HEADQUARTERS
ARMED FORCES OF THE PHILIPPINES CYBER GROUP
Camp General Emilio Aguinaldo, Quezon City

CYBERSECURITY BULLETIN: 2022-12

ONLINE BANKING FRAUD AND WAYS TO PROTECT YOURSELF FROM IT

1. Background

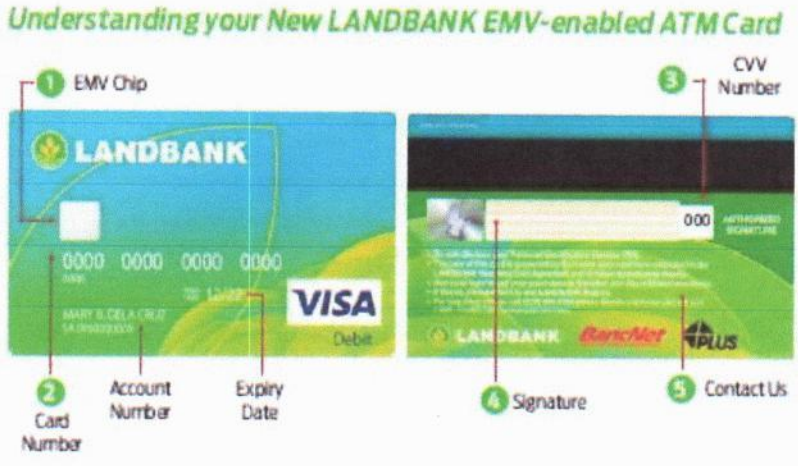
Online banking fraud occurs when a criminal gains access to your credit/debit card number – and in some cases, personal identification number (PIN) – to make unauthorized purchases, money transfers or withdraw cash from your account. In the past two years when all our activities had to be in the digital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

According to one of the victims, he received a one-time password (OTP) verification 13 times and the next day, he found out that 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.

Furthermore, back in 2018, a netizen by the name of Cho Mel warned military personnel and civilians who posted pictures of and photocopies their Land Bank of the Philippines (LBP) Automatic Teller Machine (ATM) cards. It is described in the post that to use your ATM card for online transactions, all you need to provide is the card number, the expiration date and the three-digit Card Verification Value (CVV) number. This is applicable to online shopping applications, flight and hotel bookings, online food deliveries, and even purchasing in-game credits for online games. This meant that this kind of fraud already existed even before the pandemic happened.



2. Common Types of ATM Fraud

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.

3. Important Parts of an ATM Card

In order to prevent being a victim of an ATM fraud specially online, everyone should not disclose these important parts.

a. Card Number: The card number is one of the most important parts of your card. It identifies your account with the card issuer, and those are the digits you need to provide when making purchases online or by phone. It's typically 16 digits, though some manufacturers use as little as 14 or as many as 19.

b. Cardholder's Name: This is the person authorized to use the card. That person did not necessarily open the account; they may simply have access to it as an "authorized user." Only authorized card users can make purchases with a debit or credit card, and merchants are encouraged to ask for ID before accepting payment with a card.

c. Smart Chips: These tiny metal processors make cards more secure than traditional magnetic-stripe-only cards. Chips make it harder for thieves to use stolen credit card numbers.

d. Expiration Date: You need to replace your card periodically. The move to smarter cards is just one reason banks issue new cards. Your expiration date is important because vendors may require it when you make purchases online or over the phone. Banks typically mail out new cards shortly before the old ones expire.

e. Magnetic Stripe: This black strip contains information about you and your card, and specialized devices known as card readers gather that information. Every time you swipe your card at a merchant, you run the magnetic stripe through a card reader to provide your payment details. Magnetic stripes include your name, card number, expiration date, and other details. If that information is stolen (whether hackers steal the data or a dishonest merchant runs your card through a card skimming device), the thief can use it to create a fake card with a magnetic stripe that matches your card.

f. Security Codes: Cards are printed with an additional code to help ensure that anybody using the card number has a legitimate, original card. For payments online or by phone, merchants typically require more than just the card number and expiration date from the front of your card. The security code on the back creates an additional hurdle for hackers who may have stolen your card number from merchant systems or with the help of a skimmer.

Security codes might be referred to as CVV, CVV2, CVC, CSC, CID, or other similar names. Most websites just ask for a "security code" and provide a small box for you to type the code into. On Visa, MasterCard, and Discover cards, the code is a three-digit code on the back of your card. The preceding four digits ("3456" in the image above) are the last four digits of your card number. On American Express cards,

the security code is a four-digit code on the front of the card. Look above your card number on the right side of the card.

Your security code, like all the other numbers on your card, is a critical piece of information. Don't share that code unless it's necessary for making a payment to somebody you trust.

4. Recommendations

Protect yourself from skimming, phishing, and other forms of ATM fraud by following these tips:

a. Sign up 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 of your online session once you are finished with your transaction.

c. Safeguard your mobile devices. The 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 a protected app to store your PIN and card information.
5) Avoid using unsecured Public WiFi.
6) Turn off the autocomplete feature and regularly delete your browsing history, cookies, and cache.
7) Use a 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. Discard old debit cards. Your old card is floating around with 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 or business transaction that needs a photocopy of your ATM. Do not photocopy or include the back of your ATM and/or cover your CVV number.

j. Make sure everyone in the organization knows how to avoid cybersecurity threats and risks. Organizations should invest in educating their employees about basic security practices, such as secure password tips and how to identify phishing emails. This type of education should be conducted frequently because of the ever-evolving threats.

4. Dissemination

The information provided is intended to increase the security awareness of AFP personnel and to help them behave more securely within their work environment. The increased awareness is intended to help improve the organization's overall cybersecurity posture. All units and offices are given permission and are encouraged to redistribute this bulletin that will benefit the AFP organization as a whole for educational, and non-commercial purposes.

References:

- *https://www.thebalance.com/parts-of-a-debit-or-credit-card-front-and-back-315489*
- *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*