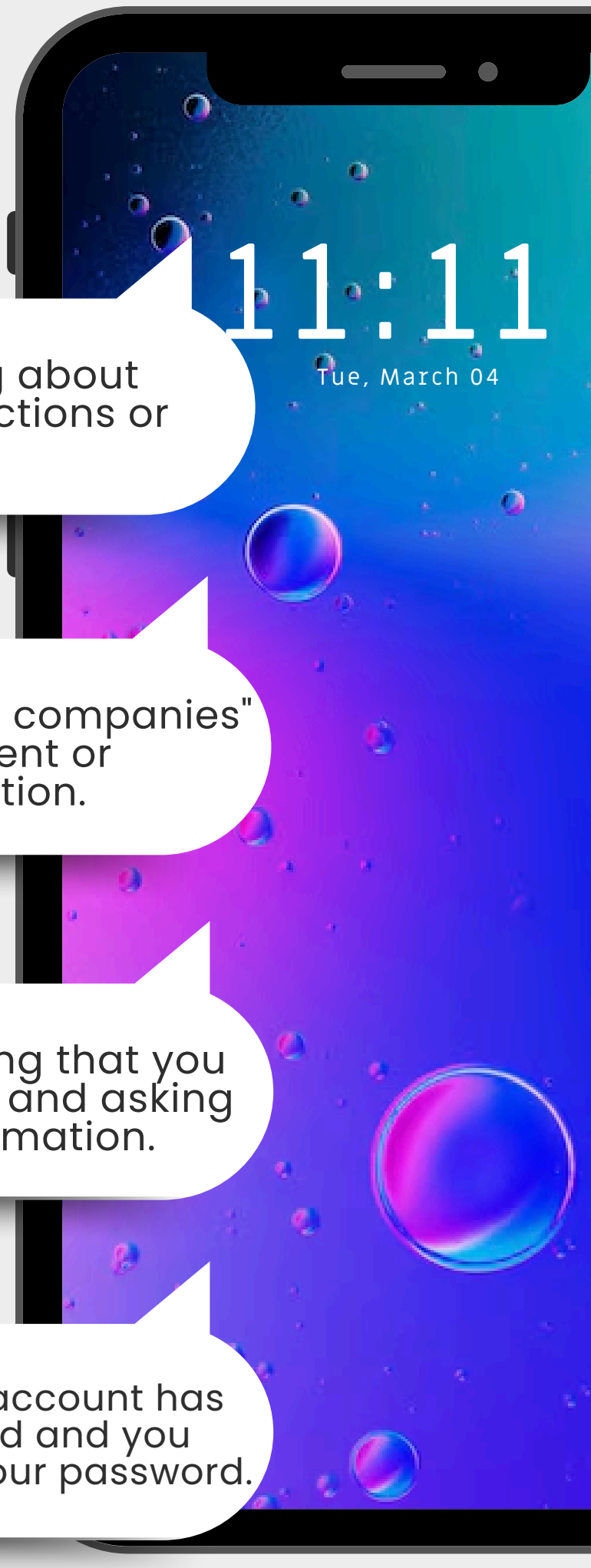
COMMON CASES OF SMISHING

AND HOW TO AVOID THEM.

Smishing is an SMS fraud where attackers impersonate trusted entities to steal data or infect devices via malicious links.



Banking notices

Messages alerting about suspicious transactions or account blocking.

Delivery packages

SMS from "courier companies" requesting payment or delivery confirmation.

Prizes and raffles

Messages claiming that you have won a prize and asking for personal information.

Technical support

Notices that your account has been compromised and you need to change your password.

HOW TO AVOID SMISHING?

- ✅ Don't click on suspicious links
- ✅ Check directly with the company or person
- ✅ Do not share personal information via SMS
- ✅ Enable two-factor authentication (2FA)

IF YOU RECEIVE A TEXT MESSAGE THAT SEEMS SUSPICIOUS, TRUST YOUR INSTINCT AND REPORT IT.

YOUR LOGO HERE

Grupo Smartekh | Security Culture Management