Phishing

Frequently Asked Questions

ABA Bank pays great attention to the customers' security and makes every effort to ensure that the cooperation between the bank and the customer is comfortable and safe. In this paper we tried to collect all the necessary knowledge and the Frequently Asked Questions about **phishing** - a type of online identity theft. Please, read this information and if there is any reason to suspect that you are a victim of fraud, contact the Bank immediately on +855 23 225 333.

What is phishing?

Phishing (pronounced "fishing") is a type of online identity theft. It uses e-mail and fraudulent websites that are designed to steal your personal data or information such as credit card numbers, passwords, account data, or other information.

How can I recognize phishing scam?

Phishing e-mail messages take a number of forms:

- They might appear to come from the bank or financial institution, a company you regularly do business with or from your social networking site.
- They might ask you to make a phone call. *Phone phishing* scams direct you to call a customer support phone number. A person or an audio response unit waits to take your account number, personal identification number, password, or other valuable personal data. The phone phisher might claim that your account will be closed or other problems could occur if you don't respond.
- They might include official-looking logos and other identifying information taken directly from legitimate websites, and they might include convincing details about your personal information that scammers found on your social networking pages.
- They might include links to spoofed websites where you are asked to enter personal information.

Example of a phishing e-mail message, which includes a deceptive Web address that links to a scam website.

To make these phishing e-mail messages look even more legitimate, the scam artists may place a link in them that appears to go to the legitimate website (1), but actually takes you to a phony scam site (2) or possibly a pop-up window that looks exactly like the official site.

Here are few phrases to look for if you think an e-mail message is a phishing scam:

"Verify your account"

Bank never asks you to send passwords, login names, or other personal information through e-mail.

If you receive an e-mail message from the name of ABA Bank, asking you to update your information, do not respond — this is a phishing scam.

"You have won the lottery"

The lottery scam is a common phishing scam known as the advanced fee fraud. One of the most common forms of advanced fee fraud is a message that claims you have won a large sum of money, or that a person will pay you a large sum of money for little or no work on your part. The lottery scam often includes references to big companies.

"If you don't respond within 48 hours, your account will be closed"

These messages convey a sense of urgency so that you'll respond immediately without thinking. A phishing e-mail message might even claim that your response is required because your account might have been compromised.

What should I do if I receive an e-mail phishing scam?

- **If an e-mail looks suspicious,** don't risk your personal information by responding to it.
- **Delete junk e-mail messages** without opening them. Sometimes even opening spam can alert spammers or put an unprotected computer at risk.
- **Do not reply to e-mail** unless you're certain that the message comes from a legitimate source. This includes not responding to messages that offer an option "Remove me from your list".
- **Do not "unsubscribe"** unless the mail is from a known or trusted sender.
- **Use the junk mail tools in your e-mail program.**

How do I report a possible phishing scam?

Please, forward suspicious e-mails or details of text messages that ask for your personal information to info@ababank.com and then delete it from your inbox without responding.

Or, please, call us as soon as possible on +855 23 225 333.

What should I do if I think I've responded to a phishing scam?

If you suspect that you've responded to a phishing scam with personal or financial information, take these steps to minimize any damage.

Step 1: Report the incident;

Step 2: Change all your passwords;

Step 3: Routinely review your statements;

Step 4: Use the most up-to-date software with spam and antiphishing capabilities, antivirus and antispyware software.

How do scammers get my e-mail address or know which bank I use?

Criminals who send out phishing scams (often called "phishers") send out millions of messages to randomly generated e-mail addresses. They fake or "spoof" popular companies in order to fool the largest number of people.

Can an e-mail message that contains a company's official logo be a phishing scam?

Yes. Phishing scams often use the official logos of the companies they're trying to spoof. If you think an e-mail message is a phishing scam, delete it, or type the web addresses directly into your browser, or use your personal bookmarks.

I received an e-mail message that requests banking information. Is it a phishing scam?

Any e-mail message that requests banking information is probably a phishing scam. Bank will not request this information by e-mail.
If you receive a message to an e-mail address that is not the one you use to log in to your bank account, this is probably a phishing scam.

What can I do to help prevent identity theft from phishing scam?

You can do the following to help protect yourself from phishing scams:

- Delete spam. Do not open it or reply to it, even to ask to be removed from a mailing list. When you reply, you confirm to the senders that they have reached an active e-mail account.

- Use caution when you click links in an e-mail message, text message, pop-up window, or instant message. Instead, type Web addresses in a Web browser, or use your online bookmarks.
- Do not open e-mail attachments or click instant message download links, unless you know who sent the message and you were expecting the attachment or link.
- Be cautious about providing your personal or financial information online. Do not fill out forms in e-mail messages that ask for personal or financial information.
- Create strong passwords and avoid using the same password for your bank and other important accounts.
- Make sure your computer's firewall is turned on and that you use antivirus software, which should also be regularly updated.
- Check your bank and credit card statements closely to identify and report any transactions that are not legitimate.
- Never pay bills, bank, shop, or conduct other financial transactions on a public or shared computer, or over a public wireless network. If you do log on to public computers, look for computers on networks that require a password, which increases security.

What should I do if I notice suspicious activity?

If you think an e-mail message might be fraudulent, we recommend taking the following precautions:

- Delete the message, do not respond or click links in it.
- Report any suspicious activity (see above for contact information).
- Fraudulent e-mail messages sometimes contain unwanted or malicious software (also known as malware). If you think you might have malware on your computer, scan your computer to check for and remove unwanted software.