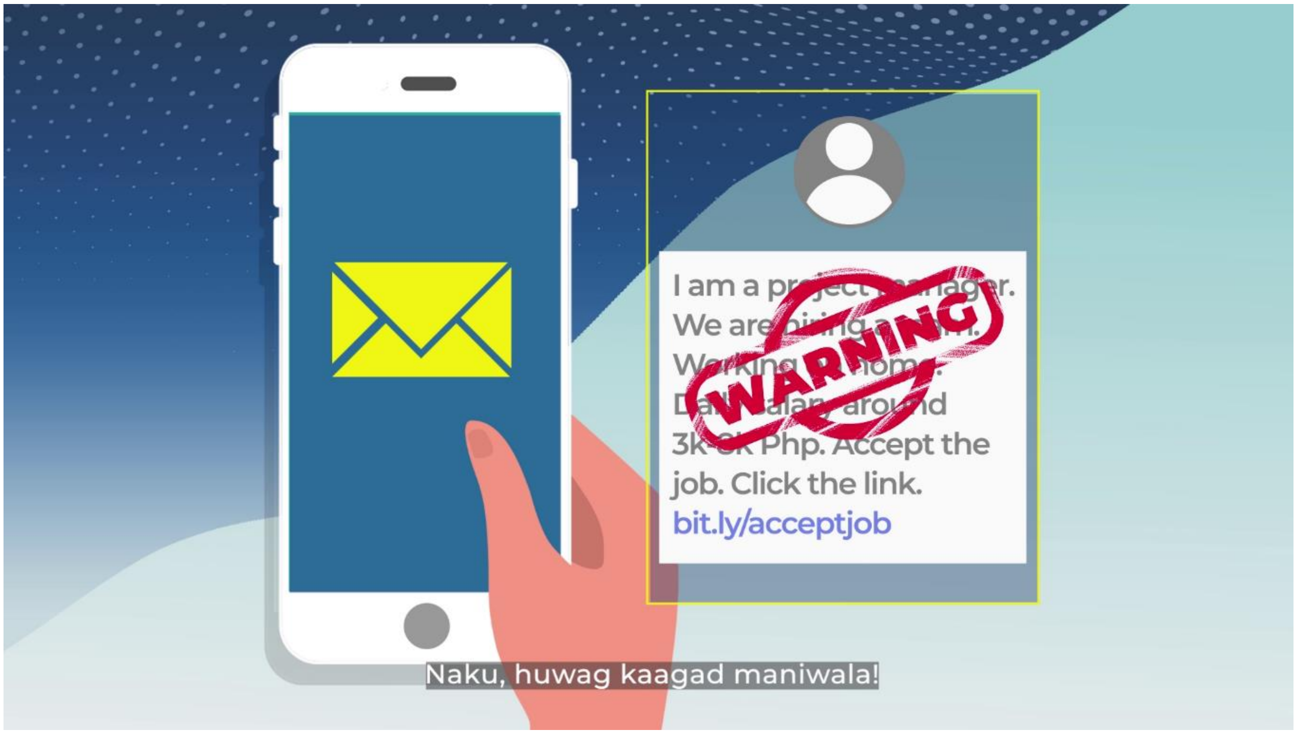
SMiShing

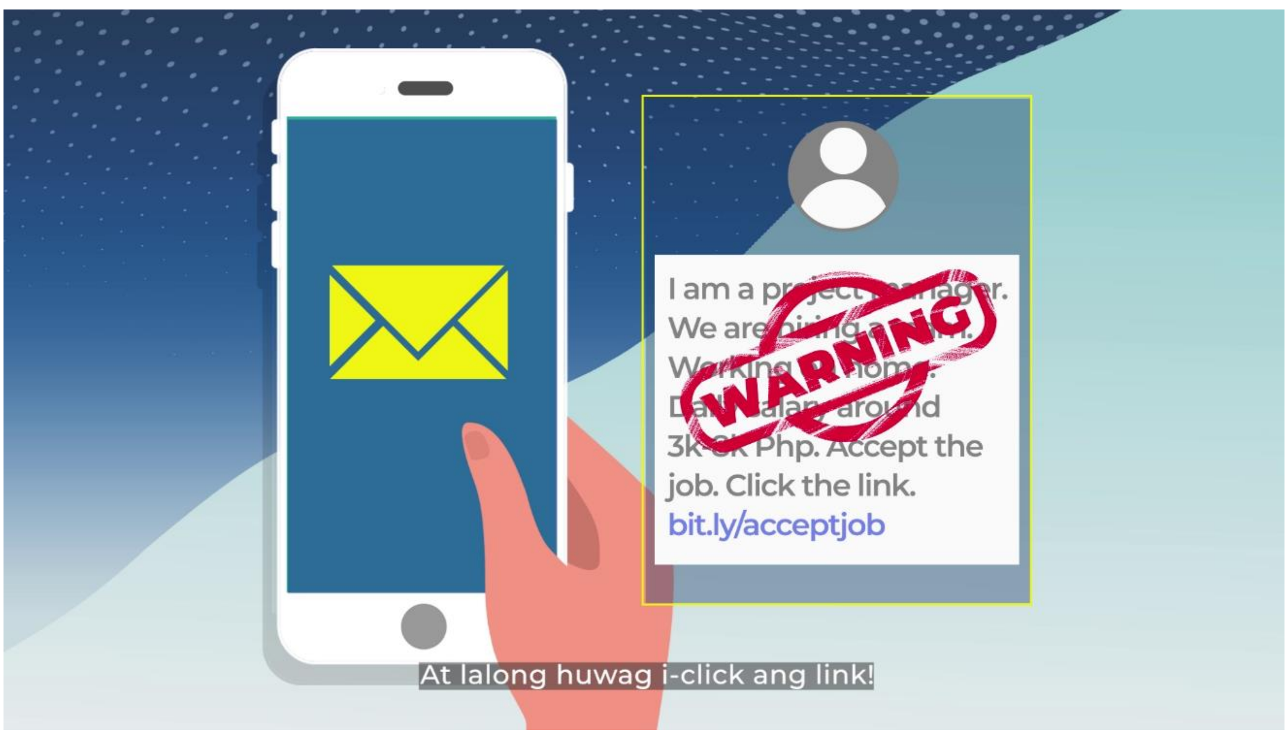
Ito ay isang halibawa ng **SMiShing**



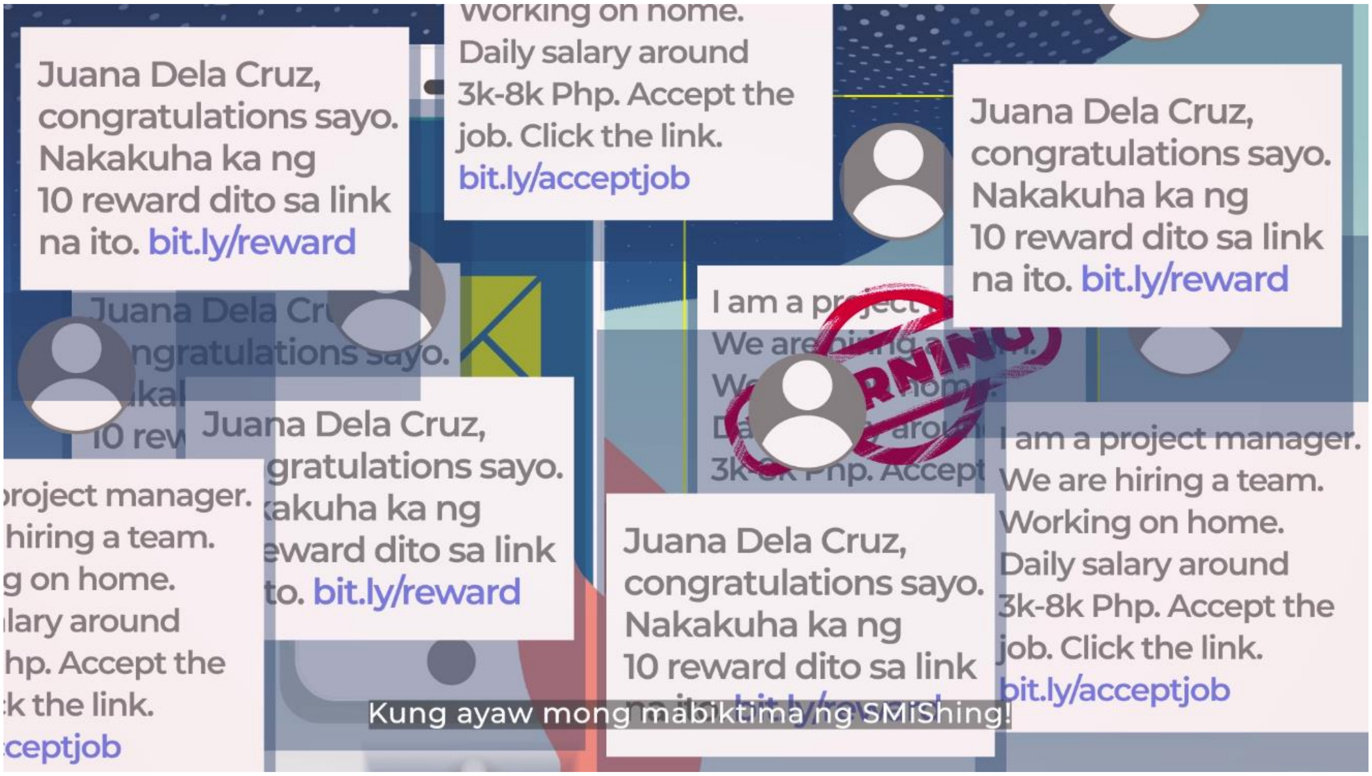
Kapag nakatanggap ka ng ganitong uri ng text message mula sa iyong bangko wag agad maniwala.



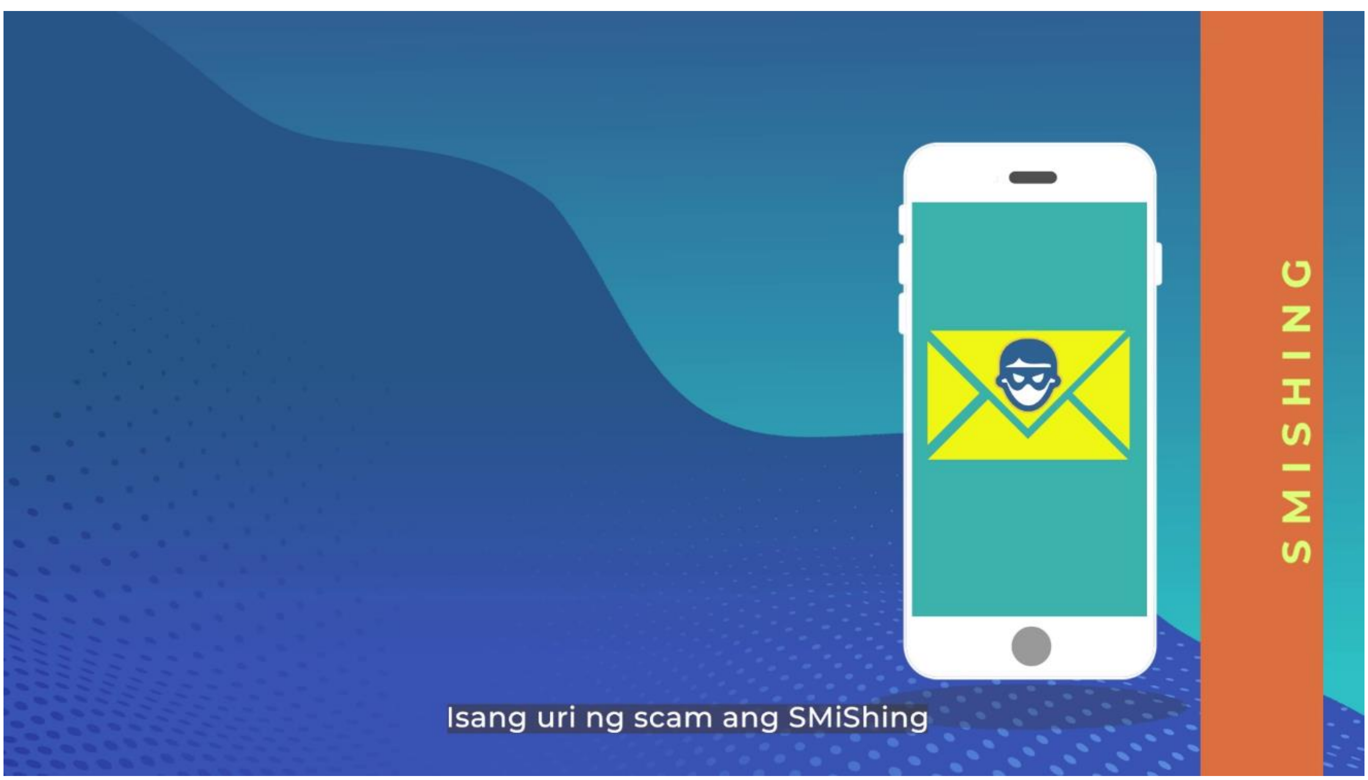
At tandaan lalong wag i-click ang link! Kung ayaw mo mabiktima ng **SMiShing**.



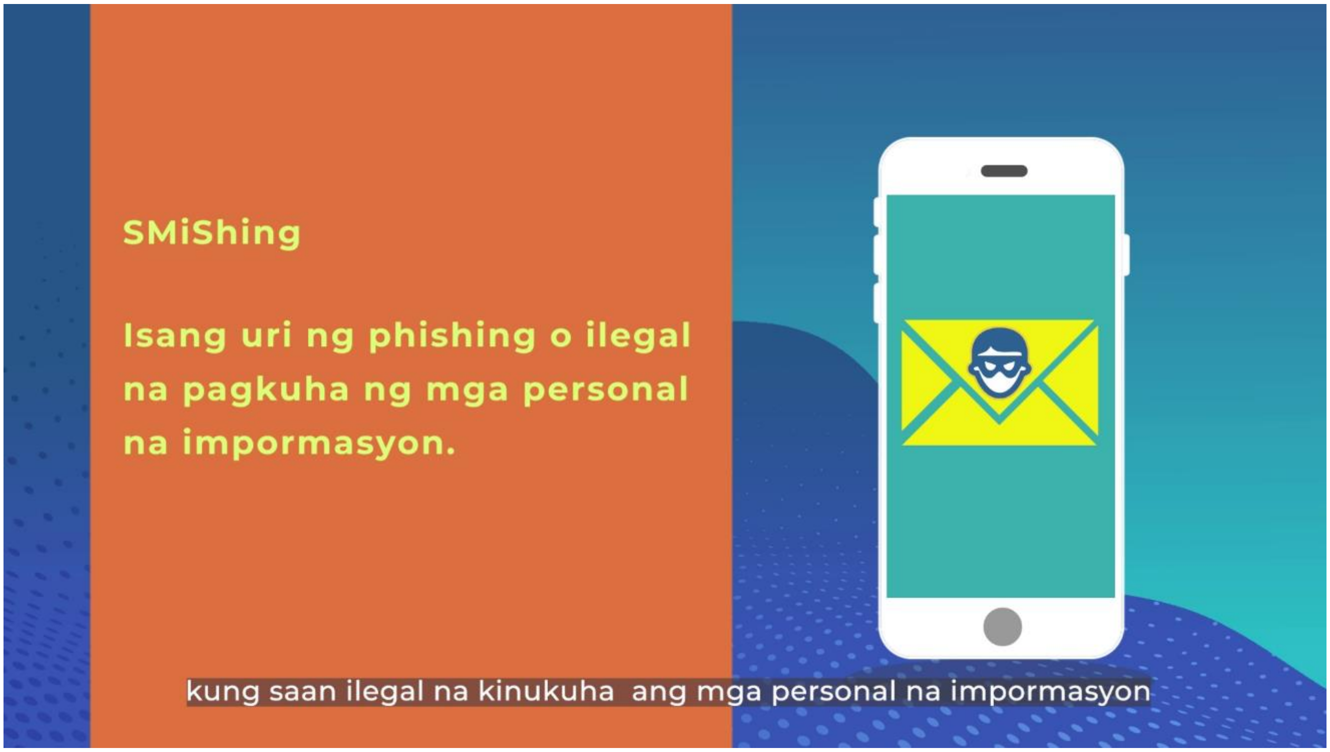
Kapag na click mo ang link. Maari kang mabiktima ng **SMiShing**.



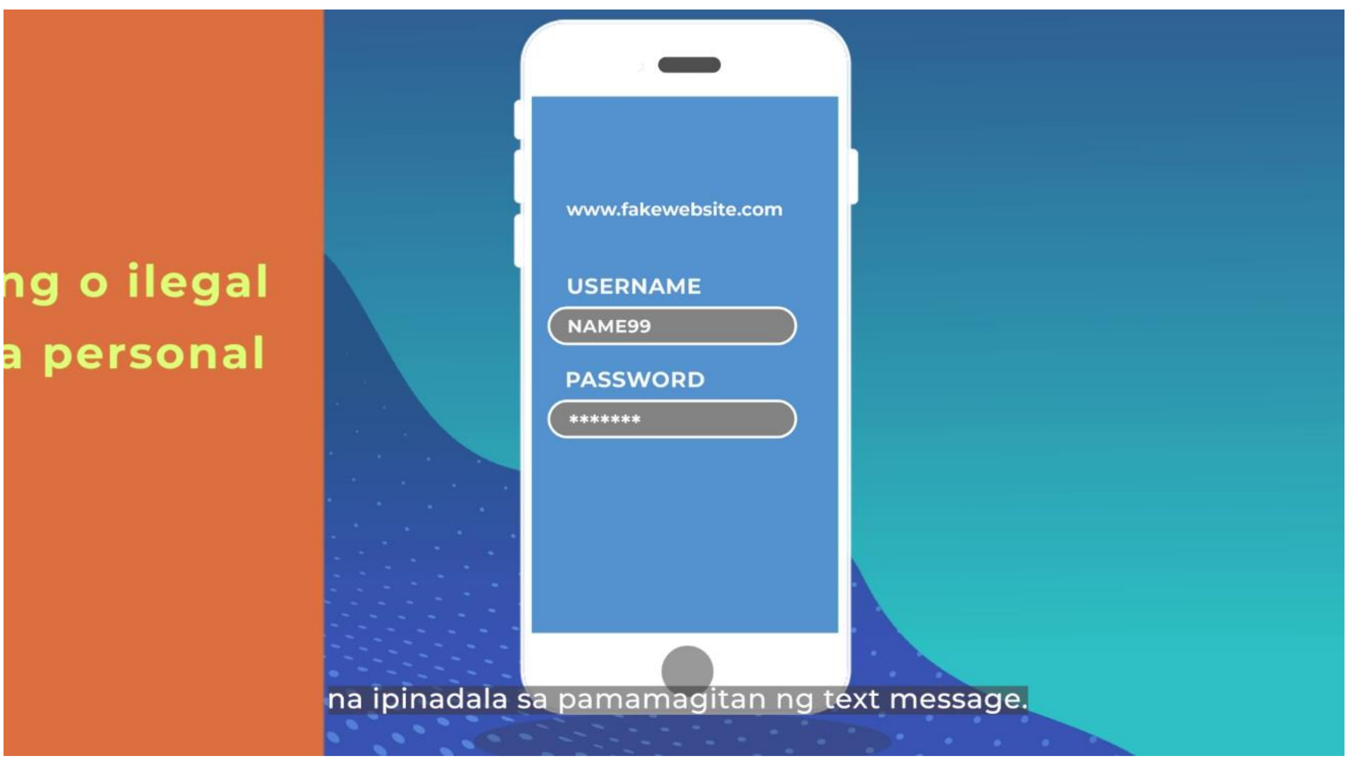
Ano ang **SMiShing?**



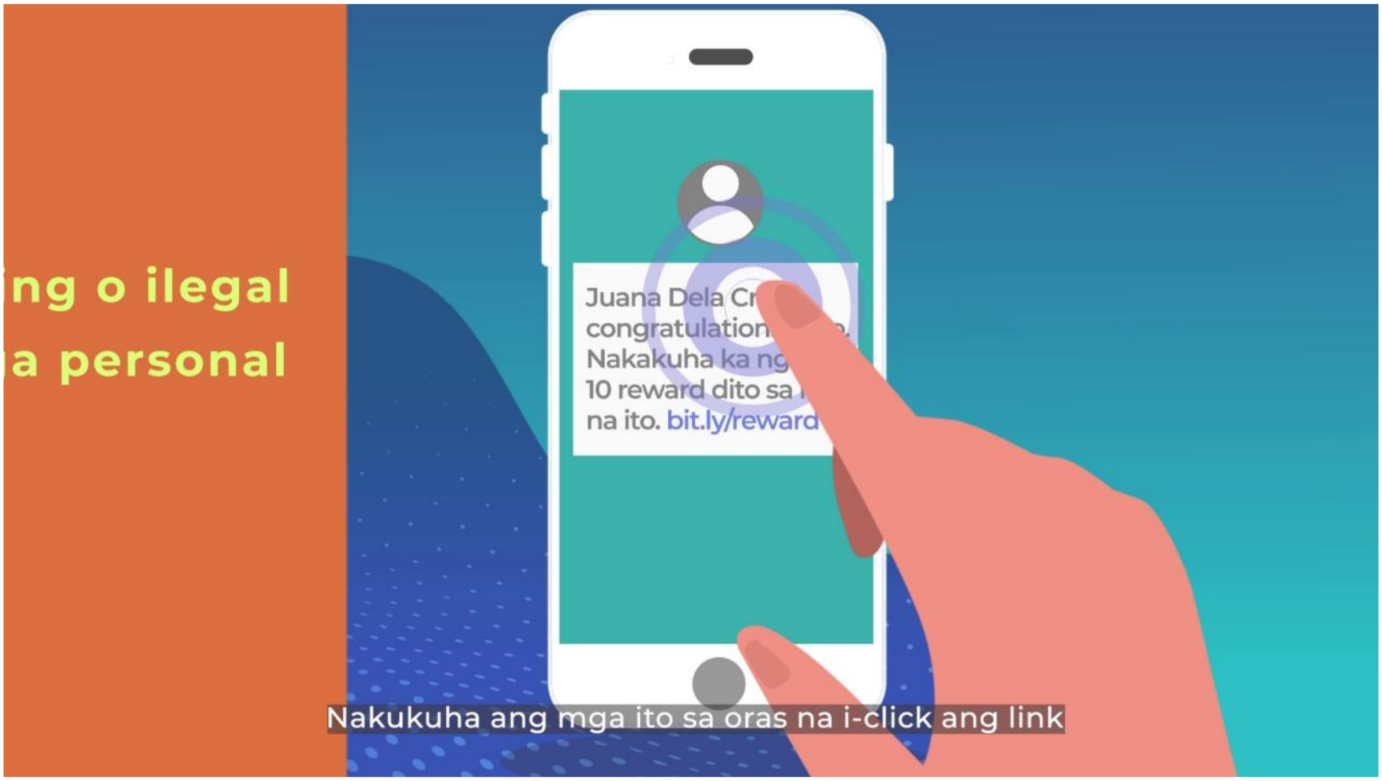
Ang **SMiShing** ay isang Scam. Kung saan illegal na kinukuha ang mga personal na impornasyon.



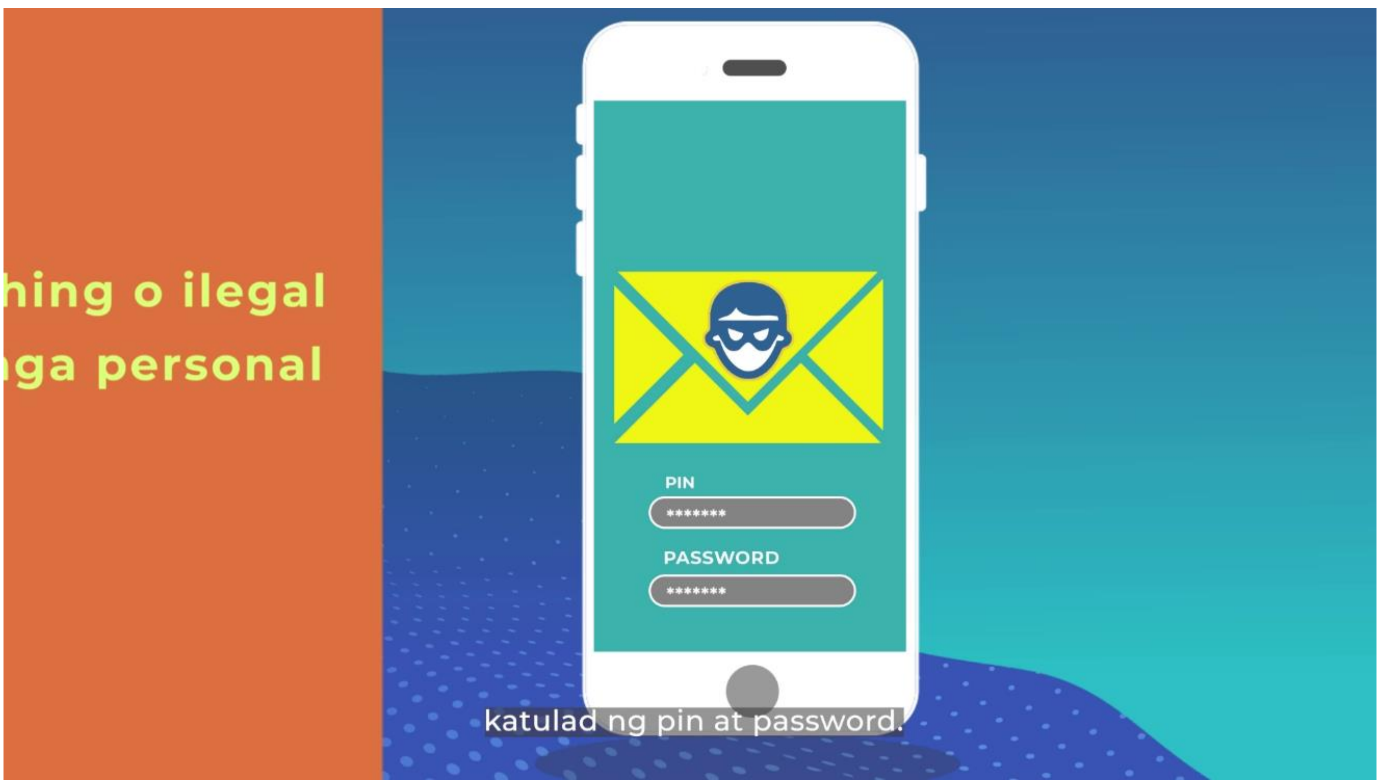
Katulad ng Pin at Password.



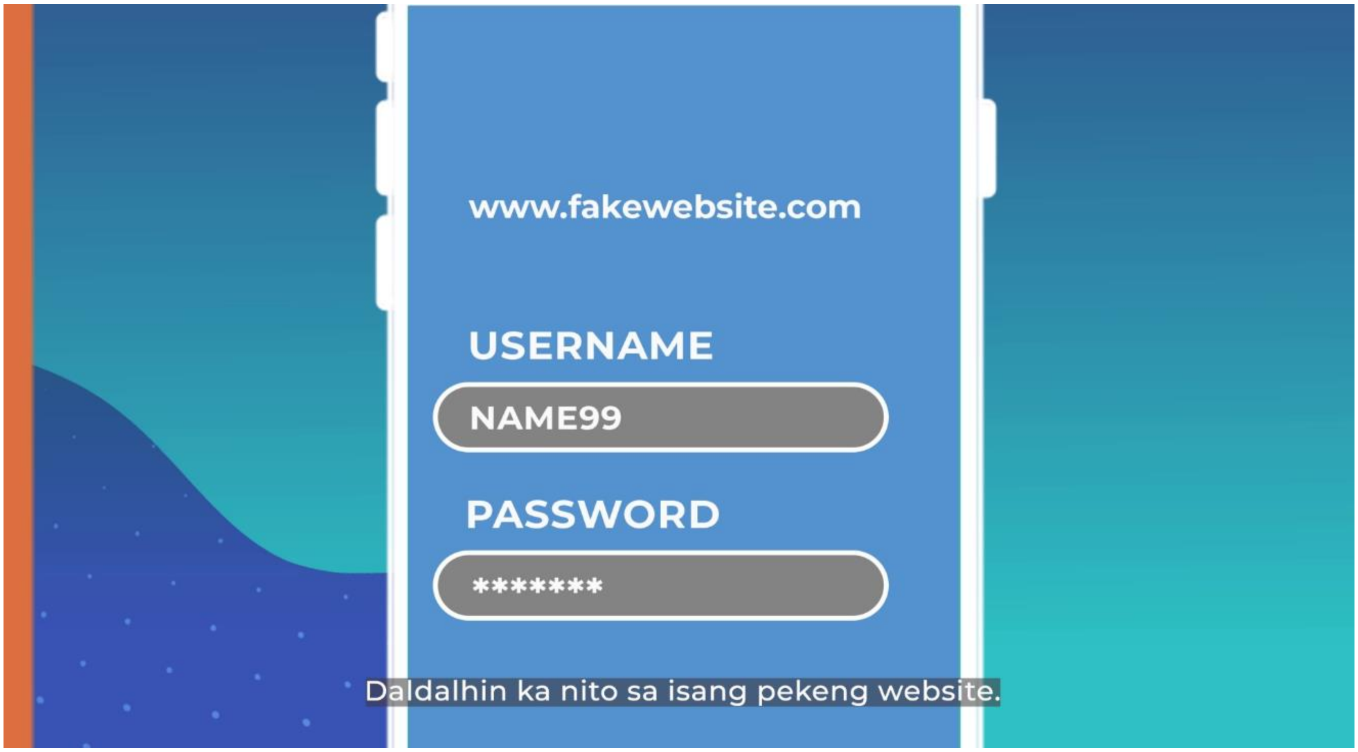
Makukuha ang mga personal na impormasyon sa oras na ma click mo ang link na ipinadala ng scammer sa text message.



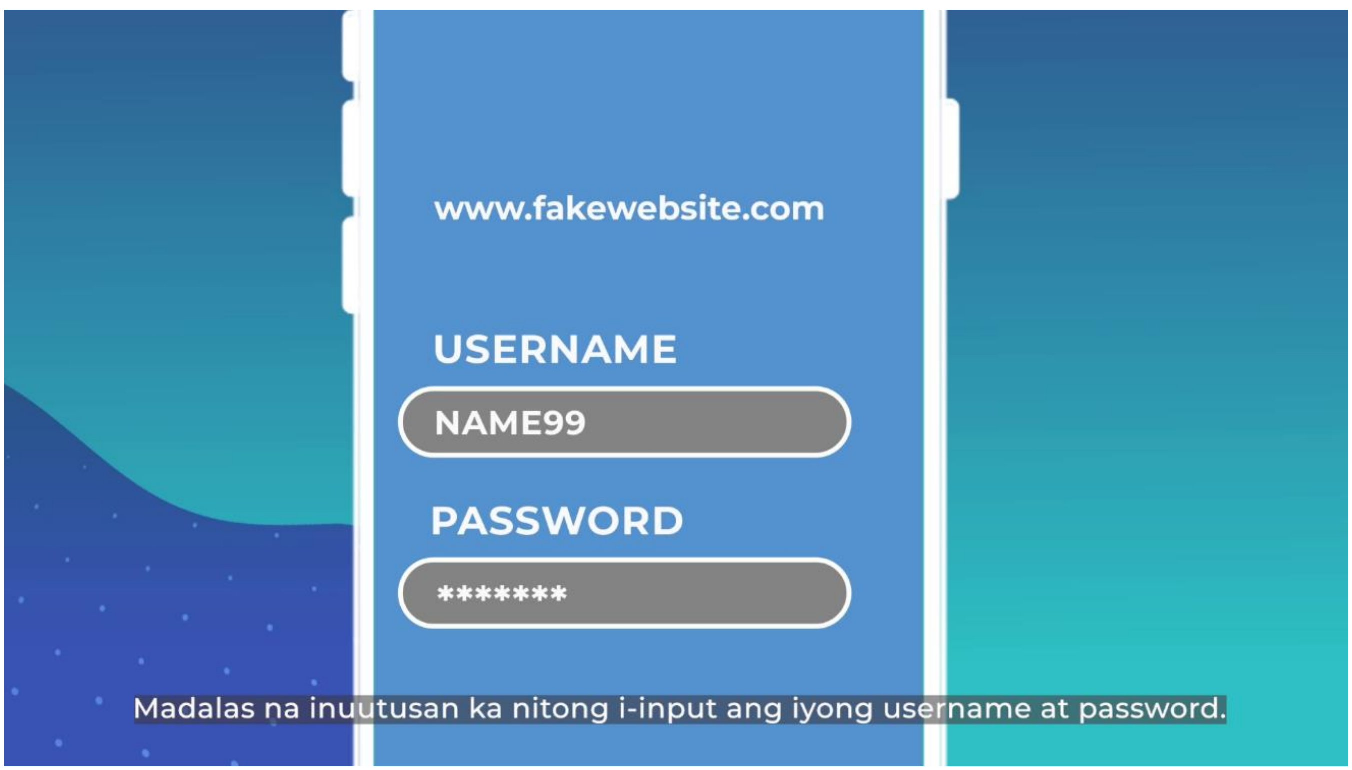
Maaaring makuha ang iyong personal na impormasyon kagaya ng password at PIN.



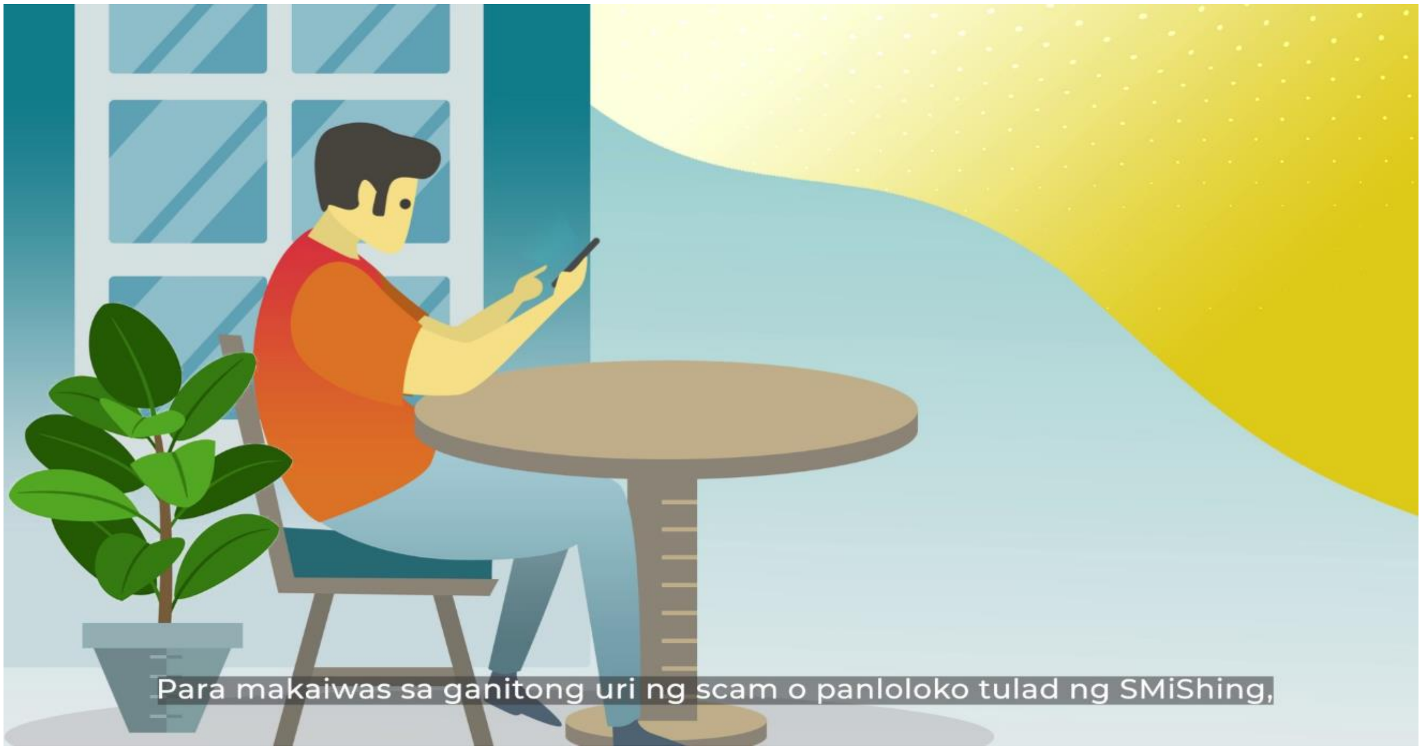
Kung saan dadalhin ka nito sa isang pekeng website.



Madalas inuutusan ka nitong i-input ang iyong username at password.

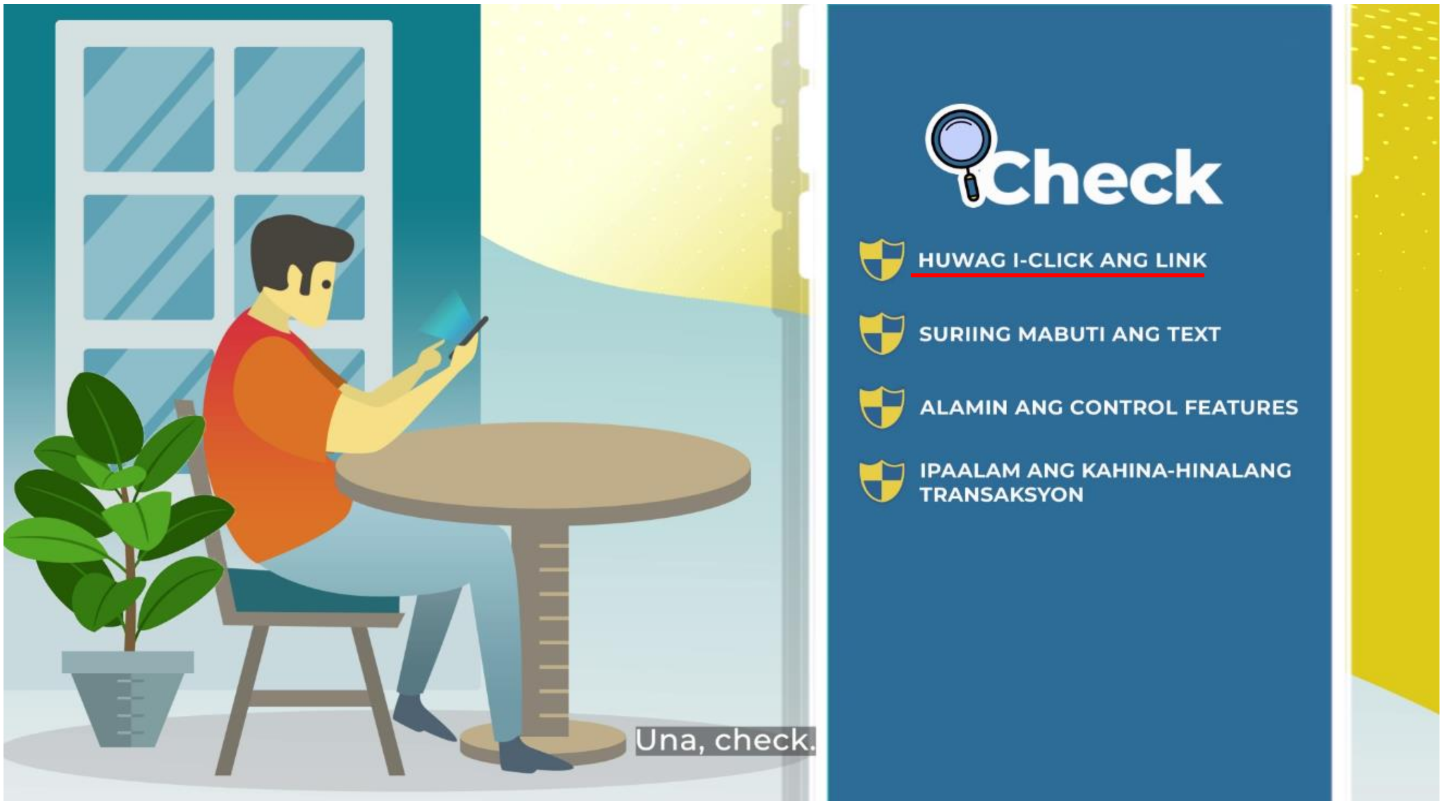


Para maka iwas sa ganitong uri ng scam o panloloko katulad ng **SMiShing,** ugaliing mag **C-P-R.**



Check-Protect-Report

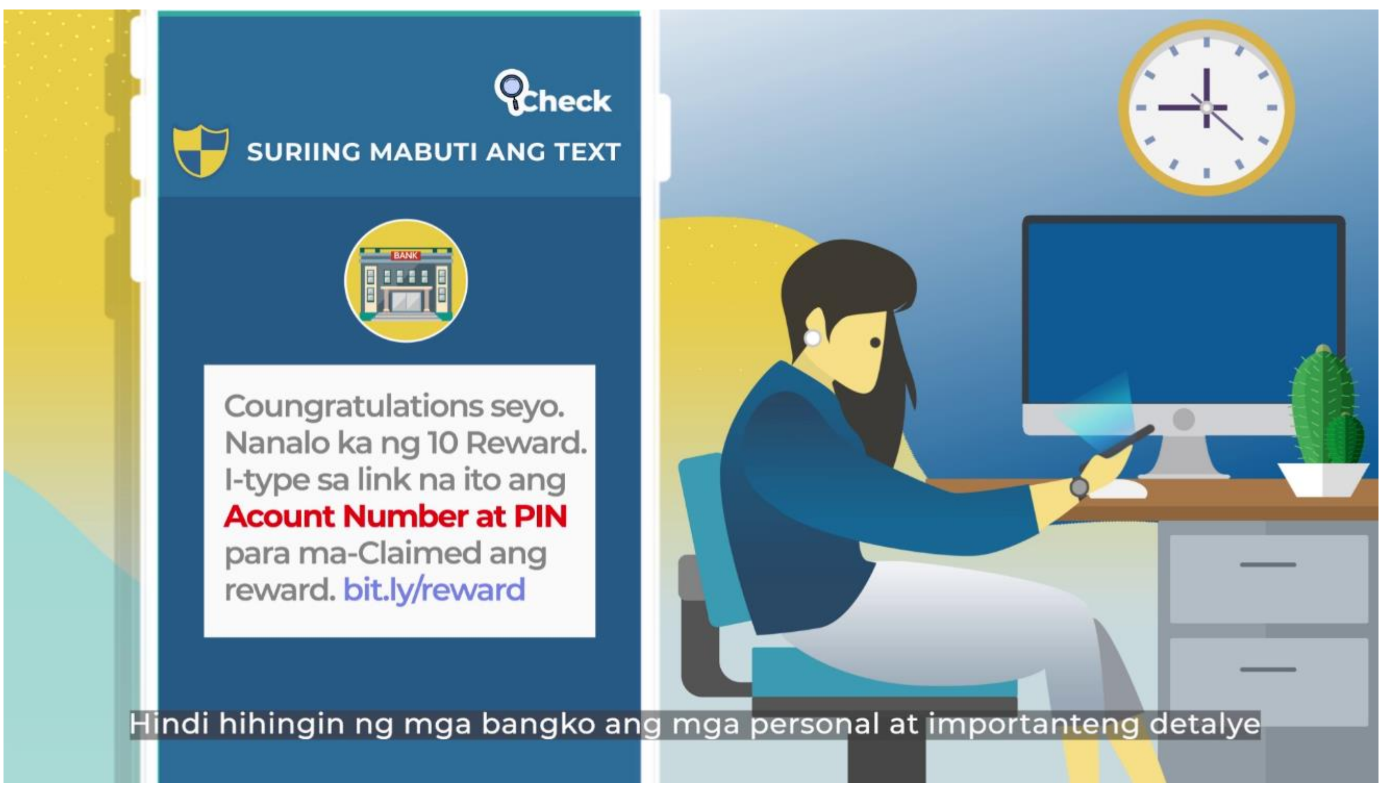
Una **CHECK!**



Huwag na huwag i-click ang link na matatangaap. Kahit mukha itong galing sa kilalang bangko, e-money issuer, mga kilalang kumpanya o brand, hindi mo dapat ito i-click. Huwag din mag reply sa text message.

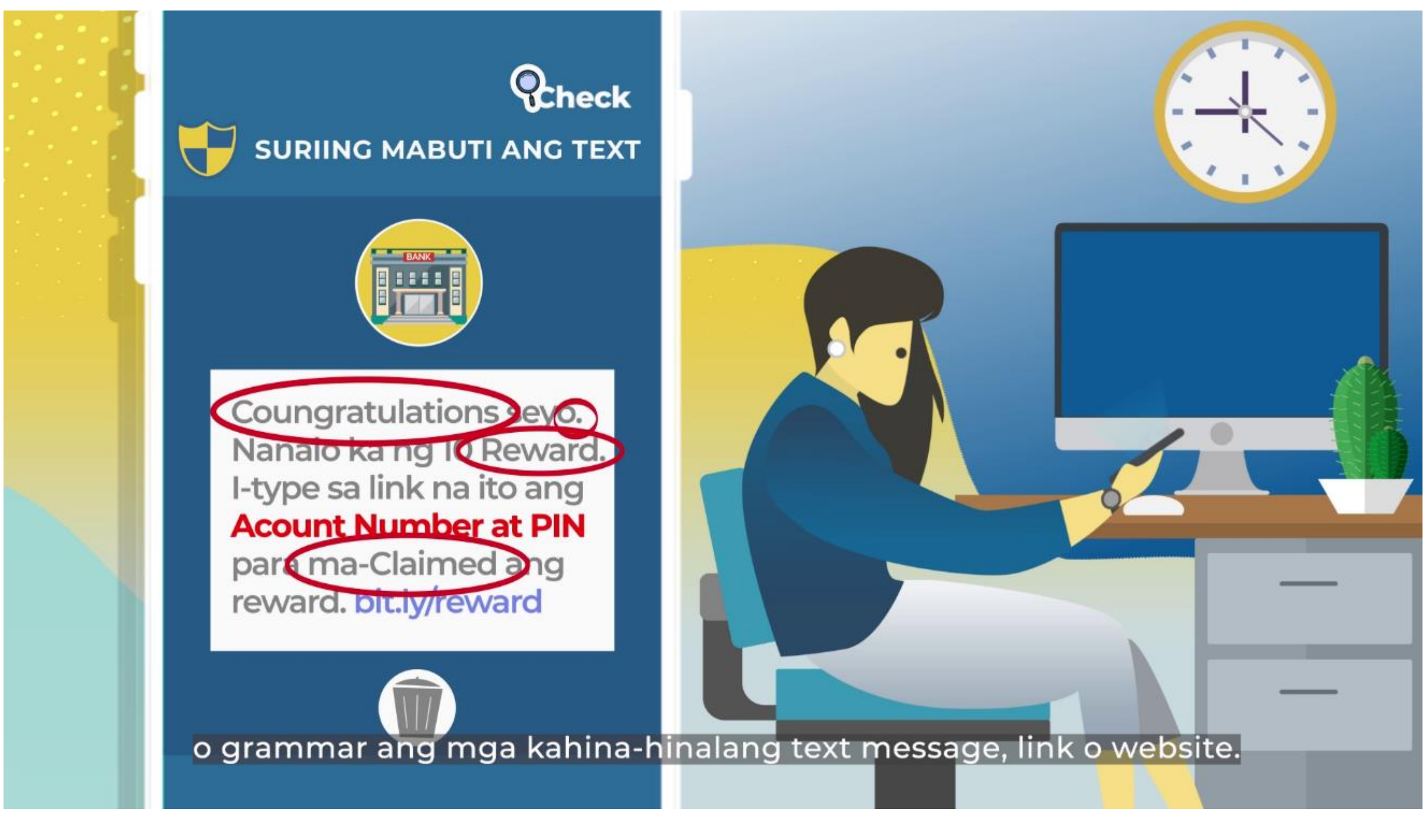
Ikalawa, suriing mabuti ang mga natatanggap na text message

Hindi hihingiin ng mga bangko ang mga personal at importanteng detalye tungkol sa inyong account sa pamamagitan ng text message.



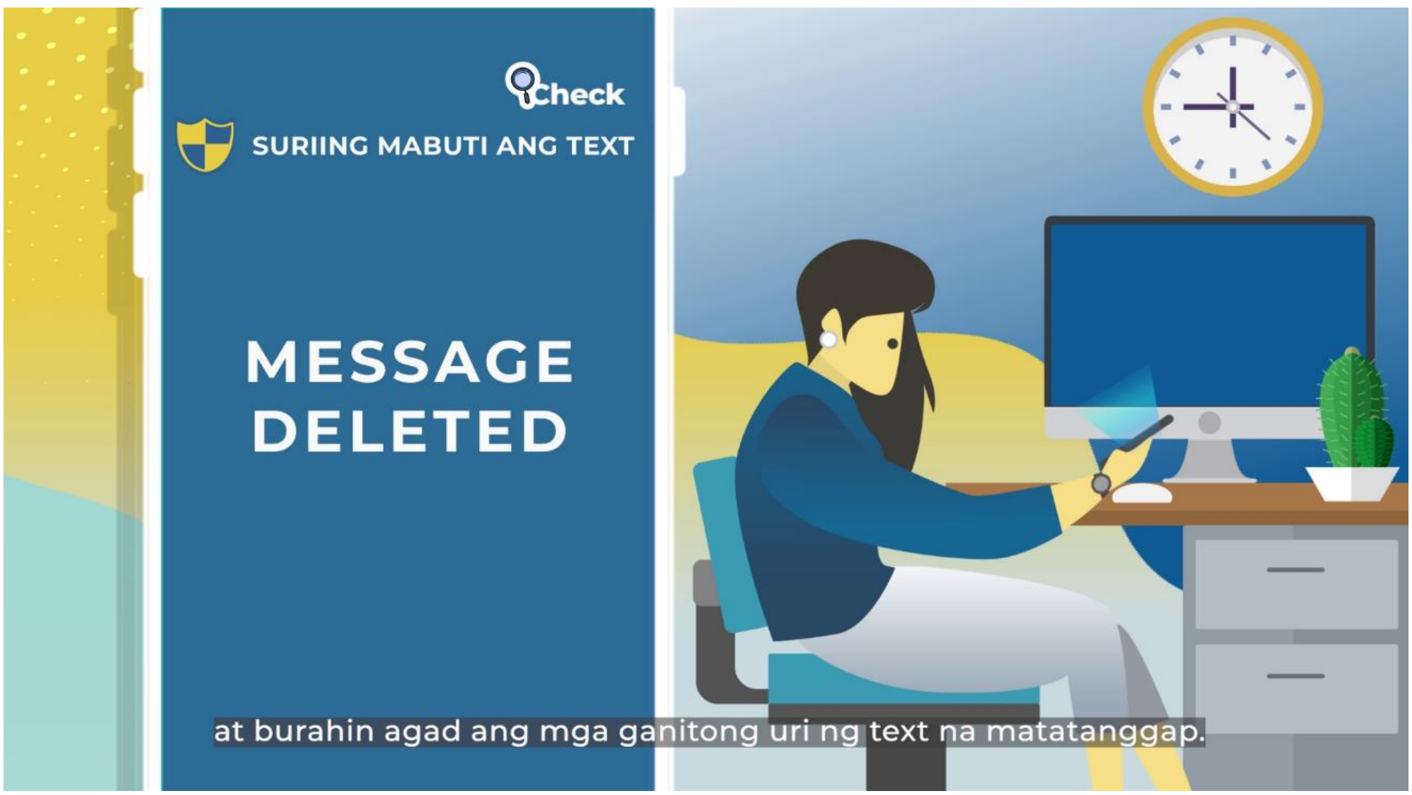
Dagdag kaalaman din, suriin ang pagkakasulat ng mensahe o laman ng link, website o kaya naman ang login page.

Kadalasang maraming makikitang mali sa spelling, punctuation, capitalization o grammar ang mga kahina-hinalang text message, link o website.

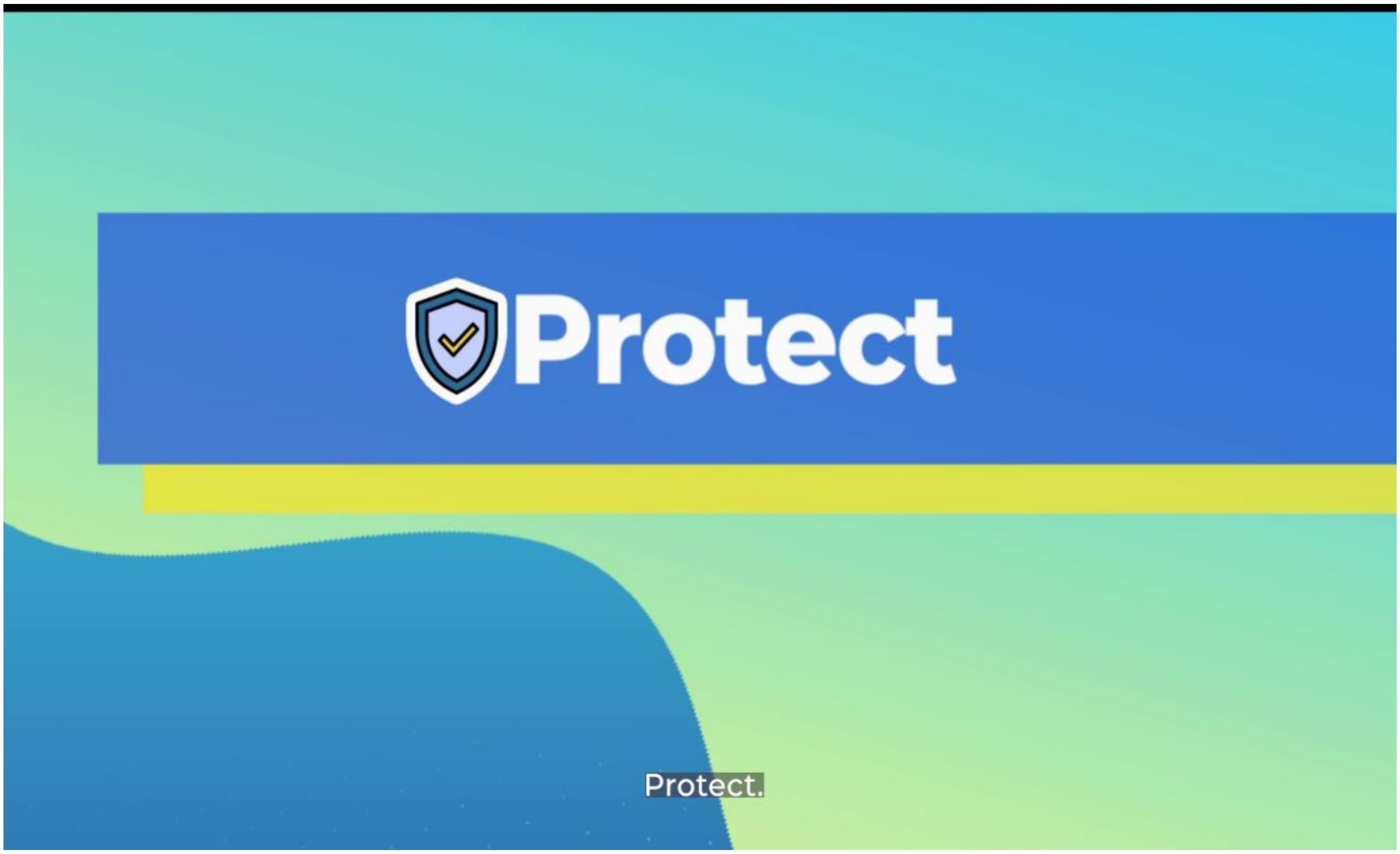


Kaya naman I block ang sender.

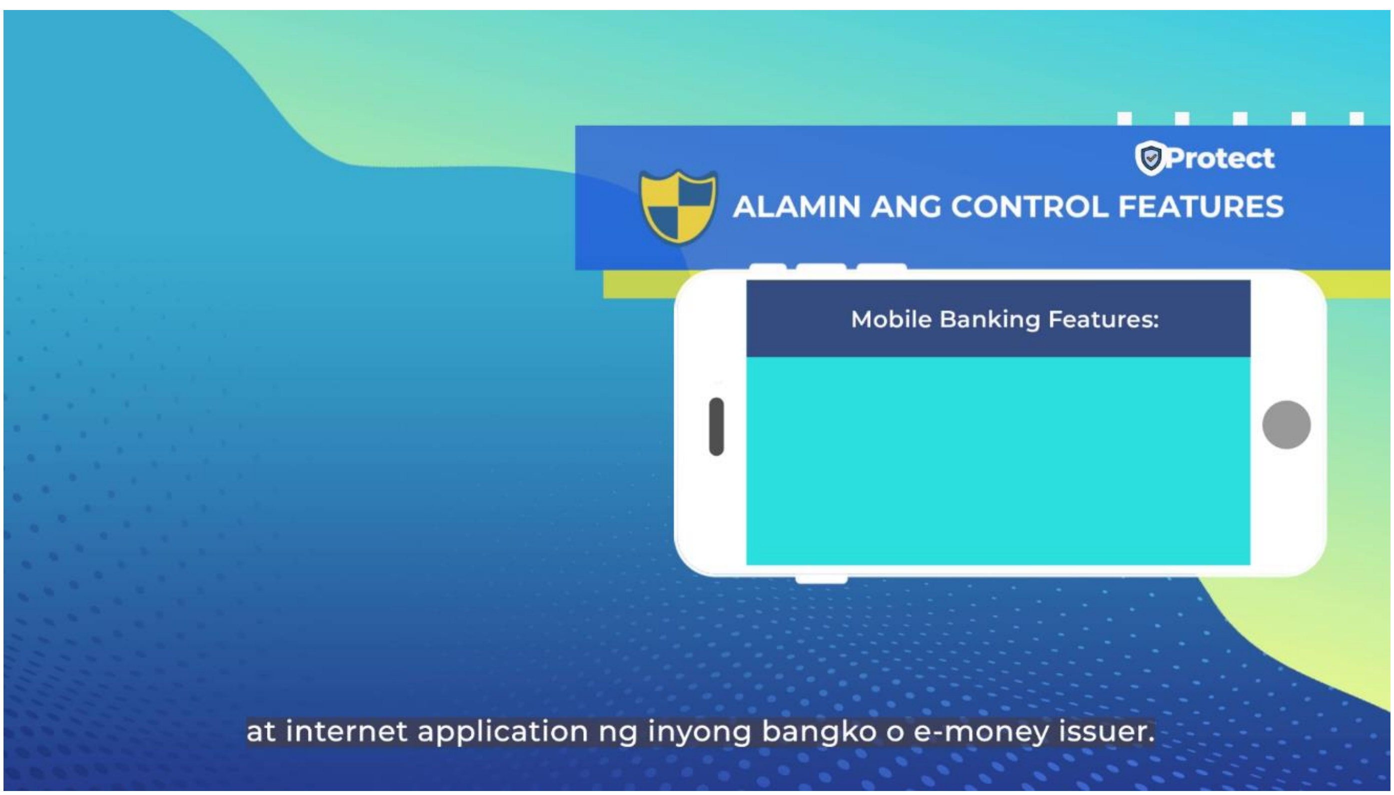
At burahing agad ang mga ganitong uri ng text na matatanggap.



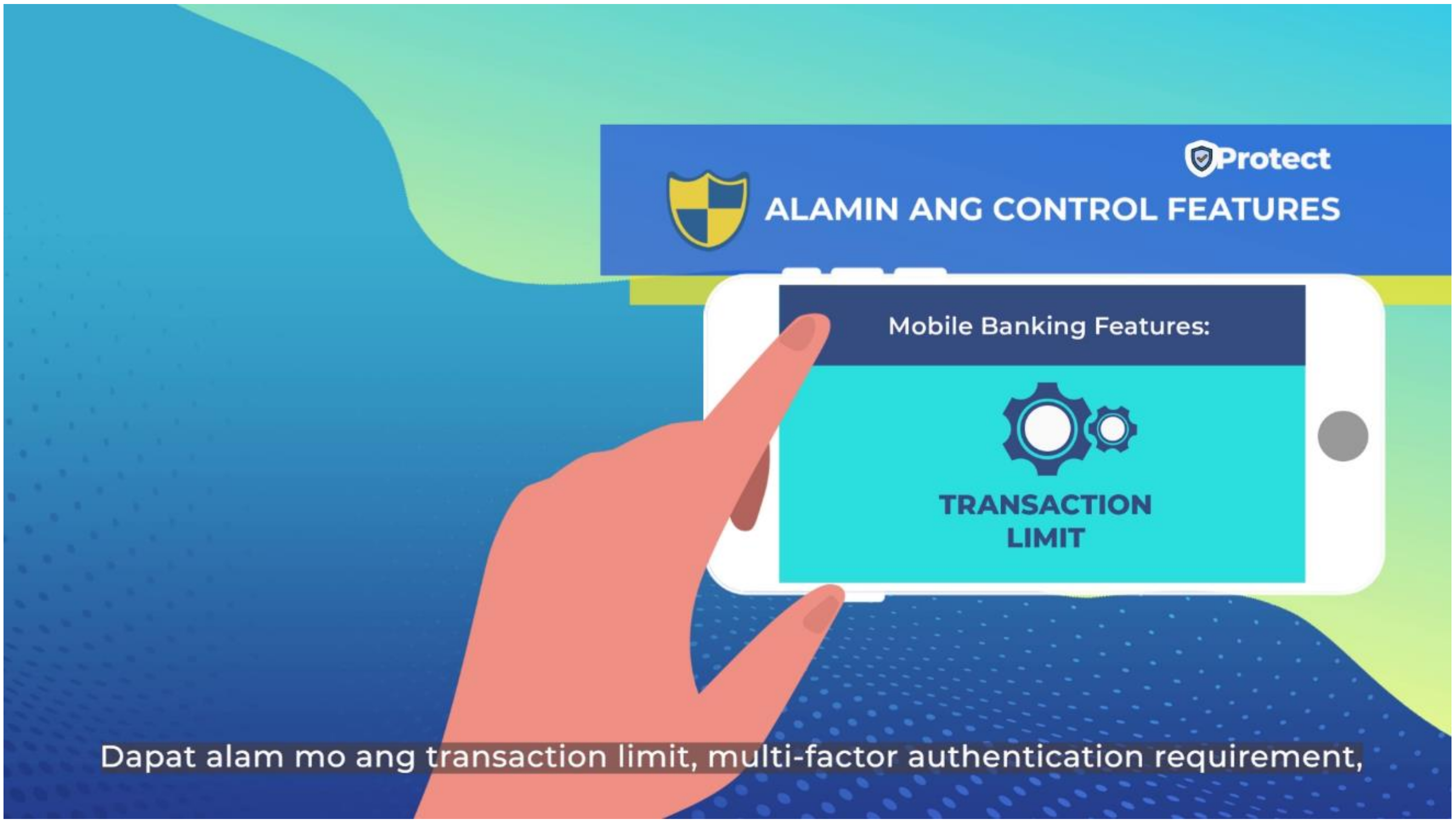
Ikalawa **Protect!**



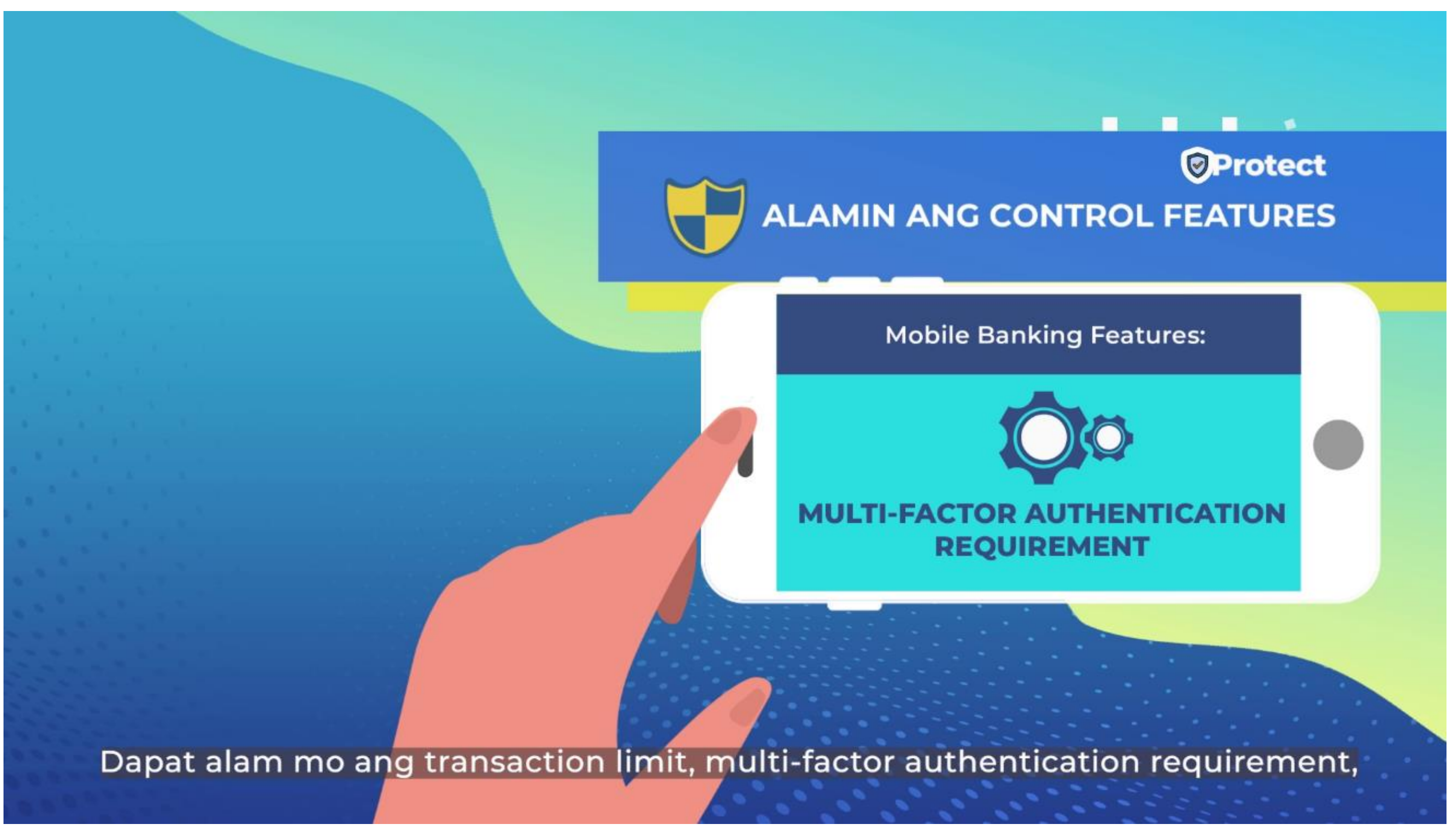
Alamin ang control features ng Mobile at internet application ng iyong bangko o e-money issuer.



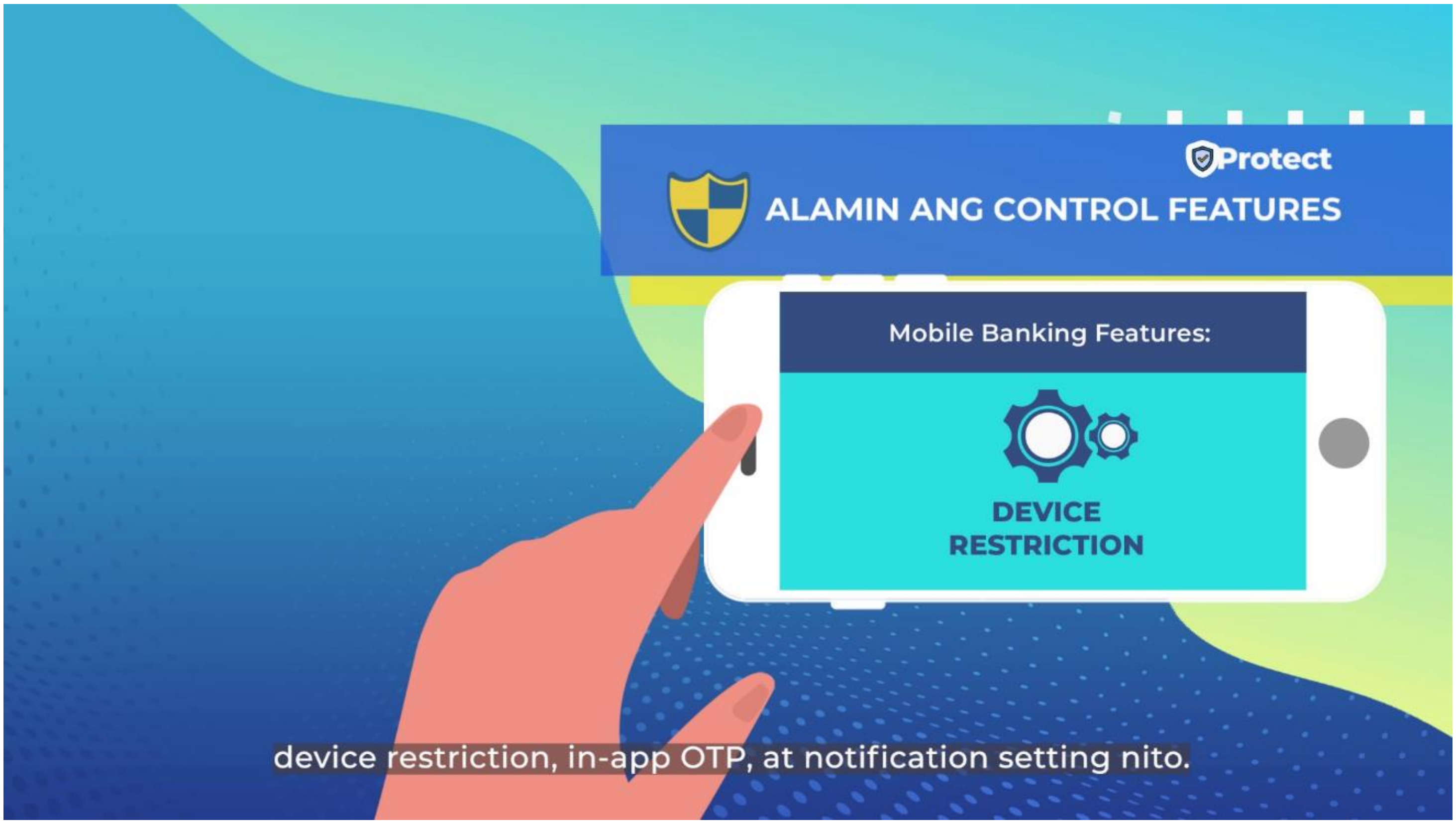
Dapat alam mo ang transaction limit,



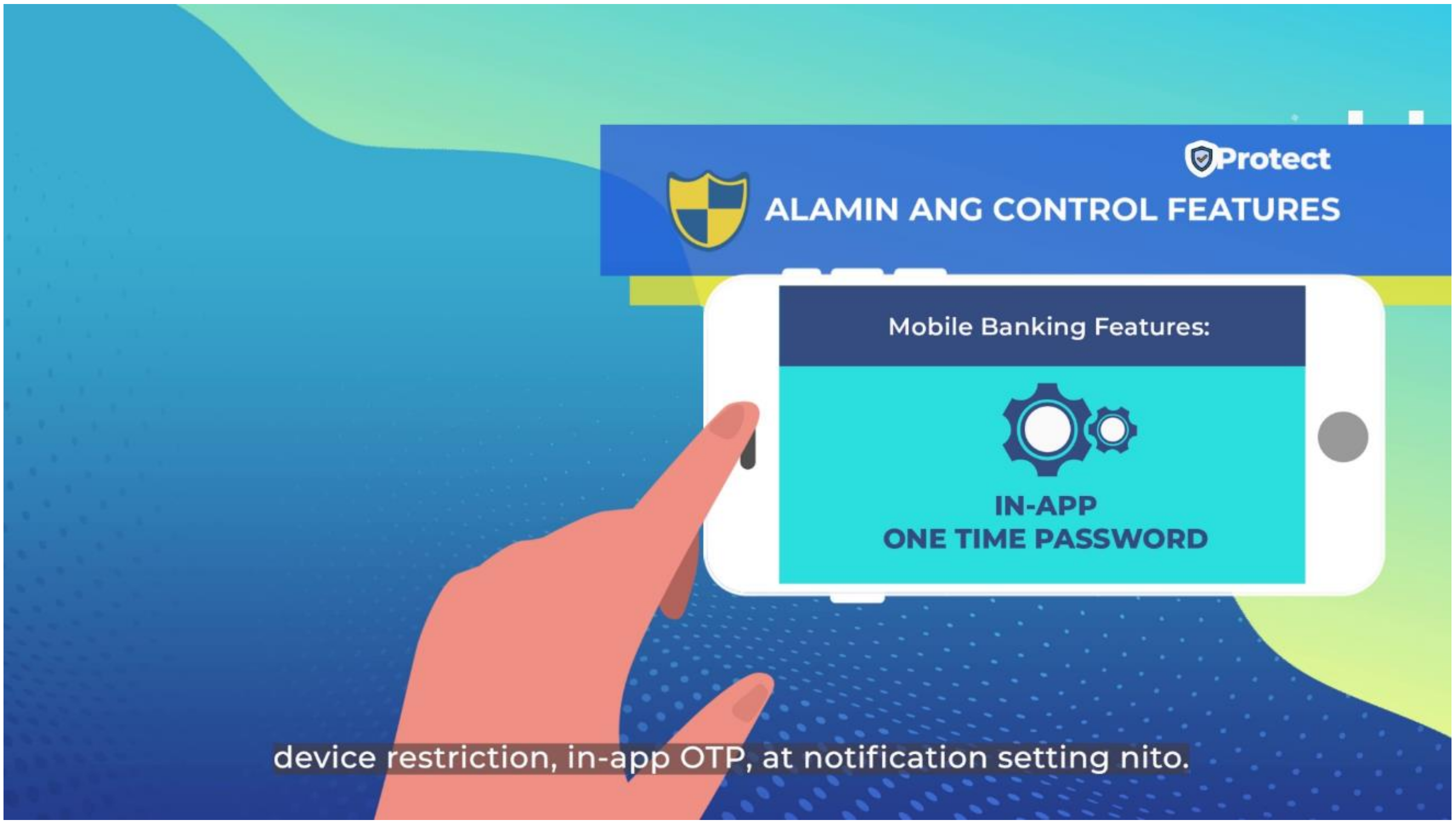
Multi-factor authentication requirement,



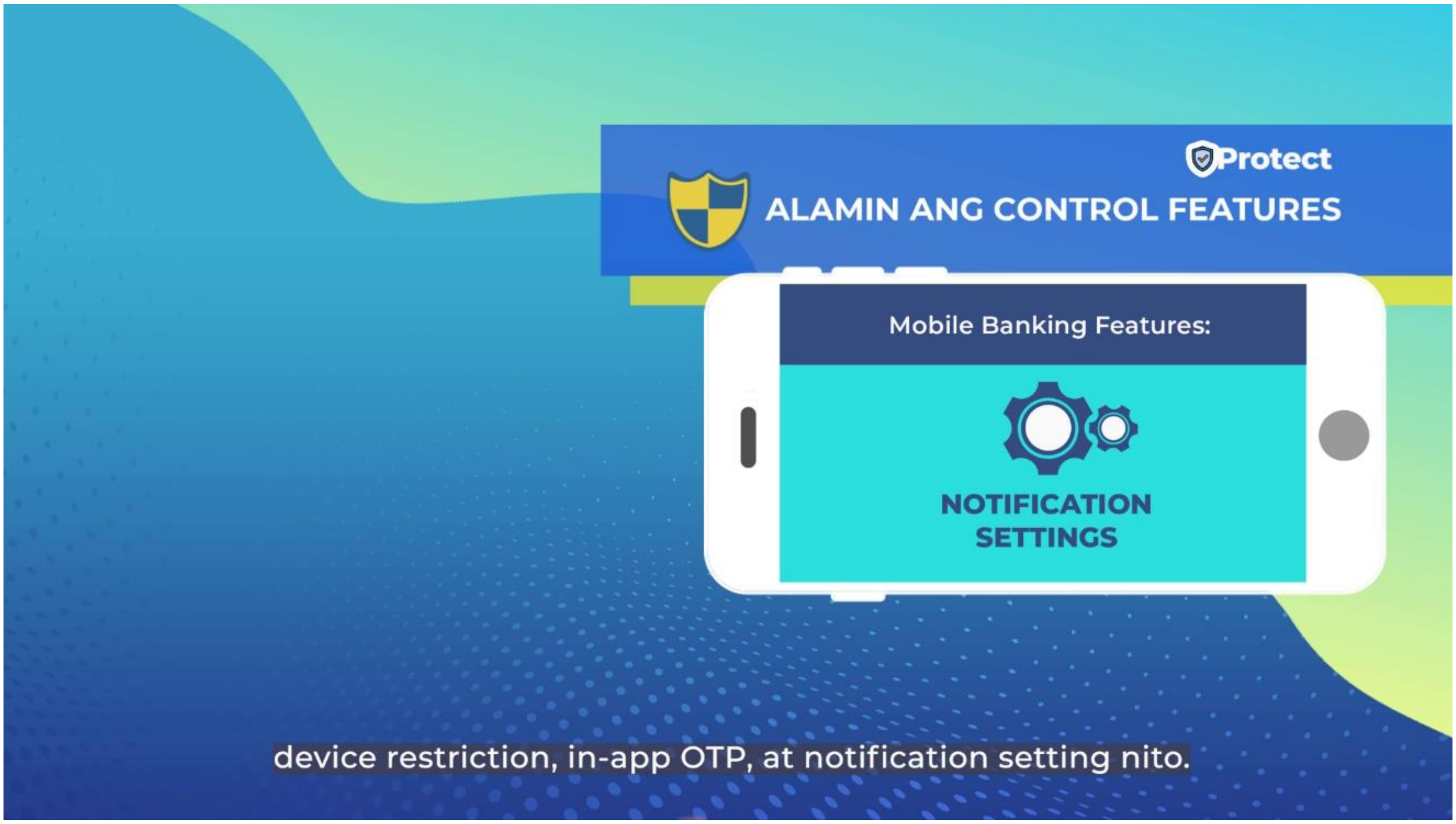
Device restriction,



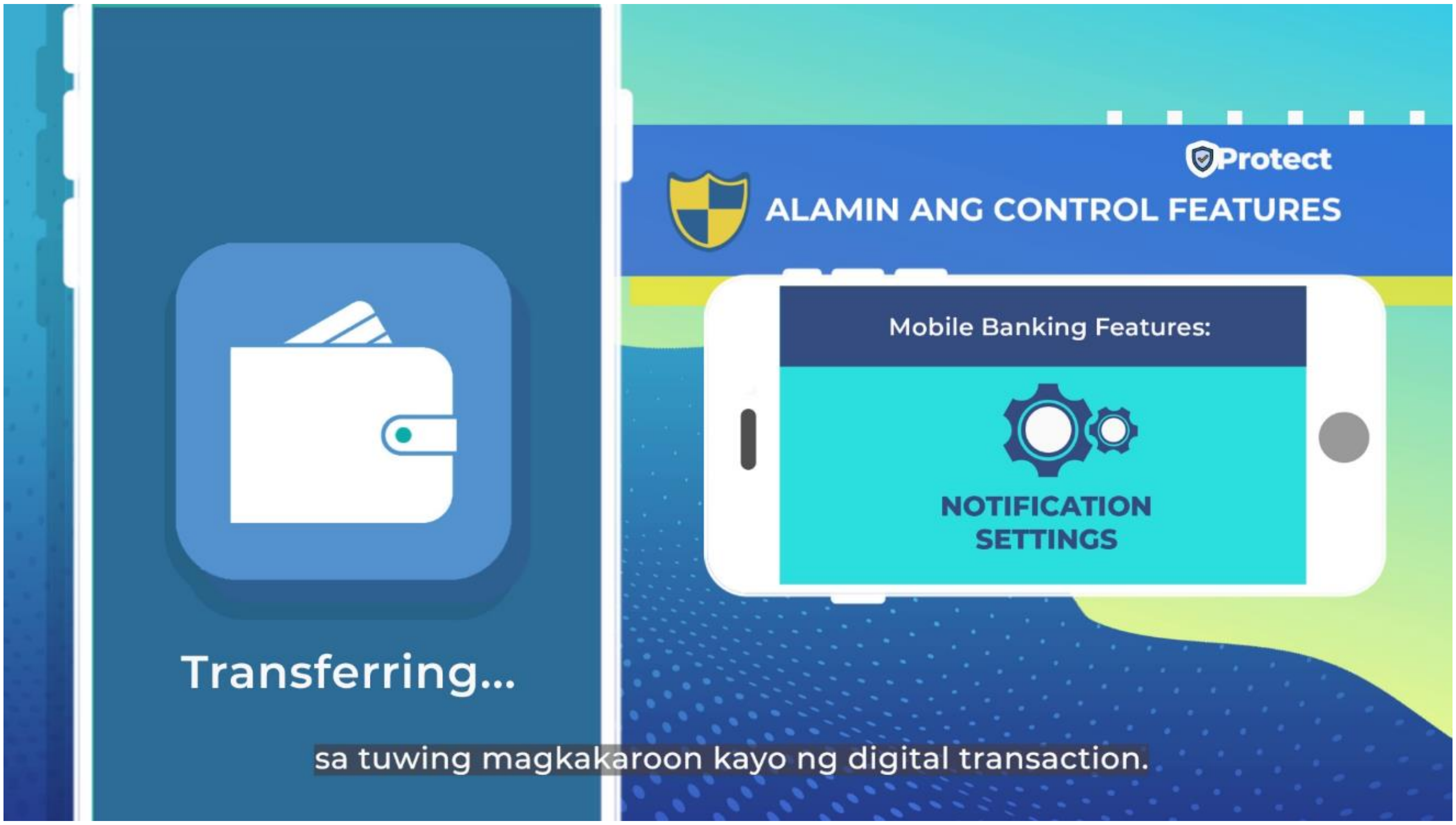
In-app OTP,



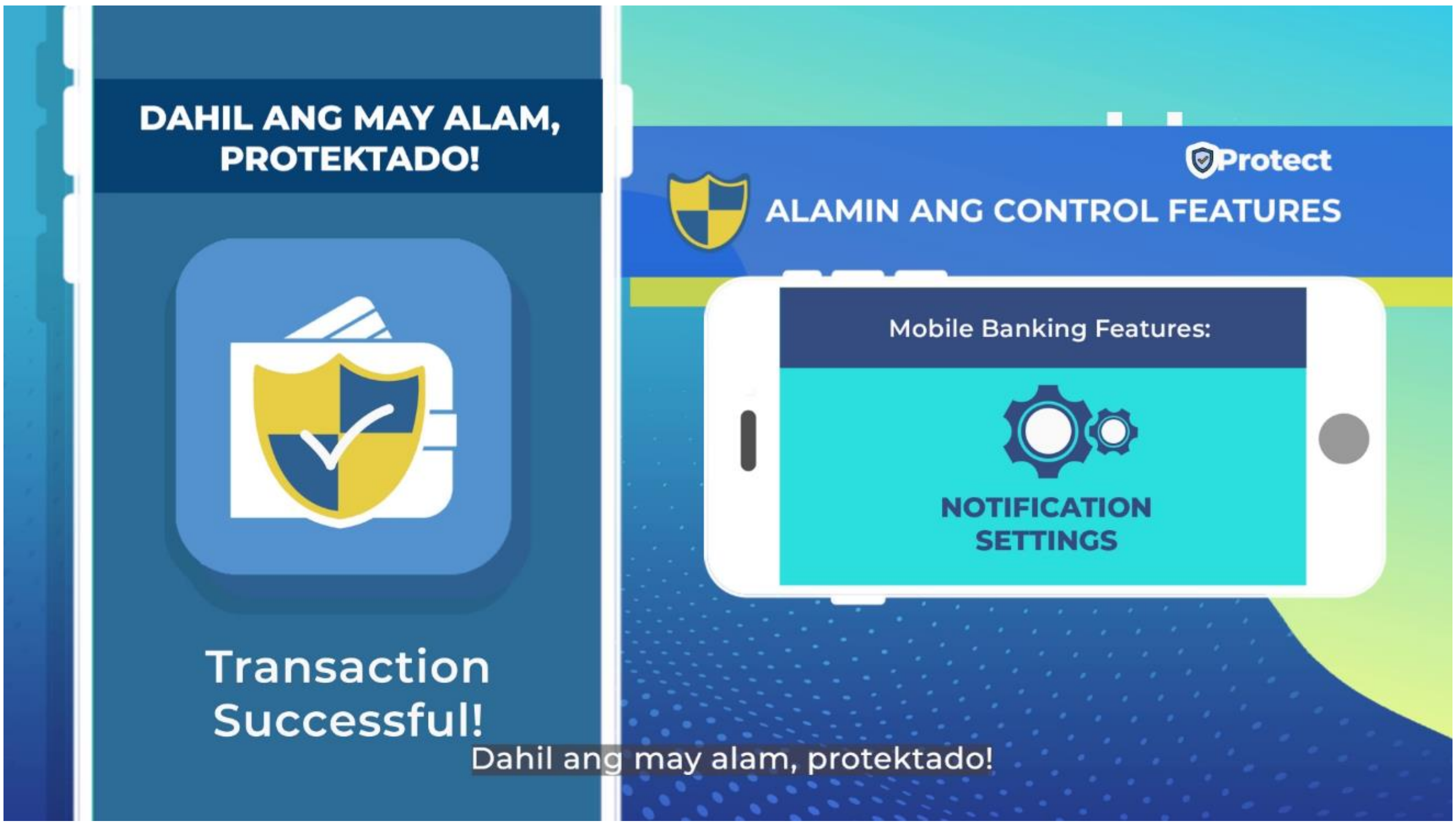
At notification setting nito.



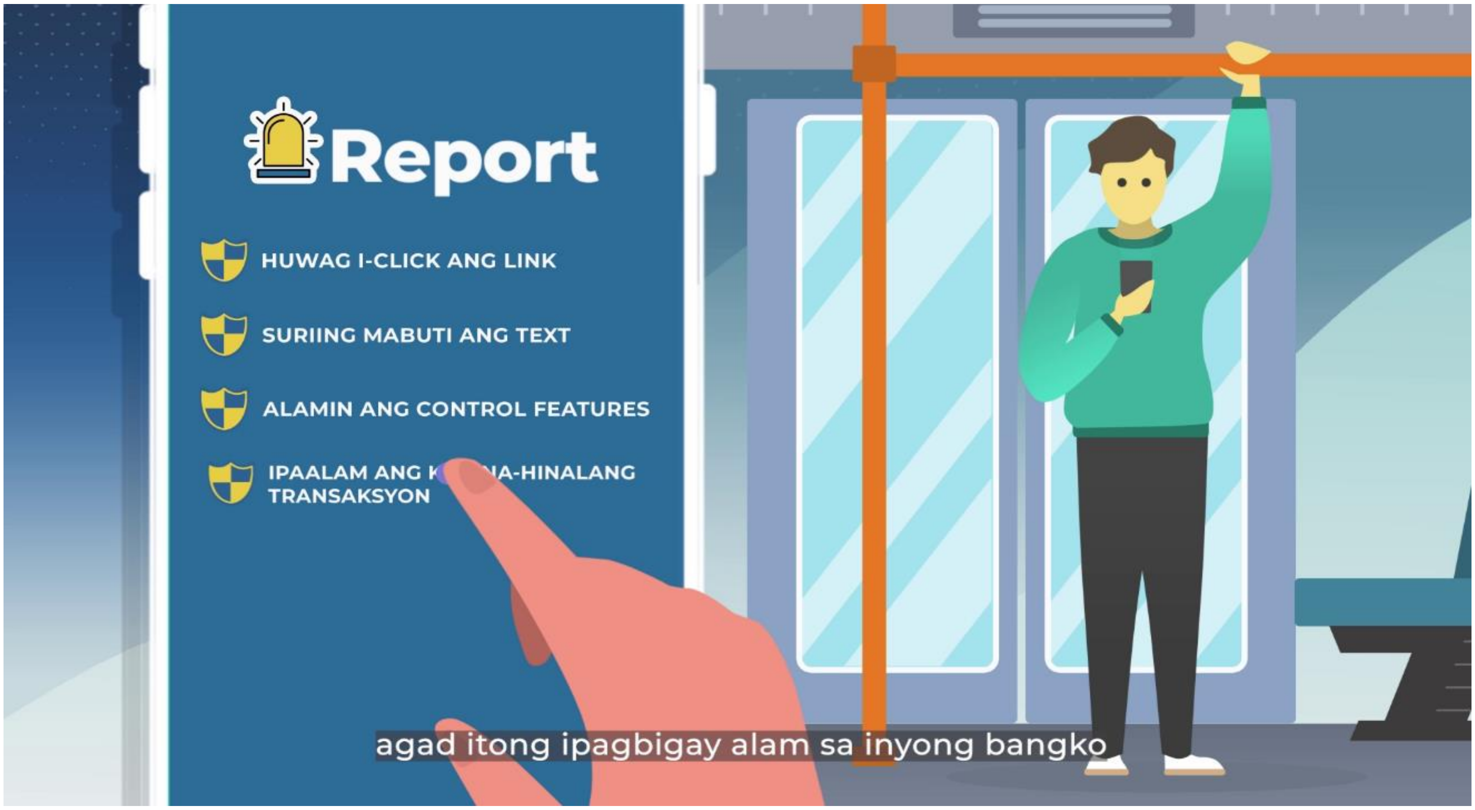
Makakatulong ito para sa dagdag proteksyon sa tuwing magkakaroon kayo ng digtigal transaction.



Dahil ang may alam, **protektado!**

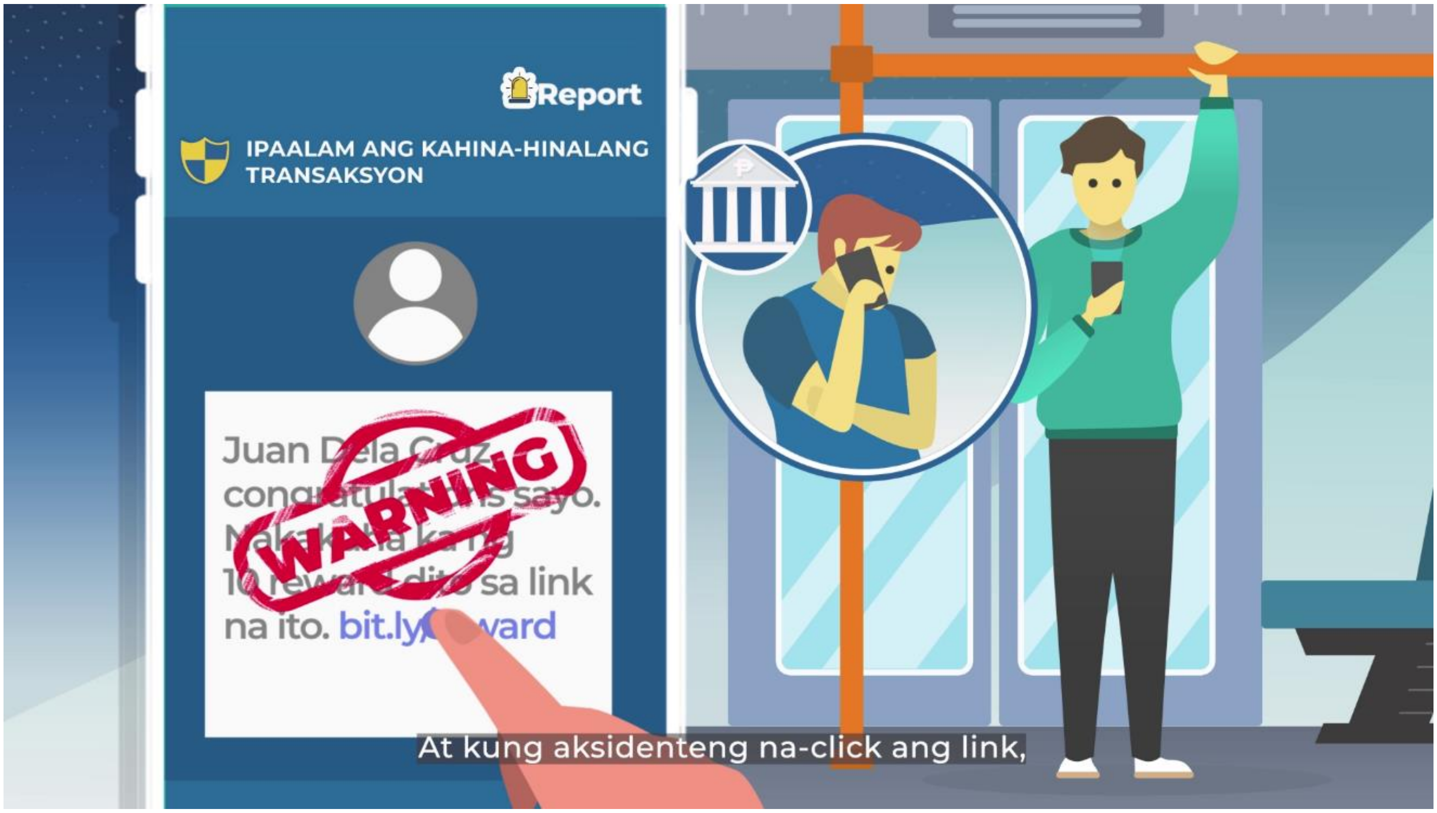


REPORT!



Kung may kahinahinalang transaksyon, agad itong ipagbigay alam sa inyong bangko o e-money issuer para magawan ito ng karampatang aksyon.

At kung aksidenteng na-click ang link,



makipag ugnayan sa iyong bangko o e-money issuer para malaman ang mga dapat gawin.

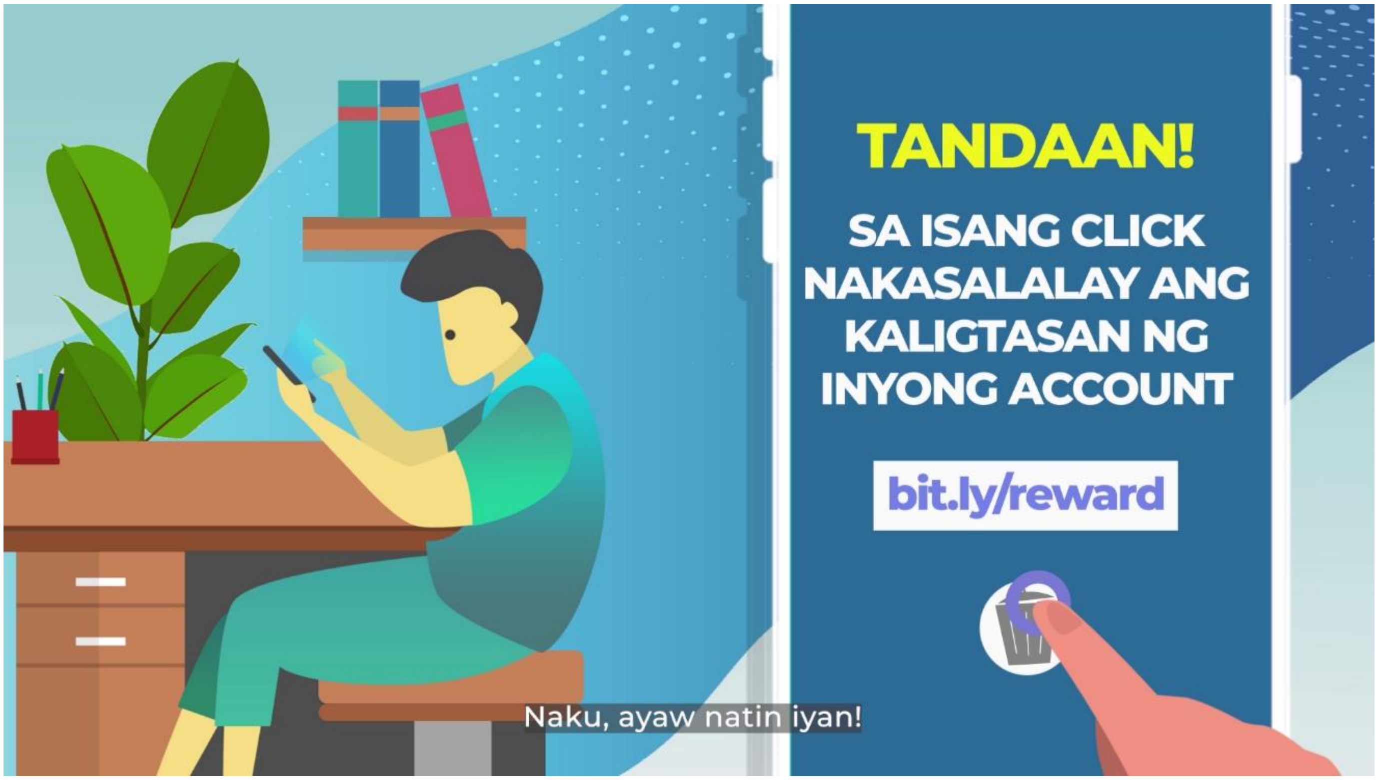
Palitan din agad ang iyong password.

Patuloy na nakikipagtulungan ang Bangko Sentral ng Pilipinas, sa mga bangko, industry association, at iba't ibang ahensya ng pamahalaan. Para tugunan ang mga panlolokong tulad ng SMiShing.

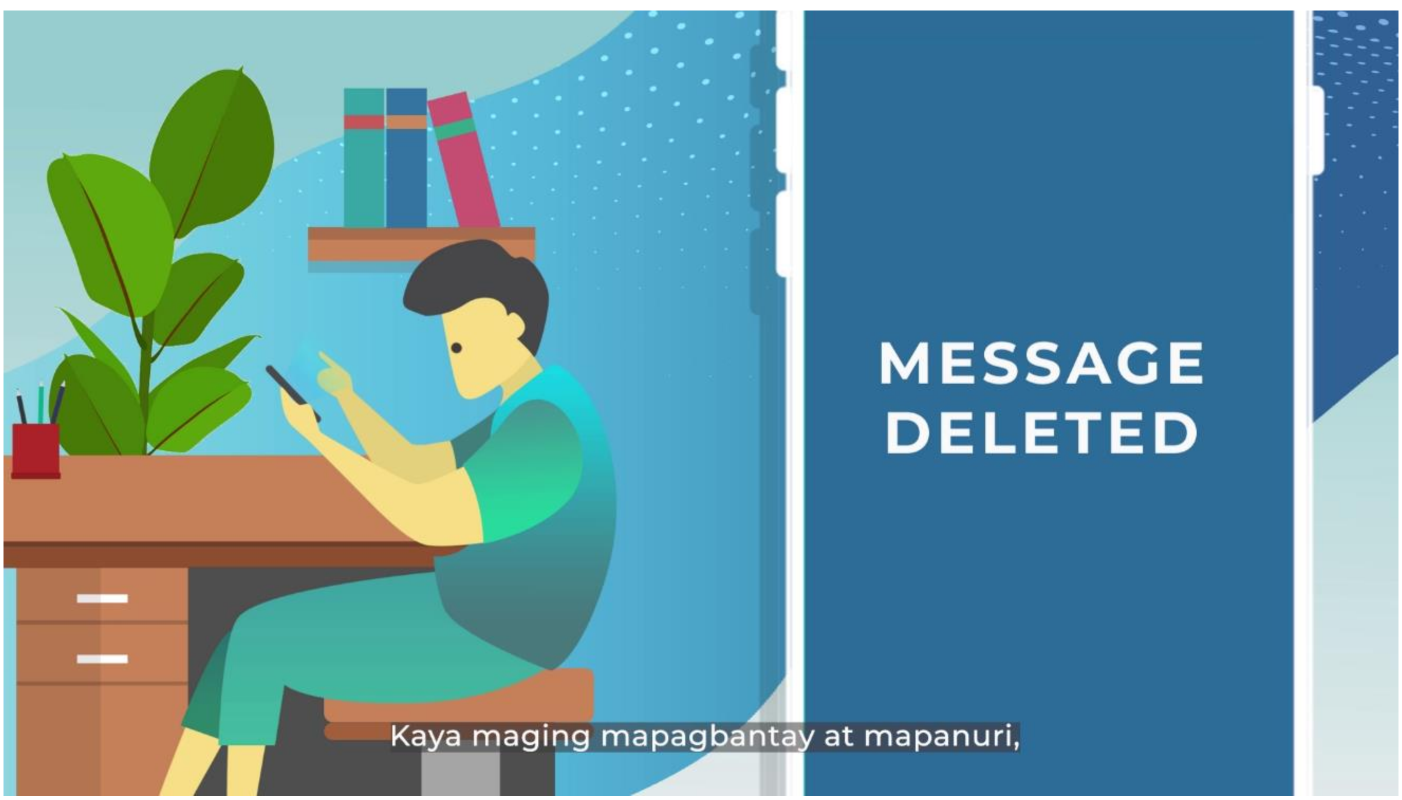
At palakasin ang cyber awareness ng mamamayan.

Laging tandaan, sa isang click, maaaring kaligtasan ng iyong account ang nakasalalay.

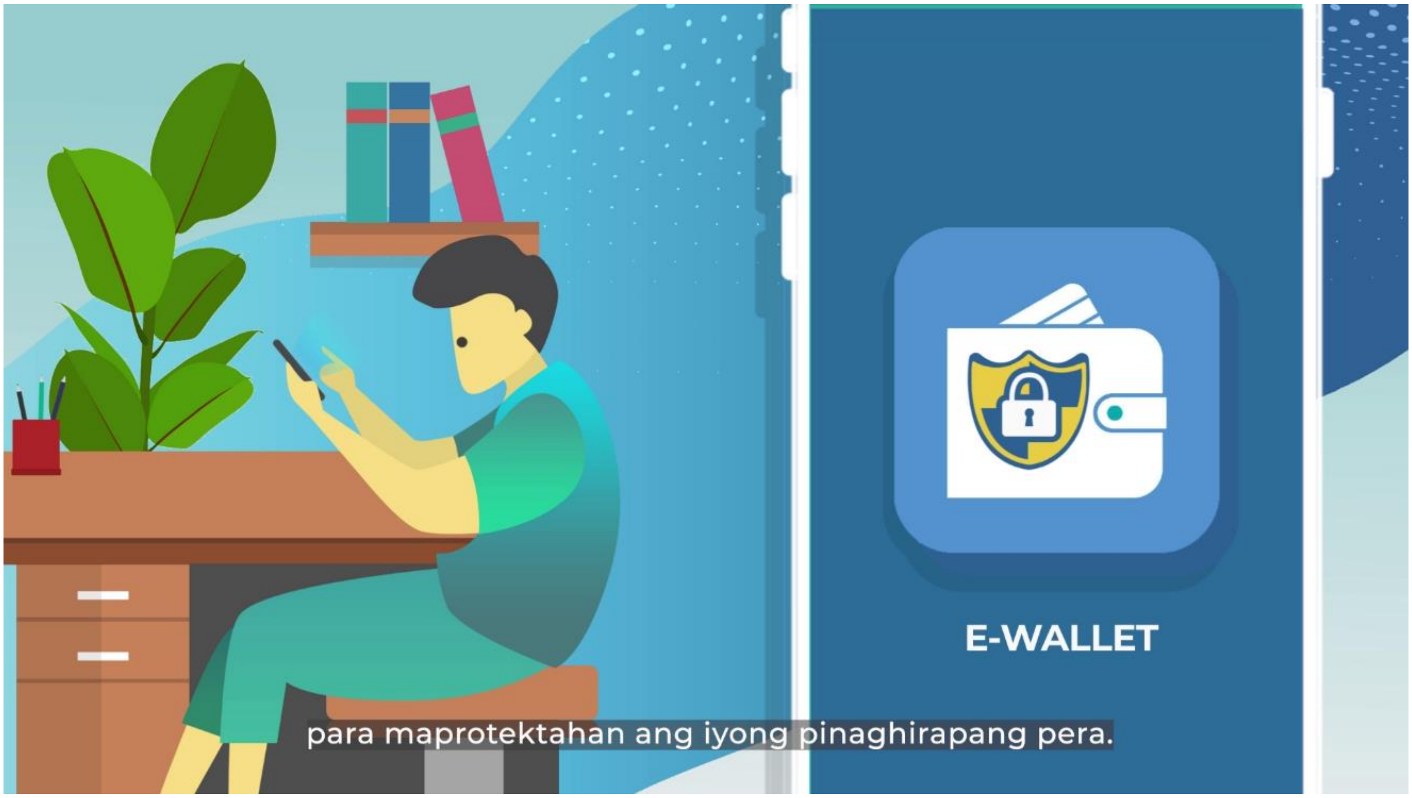
Naku, ayaw natin iyan!



Kaya maging mapagbantay at mapanuri.



Para ma protektahan ang iyong pinaghirapang pera.



Para sa mas ligtas na digital transaction.

Ugaliing mag **CPR, CHECK – PROTECT – REPORT!**

Ang materyales na ito ay mula sa BANGKO SENTRAL NG PILIPINAS

The link to the downloadable video file on SMiShing that carries BSP's CPR messaging is: **https://tinyurl.com/SMiShingCPR**