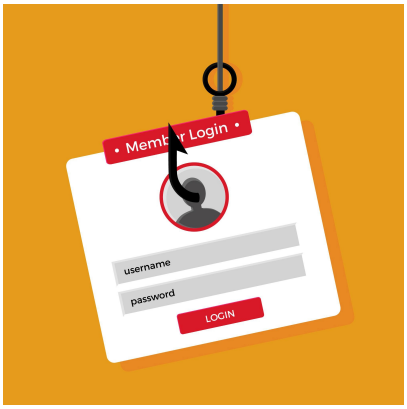

How to catch a vish

Description

Our forensic team was alerted to numerous AfroCentric colleagues recently falling victim to scams by fraudsters posing as clients or even high-ranking government officials such as the Minister of Heath.

Playing on emotion, these fraudsters all claimed to be stuck in a particular predicament and needed urgent personal assistance by way of transferring cash to them on the spot. This is a scam known as vishing.

What is vishing?

Vishing – or voice phishing – is the use of fraudulent phone calls to trick people into giving money or sharing personal information. It’s a new name for an old problem – telephone scams.

Vishing frequently involves a criminal pretending to represent a trusted institution, company or government agency. You may even be asked to buy an extended warranty, offered a so-called free vacation, told your computer is infected and you need anti-virus software, or be asked to donate to charity.

Learn to recognise a vish

Scammers or “vishers” often offer exaggerated or fake prizes, products or services. They then ask for your credit card number or other personal information to get you to pay for associated fees.

Watch out for:

- Offers from companies you do not do business with and/or have not heard of
- An announcement that you have won a prize in a contest you did not enter
- Promises of unrealistic returns for your money

Pressure to make immediate decisions to give the caller what they want, which may include:

- Money
- Financial account information
- Personal information
- Organisational information, including names and contact information of colleagues

- Threats of consequences – such as fines or penalties – if you don’t provide money or information

- Unprofessional, hostile or even obscene language
- Unsolicited calls offering to help you with debt, unpaid taxes or previous cases of fraud

Protect yourself from voice phishing

- If a caller claims to be from an institution you do business with, such as your bank, and they ask for personal information (account numbers, etc.), hang up, find that institution’s phone number and call them to verify. If the call you received was fraudulent, report it!
- If a caller claims to be from a tech support company (often a well-known company or one with which you do business) and says they need to fix a security alert or a problem with your computer or bank account using remote desktop software (a client application that allows a “client” computer to connect to a “host” computer from a remote location), hang up.
- Do not pay fees for prizes or rewards offered by phone.
- Do not transfer money or make payments to individuals, even if they pose as the principal officer of a client scheme or claim to be a well-known person you may have heard of.
- Only scammers demand immediate payments using specific methods, such as prepaid gift cards, debit cards or bank transfers.
- Do not send money or give out personal information (such as credit card numbers and expiration dates, bank account numbers or dates of birth) in response to unsolicited phone calls from unfamiliar companies or unknown persons.

Category

1. Our Knowledge Centre