

SBA PRESS RELEASE:

SBA Warns of Fraudulent Attempts to Obtain Bank Account Information from Small Businesses

WASHINGTON – The U.S. Small Business Administration issued a scam alert today to small businesses, warning them not to respond to letters falsely claiming to have been sent by the SBA asking for bank account information in order to qualify them for federal tax rebates.

The fraudulent letters were sent out with what appears to be an SBA letterhead to small businesses across the country, advising recipients that they may be eligible for a tax rebate under the Economic Stimulus Act, and that SBA is assessing their eligibility for such a rebate. The letter asks the small business to provide the name of its bank and account number.

These letters have not been sent by or authorized by the SBA, and all small businesses are strongly advised not to respond to them.

The scheme is similar in many ways to e-mail scams often referred to as “phishing” that seek personal data and financial account information that enables another party to access and individual’s bank accounts or to engage in identity theft.

The SBA is working with the SBA Office of Inspector General to investigate this matter. The Office of Inspector General asks that anyone who receives such a letter report it to the OIG Fraud Line at 1 (800) 767-0385, or e-mail at OIGHotline@sba.gov.

###

(more tips below)

Watch out for Phishing!

Fraudulent Email and Phone Scams and How to Avoid them

Protect Yourself!

1. Do not provide any confidential information in suspicious emails or websites.
2. Protect your online banking username, password, and answers to security questions. Do not write them down or share them with anyone.
3. Install, Run, and keep anti-virus software updated.

Fraudulent Emails (phishing)

Phishing is usually a two-part scam involving emails and spoof websites. Fraudsters, or Phishers, send email to a wide audience that appears to come from a reputable company. This is known as a phish email.

In the phish email, there are links to spoof websites that spoof (imitate) a reputable company's website. Fraudsters hope to convince victims to provide their personal information by using clever and compelling language, such as an urgent need for you to update your information immediately or a need to communicate with you for your own safety or security.

Once obtained, personal information can be used to steal money or transfer stolen money into another account.

How fraudsters obtain email addresses

Fraudsters obtain email addresses from many places on the internet. They also purchase email lists and sometimes guess email addresses. Fraudsters generally have no idea if people to whom they send bank-related phish emails are actual bank customers- they just hope that a percentage of them will be received by actual bank customers.

If you receive a fraudulent email that appears to come from Country Club Bank, **this does not mean that your email address, name, or any other information has been taken from Country Club Bank's systems.**

Fraudulent Websites (phishing or spoof websites)

Online fraudsters may attempt to direct you to fraudulent websites via emails and pop-up windows. These websites are used to try to obtain your personal information. One way to detect a phony website is to consider how you go to the site. You may have followed a link in a fraudulent email requesting your account information. Therefore, you should not click on any links in suspicious emails or pop-up windows.

Pop-up Windows Activation

Fraudsters may use pop-up windows- small windows or ads- to obtain personal information. These windows may be generated by programs hidden in free downloads such as screen savers or music-sharing software. While many of these programs are harmless, some contain potentially harmful Trojan horse programs that monitor your web viewing activity.

Country Club Bank does not use pop-up windows to request customer account information.

All of our pop-up windows are user-initiated. We will never display a pop-up window on our site that you haven't requested by clicking on a link.

Fraudsters try to locate and defraud potential victims using various means, such as USPS mail, telephone calls, faxes, and online chat rooms. Once they contact potential victims, fraudsters use compelling language and scenarios to scam them.

If you are involved in a situation that fits one of the following descriptions, it could be a scam and you should contact Country Club Bank immediately.

Job scams: You accept a job in which you are paid to receive a commission to facilitate money transfers through your account or apply for a job that asks you to set up a new bank account.

Job scammers use reputable online job boards to offer work-at-home jobs or accounting positions. These job scams may require employees to receive money into their existing bank account (or open new accounts) and then transfer the money to another account, often overseas. As payment, the job seeker is instructed to keep a small percentage of the transfer.

Lottery or sweepstakes scams: You receive notice that you are the winner of a lottery that you did not enter, but must pay a small percentage for fake taxes or other fees before you can receive the rest of your prize.

Dating scams: Someone you met through an online dating site or chat room asks you to send money for a variety of reasons, including a need for urgent surgery or to make travel arrangements to meet in person.

Internet scams: You receive a check for something you sold over the internet, but the amount of the check is more than the selling price. You are instructed to deposit the check, but send back the difference in cash.

OR

You receive a check from a business or individual different from the person buying your item or product.

OR

You are instructed to transfer money, or receive a transfer of money, as soon as possible.

Telephone scams: Unless you initiated the contact, do not give out personal information over the telephone. *If the call is not initiated by you, always ask for a call-back number.*

Remember, if it sounds too good to be true, it probably is.

Scam Prevention Tips

- First and foremost, use common sense. If it sounds too good to be true, it probably is.
- Never give personal information to a stranger who contacts you, whether by telephone, email, or other means.
- Don't accept payments for more than the amount of the service with the understanding that you send the buyer the difference.
- Don't accept checks from individuals you've only met online.
- Don't accept jobs in which you are paid or receive commission for facilitating money transfers through your account.
- No matter how urgent someone claims a deal is, you can always wait a few days to research and confirm legitimacy. Time is on your side, not the fraudster's.
- You are ultimately responsible and liable for all deposits made into your account, whether they are a check, money order, transfer, etc.