Additional Information:

What is Skimming?

"Skimming" is a type of fraud associated with duplicate bank card creation due to the use of special devices for unauthorized reading of magnetic stripe data ("skimmers") installed on ATMs and similar in type of self-service terminals.

Skimmer

Skimmer is an overlay inside which there is a device that reads information from the magnetic strip of the payment card. In the future, this information will be used to make a duplicate card. Typically, skimmers are attached to the ATM to find out the PIN code, scammers use hidden video cameras and overhead keyboards.

Skimming devices

Overlay card reader

The overlay on the card reader is a skimming device made in the form of a card reader, intended for copying data from a chip or a magnetic strip of a card.

EPP Keyboard Cover

The EPP keyboard cover is a skimming device made in the form of an EPP keypad designed to copy the PIN code of a bank card.

Video camera

Video Camera - concealed device manufactured in the form of various bank supplies: parts ATM (card reader, cash dispenser lining on walls, wall paper holders, etc.). It is designed to record a PIN code of a bank card.

Other types of fraud
Lebanese loop

The Lebanese loop is a device for blocking the card reader, it is made as a loop from an old film, designed to steal bank cards.

Operating principle

1. The fraudster inserts a loop into the card reader.
2. When you enter a bank card into the card reader, the next customer, the card rests against a loop.
3. The swindler is nearby and comes first to help.
4. He explains that he already faced this situation and knows the method of drawing the map.
5. The method consists in reintroducing a PIN code or introducing a combination of digits, "*", "#" And a PIN (* 1 * PIN #)
6. When the card does not appear, the fraudster claims that the method has acted in the past or operates on another kind of ATM (in another bank).
7. The client leaves
8. The fraudster takes the card

Trapper

Trapper - a device for blocking the tent curtain, is made in the form of sticky overlays, designed to steal the money

Operating principle

1. Scammers put the trapper in the tent curtains
2. When trying to withdraw money from ATM, money is stuck to the overlays
3. The ATM can not give out money or draw it back
4. The client leaves, thinking that the ATM is not working.
5. The swindler takes money and lining

Protection measures

General provision

When suspicious devices are detected, contact the bank's security staff. Do not attempt to remove the device data yourself.

Anti-skimming

Anti-Simming - a device made in the form of an overlay on the card reader, prevents the installation of a skimming card reader.

Note: Anti-camming is very similar to skimming card reader. Having seen it on one ATM, the client can take a skimming card reader for an anti-immigration device on another device.

Installation in offices

Installation in offices of enterprises having a credit of trust.

Monitoring

1. Employees of offices where ATMs are installed should inspect ATM every three hours.
2. If you find suspicious devices, contact the security staff.
3. Do not attempt to remove suspicious devices yourself.

Note: Pay special attention to the card reader, EPP keyboard, tent devices and "extra" accessories (booklets, canopies, etc.)

Video invigilation
Video invigilation for ATM interface.

Precautions for bank customers

• Inspect the front of the cash dispenser, for extraneous devices in the form of advertising booklets, overlays on the card reader, PIN-keyboard and other foreign objects.
• When covering transactions with a bank card, cover the PIN-keyboard.
• Set the SMS alert function to the card account
• Set a limit for day operations with bank card money.

PHISHING

What is "phishing"?

Phishing - a kind of Internet fraud, the purpose of which is to obtain user identification data. These include the theft of passwords, payment card numbers, bank accounts and other confidential information.

Phishing is a fake message that came to the post from banks, providers, payment systems and other organizations that for some reason the recipient urgently needs to transfer / update personal data. The reasons can be called different. It can be loss of data, breakage in the system and so on.

Attacks of phishers are becoming more thoughtful, methods of social engineering are applied. But in any case, the client is trying to scare, to come up with a critical reason for him to give out his personal information. Typically, messages contain threats, for example, block the account if the recipient does not fulfill the requirements set forth in the message (for example, if you do not provide your details within a week, your account will be blocked). Often, as a reason why a user ostensibly must give out confidential information, phishers call the need to improve anti-phishing systems (for example, if you want to protect yourself from phishing, click on this link and enter your login and password)

CJSC “Bank of Asia” officially informs cardholders that under no circumstances will they request information via e-mail intended for identification of cardholders (PIN-code to the Card, payment card number, mailbox authorization, codeword, CVV2 number, as well as other personal information of the holder) and strongly recommends that you remove the newsletter offering to reveal sensitive information on your Maps.

WISHING

Wishing - a relatively new type of fraud, the first cases of which were reported in 2006. The essence of the method is the theft of personal data relating to a credit card, and the method itself comes from a phishing that is known to everyone and is obsolete and losing its effectiveness**.**

Wishing scams are based on methods of social engineering, when the victim personally sends all the necessary data, almost without enforcement, requests or threats. The essence of the method is that the victim's phone rings when answering, to which the pre-recorded message is played, that there are some problems with servicing the payment card and for their elimination, it is necessary to call back to the number indicated in the message. If you call this number, the exact same answering machine will ask you to dial the card number from the phone keypad or leave other personal information necessary to identify the user. Thus, attackers receive all the necessary information used to perform operations with the victim's credit card.

It should be noted that Internet telephony and the VoIP communication protocol are used for the phishing, which allows reducing communication costs for companies and individual users, but at the same time making it impossible to track the number and location of the subscriber. Thus, scammers get an excellent opportunity to maintain their confidentiality.

How to understand that you are trying to involve in a fraud?

If your phone receives a call allegedly from the bank and a characteristic voice in the record asks you to call back to some number, while not using your name and surname, and using the words "you", "dear customer", etc. for circulation . with a high degree of probability - this is a trick of intruders. A self-respecting bank strives to maintain confidentiality and confidential relations with the client, so when calling, the operator should introduce himself and address to you by name and patronymic, if necessary, independently identify the identification number or other information that only you and the bank know about.

On the reverse side of the payment card the phone numbers of the bank branches are indicated and if there are any doubts, you can independently contact the bank and clarify the situation.

Ways of protection

Despite the fact that many years have passed since 2006, no software or technological methods of protection against vishing have appeared. The best and only way to protect is your intuition and judgment, which makes it clear that you have been attacked by scammers.

To protect against цishing, you should follow simple rules:

- When you receive a suspicious call, immediately call the bank and clarify the situation;
- Do not call the number dictated in the message and do not give out any personal information;
- Be careful when transferring any personal data through the Internet, telephone, etc .;
- Regularly monitor the status of your account, monitor all spending on the card;
- Be vigilant, observe safety rules and regularly monitor the status of your account, only in this way you can guarantee your own financial security.

PHARMING

No matter how dangerous phishing and wishing, the web is even more insidious threat - pharming. This is a redirection of the victim to a false address. "An attacker spoils the navigation infrastructure on which the browser depends, and takes over some of it. This can be a local version, a hosts file, or a domain name system (DNS) used by an Internet provider to point the browser at the desired object, "says Peter Cassidy, secretary general of Anti-Phishing.org.

How does this happen? The mechanism of pharming has much in common with the standard virus infection. The victim opens an unsolicited e-mail message or visits a web server with an executable file that is secretly launched in the background. This distorts the hosts1 file. The operation takes only a second, but malware can contain URLs of many banking structures. The redirection mechanism is activated at the moment when the user dials a familiar trusted address corresponding to his bank ... and gets on one of the false sites.

Special mechanisms for protection from pharming now simply do not exist, so you need to carefully monitor incoming mail, regularly update the anti-virus database, close the preview window in the mail client, etc.