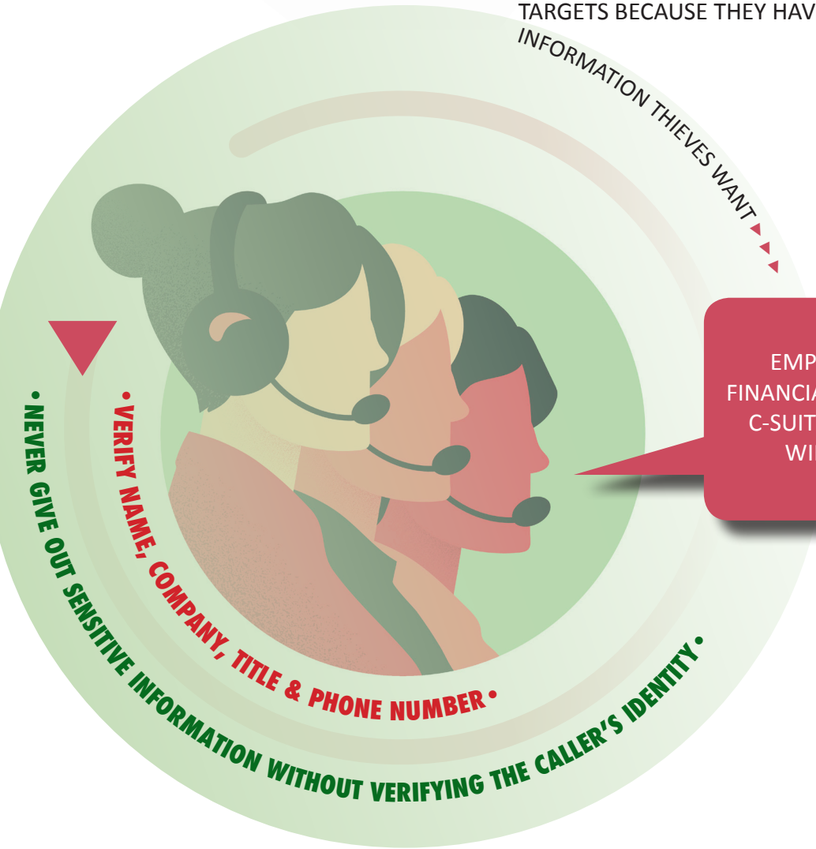
VISHING

PHISHING BY PHONE CALL

CUSTOMER SERVICE AND
IT HELP DESKS ARE FREQUENT
TARGETS BECAUSE THEY HAVE
INFORMATION THIEVES WANT



- NEVER GIVE OUT SENSITIVE INFORMATION WITHOUT VERIFYING THE CALLER'S IDENTITY
- VERIFY NAME, COMPANY, TITLE & PHONE NUMBER

EMAIL ADDRESSES
EMPLOYEE ID NUMBERS
FINANCIAL & ROUTING INFO
C-SUITE STAFF SCHEDULES
WIFI & INTERNET INFO
VENDOR NAMES

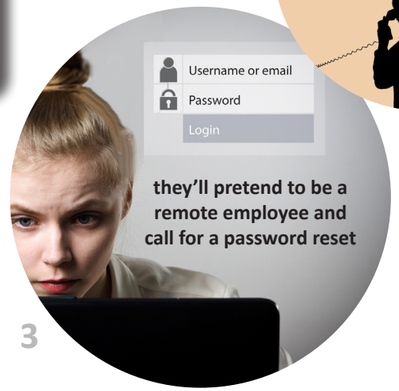
3
TACTICS
"VISHERS"
USE OFTEN

mehbmnph...

they'll mumble security answers they don't know hoping you'll accept a garbled response

they'll claim to be calling for a deaf person or someone with a disability, using this as an excuse for not knowing security answers

2



they'll pretend to be a remote employee and call for a password reset

3

POOR AUDIO, GRAMMAR & UNFAMILIAR DIALECTS FREQUENTLY INDICATE VISHING

[this is emergency call from bank your account has a comprised status and ..mmediate action equipment hold r banker have account numbers ready]

PHISHING BY TEXT MESSAGE

SMISHING

THINGS TO WATCH FOR TO AVOID BEING SMISHED:

A SENSE OF URGENCY

"respond immediately or your account will be closed!"

SUSPICIOUS LINKS

HTTP//getafreeweekend-getawayjustbyclickinghere

URGENT PASSWORD RESET REQUESTS

Your password has expired. You must log in immediately to change it.

IF YOU RECEIVE A TEXT OF THIS NATURE, DON'T CLICK ANY LINKS IN IT OR RESPOND. DELETE IT.