HEADQUARTERS
CYBERSPACE SECURITY GROUP
COMMUNICATIONS, ELECTRONICS AND INFORMATION SYSTEMS SERVICE
ARMED FORCES OF THE PHILIPPINES
Camp General Emilio Aguinaldo, Quezon City

CSG 16 August 2022

CYBERSECURITY BULLETIN: CSG, CEISSAFP-2022-01

Online Banking Fraud and Ways to Protect Yourself from It

1. Background:

Online banking fraud occurs when a criminal gains access to your credit/debit card number – and in some cases, personal identification number (PIN) – to make unauthorized purchases, money transfer or withdraw cash from your account. In the past two (2) years when all our activities had to be in the digital world due to the pandemic, the threat that hackers pose to our financial and social security become even more prominent.

On 16 August 2022, the Manila Bulletin published a report on alleged unauthorized transactions experienced by two (2) teachers who maintain payroll accounts with LandBank. The LandBank said that their initial investigation shows the device of the teachers, and their personal information were compromised by way of phishing – a scheme wherein hackers pretend to be legitimate banking representatives to obtain confidential bank details from clients and use it to infiltrate their accounts.

According to one (1) of the victims, he received a one-time password (OTP) verification 13 times and the next day, he found out that his P121,000.00 had been taken from his LandBank account and transferred to a digital wallet account.

Another teacher lost around P85,000.00 after the money was also transferred to an electronic wallet account and another bank account.

2. The most common Types of ATM Frauds:

a. **Skimming**: This type of ATM scam involves a skimmer device that criminals place on top of or within the card slot. To record your PIN number, the criminals may use a hidden camera or an overlay that covers the original PIN pad. Using the card numbers and PIN's they record; thieves create duplicate cards to withdraw money from consumers' accounts. Unlike losing your debit card or having it stolen, you won't realize anything is amiss until unauthorized transactions take place.

b. **Shimming**: This is the latest update to skimming. Instead of reading your card number, criminals place a shimming device deep inside the ATM to record your card's chip information. The result is the same as skimming because thieves use the stolen chip data to create "cloned" versions of your debit card.

c. **Cash-out**: This scam targets multiple accounts from the same financial institution. Armed with a hacked bank employee's credentials, the criminal alters account balances and withdrawal limits. Using stolen debit card numbers captured from a separate skimming attack, they can "cash out" the ATM until it's out of money.

d. **Jackpotting**: While there are multiple types of jackpotting attacks, typically, these incidents involve gaining physical access to the inside of the machine. The criminals may replace hardware or install malicious software giving them control of the cash dispensing function. Jackpotting is like a cash out scam, but it does not require the criminal to have any customer account details or stolen debit card information.

e.

3. Ways to Protect Yourself:

a. Signup for online banking and make it a habit to review your account activity online and monitor your account for suspicious activity. If you see anything suspicious, immediately report it to the bank.

b. Always log-out from your online session once you are finished with your transaction.

c. Protect your mobile devices. Following are tips on how to protect your mobile devices from hackers:

1) Change your default passcode. Change your code to something more complex.
2) Never leave your mobile device unattended.
3) Avoid using unprotected Bluetooth networks and turn off your Bluetooth service when you are not using it.
4) Use protected app to store your PIN and card information.
5) Avoid unsecured Public WiFi.
6) Turn off autocomplete feature and regularly delete your browsing history, cookies, and cache.
7) Use security app that increases protection.

d. Avoid making purchases with your debit card. Use a credit card, which offers greater protection against fraud, rather than a debit card.

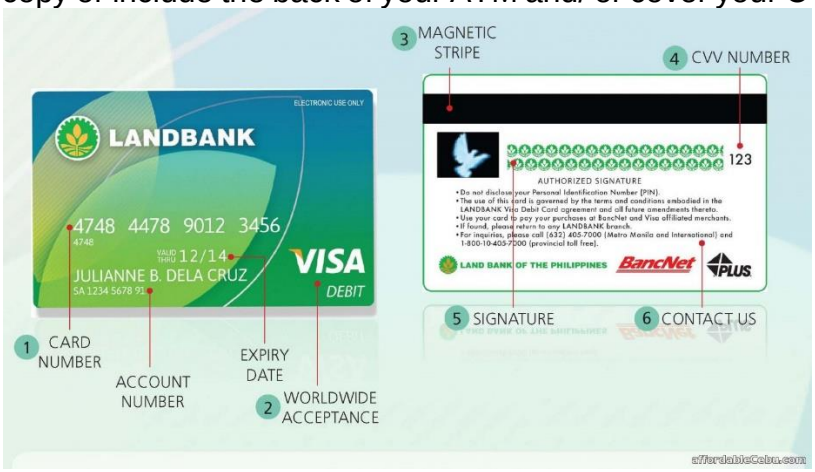
e. Destroy old debit cards. Your old card floating around your information at risk. Prevent hackers from getting access to your personal/sensitive information.

f. If your debit card is lost or stolen, or you believe sensitive information such as your PIN, card number, or online banking login has been compromised, call your bank right away.

g. Watch out for anything suspicious on the ATM. Shake the card reader or PIN pad to ensure that there are no foreign objects attached to it.

h. Be vigilant of your surroundings when approaching and using an ATM. Make it habit to cover your hand and pin pad as you enter your PIN on the ATM.

i. If you have government/business transaction needs a photocopy of your ATM. Do not photocopy or include the back of your ATM and/ or cover your CVV Number.



j. Beware of phishing scams. When checking your email or doing business online, make sure you know who you are interacting with. An identity thief may set up phishing website that looks like it belongs to your bank or another business you have an account with. Scammer is looking to get access to your personal information and may attempt to access your bank account.

4. Dissemination:

The information provided is intended to increase the security awareness of AFP personnel about online banking fraud and help them understand the perspective or motive of cybercriminal and ways to protect yourself from fraudsters. All units and offices are given permission and are encouraged to redistribute this bulletin in whole educational, non-commercial purposes.

References:

https://newsinfo.inquirer.net/1544416/landbank-says-banking-systems-are-secured-as-teachers-accounts-were-hacked-via-phishing

https://www.securitybank.com/blog/10-ways-to-protect-yourself-against-debit-card-fraud/

https://www.landbank.com/online-security-policy

https://www.investopedia.com/articles/pf/09/debit-card-fraud-at-risk.asp

https://www.webroot.com/us/en/resources/tips-articles/how-to-prevent-phone-hacking-and-sleep-like-a-baby-again

https://www.ublocal.com/atm-fraud/#:~:text=Shimming%3A%20This%20is%20the%20latest,versions%20of%20your%20debit%20card.