MISA. CABANGA. UNGABHALWA.

IZIMPAWU ZOKUKHWABANISA NOKUHWEBA NGOKWEZENHLALAKAHLE

BHEKA PHANSI:

1

Izilimi eziphuthumayo noma eziyingozi ("I-akhawunti yakho izovalwa ezinsukwini eziyi-24!")}

2

Izipesheli ezinhle kakhulu ukuze kube yiqiniso(Izimpopoli, imiklomelo, "imivuzo" mahhala

3

Izicelo zolwazi olubucayi (amagama okungena, imininingwane yezezimali, izinombolo ze-ID)

4

Umthumeli ongaziwa noma ikheli elinqunywe (libonakala lisondela kumgomo wenkampani yakho kodwa alikho)

okufanele ukwenze

- Ungachofozi izixhumanisi eziphazamisayo noma uvule okokufaka okungakulindelekile
- qinisekisa umthumeli ngalezi zindlela ezisemthethweni
- Bika ama-imeyili angaziwa ngokushesha ku-[security@company.com]

Khumbula:

2 I-Phishing kanye nezokuxhumana zikhomba abantu, hhayi izinhlelo. Hlalani ninophebezi. Vikelani nina. Vikelani inkampani.

STOP. THINK. DON'T GET HOOKED!

PHISHING & SOCIAL ENGINEERING RED FLAGS

BE ON THE LOOKOUT FOR:

1

Urgent or threatening language ("Your account will be locked in 24 hours!")

2

Too good to be true offers (Lotteries, prizes, "free" rewards

3

Requests for sensitive information (passwords, banking details, ID numbers)

4

Unfamiliar sender or spoofed address (looks close to your company domain but isn't)

What to do

- Do not click suspicious links or open unexpected attachments
- Verify the sender through official channels
- Report suspicious emails immediately to [security@company.com]

Remember:

Phishing and social engineering target people, not systems.
Stay alert. Protect yourself.
Protect the company.