BANK OF AMERICA

GLOBAL INFORMATION SECURITY

Be Cyber Secure: Vishing

Criminals use phone calls, called “vishing” or voice phishing, to steal information and money. Here’s how you can avoid falling for the latest tricks.

It usually comes as a phone call that sounds urgent or alarming. An unsolicited caller tells you your bank account has been compromised, and that they need your PIN so they can verify your identity or unlock the account. Or they say they’re from a government agency, such as the IRS or the Social Security Administration. Sometimes they insist you owe money. Or they might announce you’re a lucky winner — but you’ll need to pay for shipping and handling to claim your prize.

These are all examples of “vishing,” a term that combines “voice” and “phishing” to describe a scam that relies on either a mobile or landline phone. Phishing refers to any attempt by cyber criminals to steal money or personal information from people through deceptive practices. It can also be perpetrated through email and short message or texting systems (known as “smishing”).

Criminals continue to use vishing techniques because they realize that talking quickly and persuasively can catch many people off guard. While some of these attempts are easy to detect, others are subtle enough to fool even cautious consumers, especially when the caller makes it seem like urgent action is needed.

Defining the terms

Phishing:

A common social engineering method where seemingly legitimate messages are sent via email or messaging platforms.

Vishing:

A cyber criminal impersonates a trusted source or utilizes tactics such as robocalls, to scam people out of data and money over the phone.

Smishing:

Utilizes SMS and messaging apps to scam people out of data and money.

Spoofing:

Disguises communications in order to appear to be from someone else, including legitimate businesses or employees. Cyber criminals can spoof emails, phones numbers and websites.

BANK OF AMERICA

How to stay safe from vishing scams

There are a few simple but critical rules to remember before you answer an unsolicited call:

- Don't answer calls from numbers you don't recognize. Bear in mind, however, that vishing scammers sometimes leave voicemails with a callback number. Do not call a number back without checking to see if it belongs to a business you know. Note that most government agencies, such as the IRS, will not call you unless they have contacted you by mail first.
- Do not trust caller ID numbers. Criminals are routinely spoofing legitimate numbers of established companies and services.
- If you are suspicious, even if you recognize the caller's organization, hang up before you give out any information or do not answer. If you think the call might be legitimate, call back a number you've verified independently — do not use your callback function. For instance, you should hang up on a caller who says they are with Bank of America but is not your normal contact.
- Do not give any caller personal or company Information, even if they know some of your personal information already. Scammers can steal personal information from other sources or find it on the dark web and will use what they know to trick you into giving them more. The fact that a caller knows something about you or your company is not enough of a reason for you to trust them.
- Remember that Bank of America, like many businesses, will never ask you for account or CashPro®, Online Banking or Private Bank credentials unless you call us first.