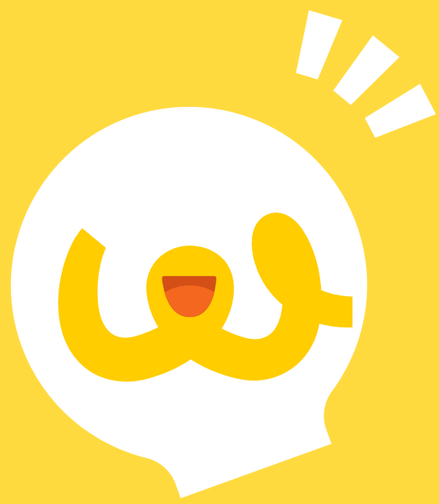
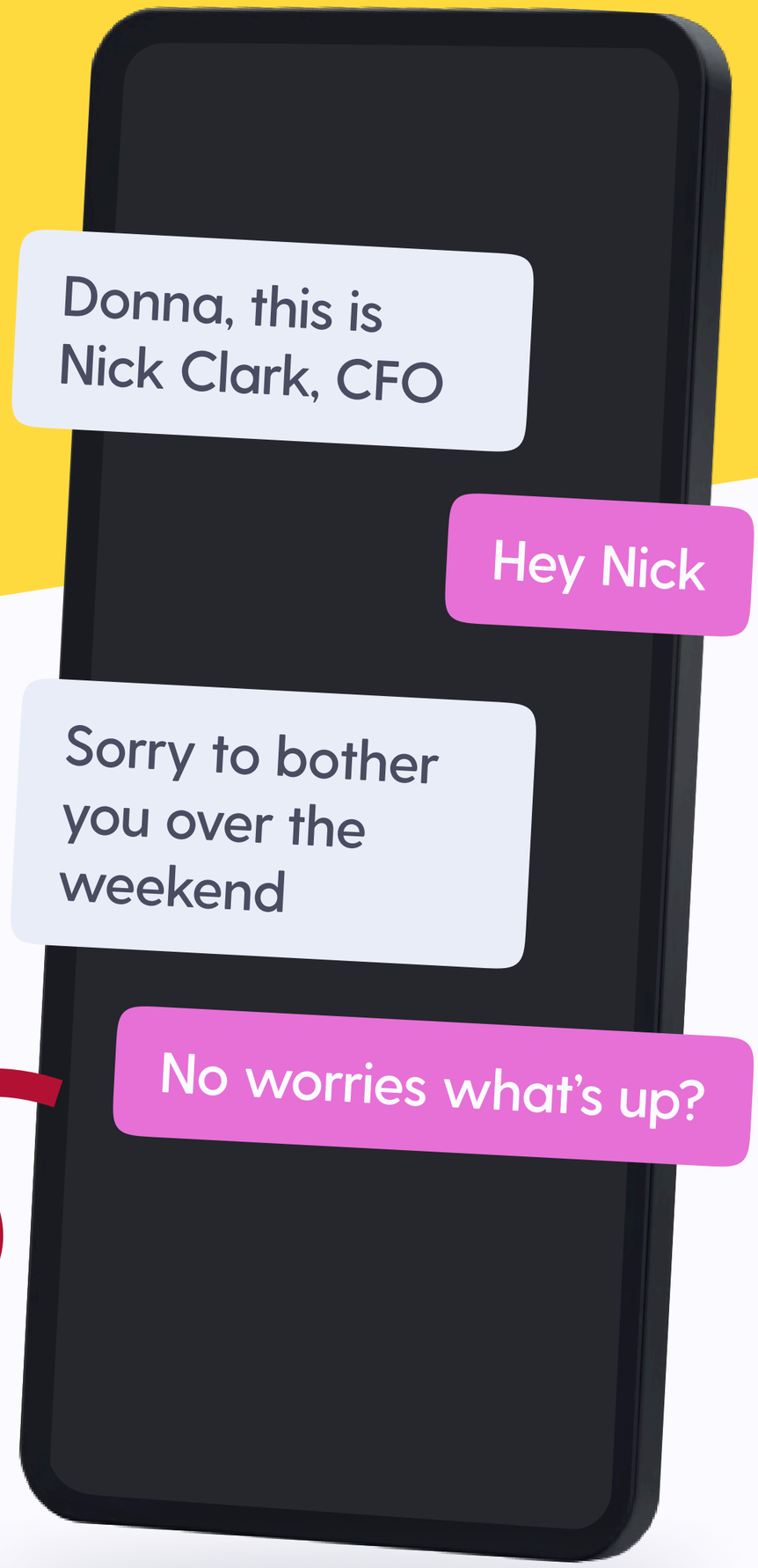


Anatomy of a CXO Smish

Don't Get Hooked: **Stop and Think Before Logging In**

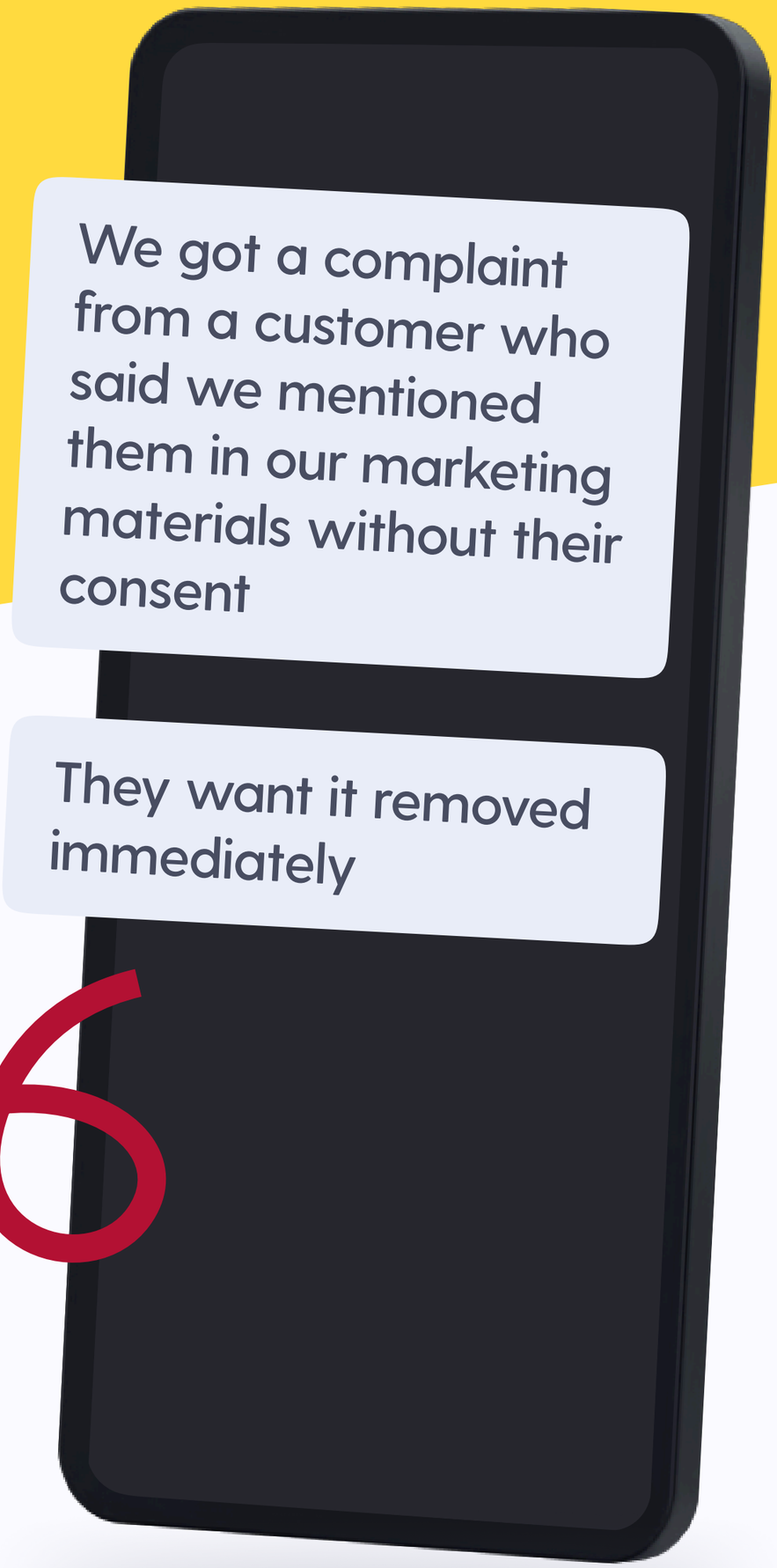
Surprise! You get a text from a company exec you don't usually hear from. Seems odd... but you go with it.



TIP

Scammers often impersonate authority figures to make it harder to say 'no'.

Then comes an urgent issue needing immediate action.



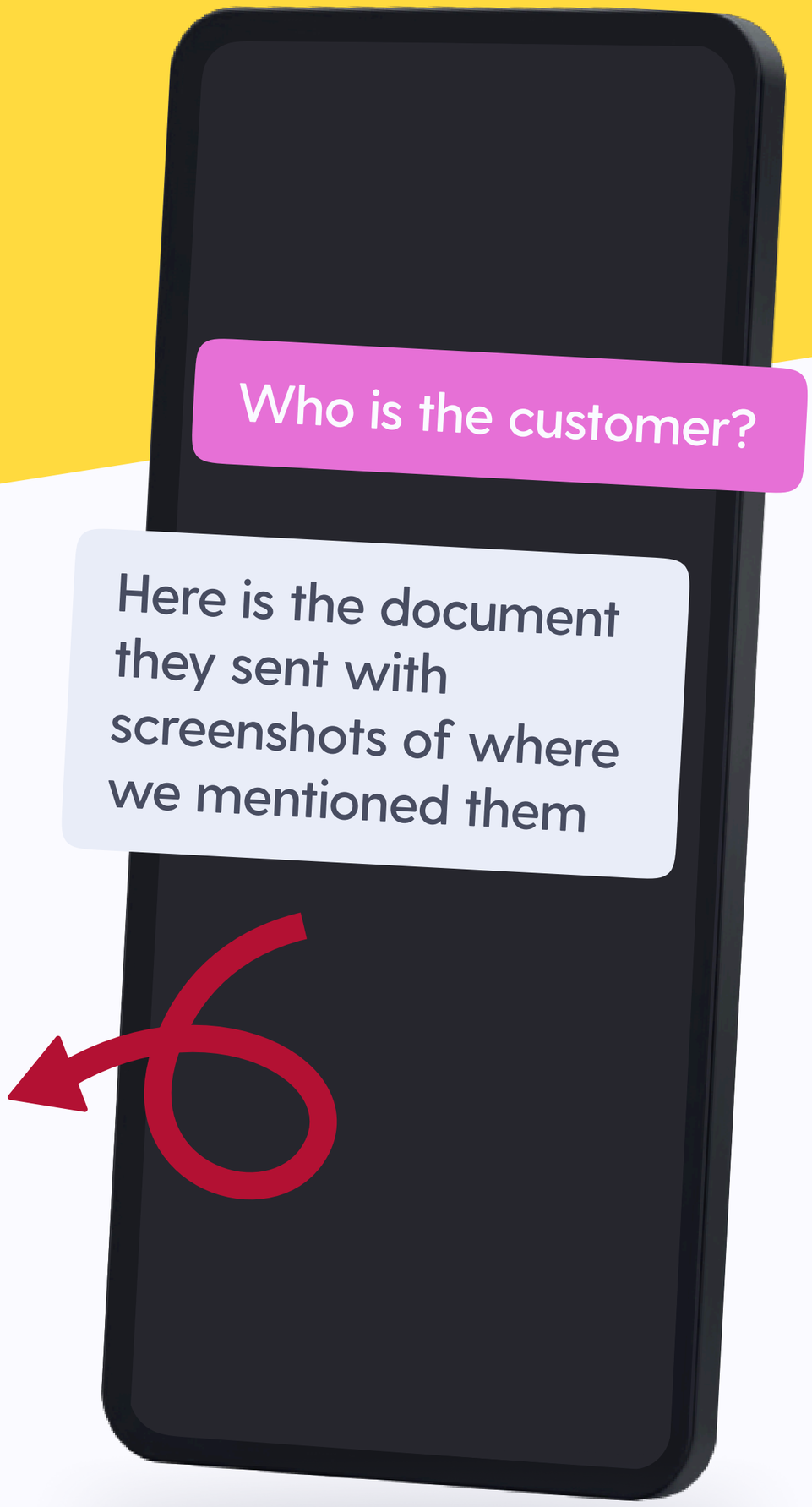
TIP

Scammers manipulate by getting us emotionally charged whether it is shocking, upsetting, or exciting.

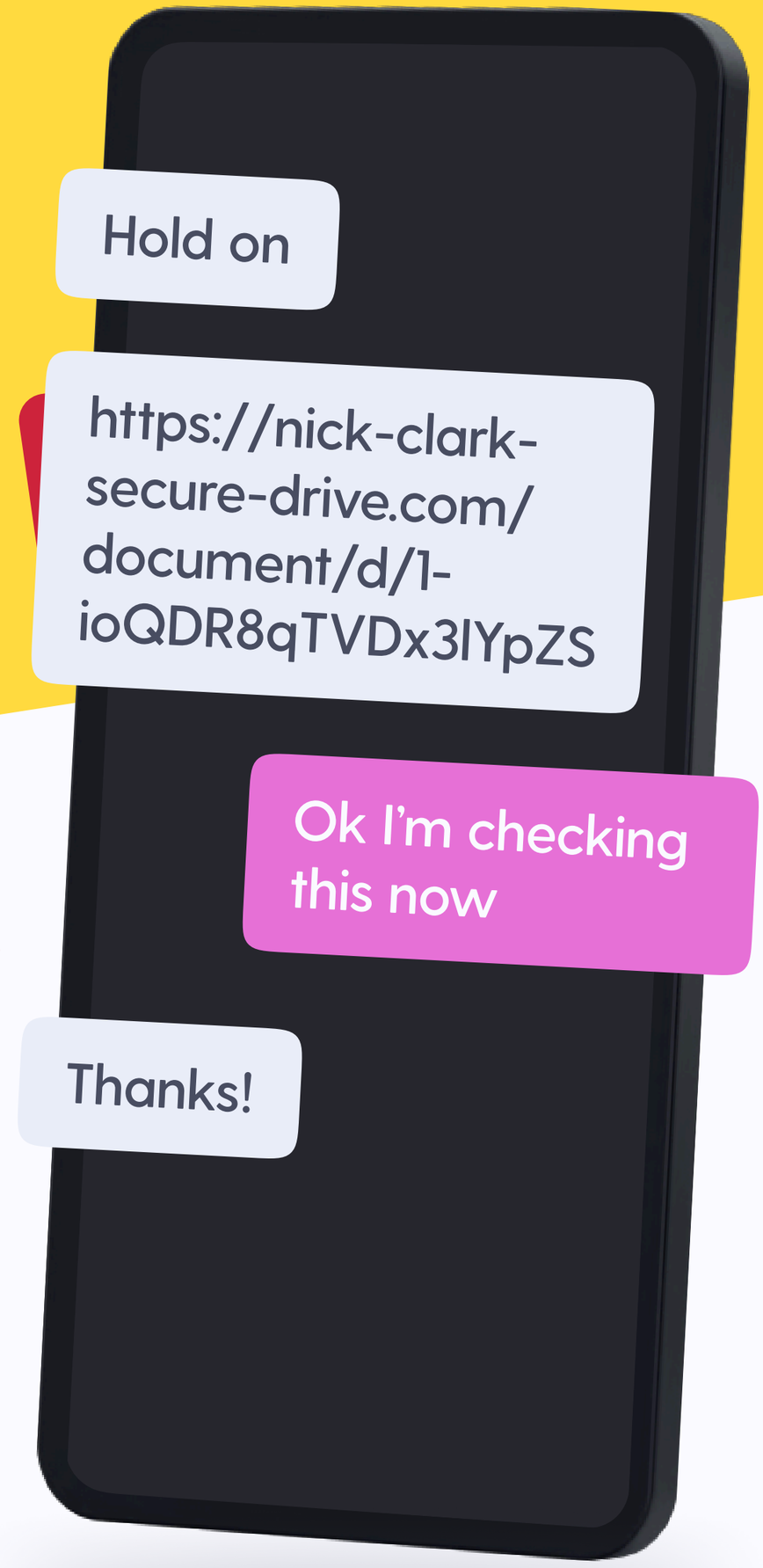
When asked a specific question, scammers ignore it in order to push their narrative.

TIP

Don't let it slide if a specific question isn't answered. That's a red flag you need to verify this conversation another way.



A phishy link is sent, without answering the previous question, pushing recipient to take action.

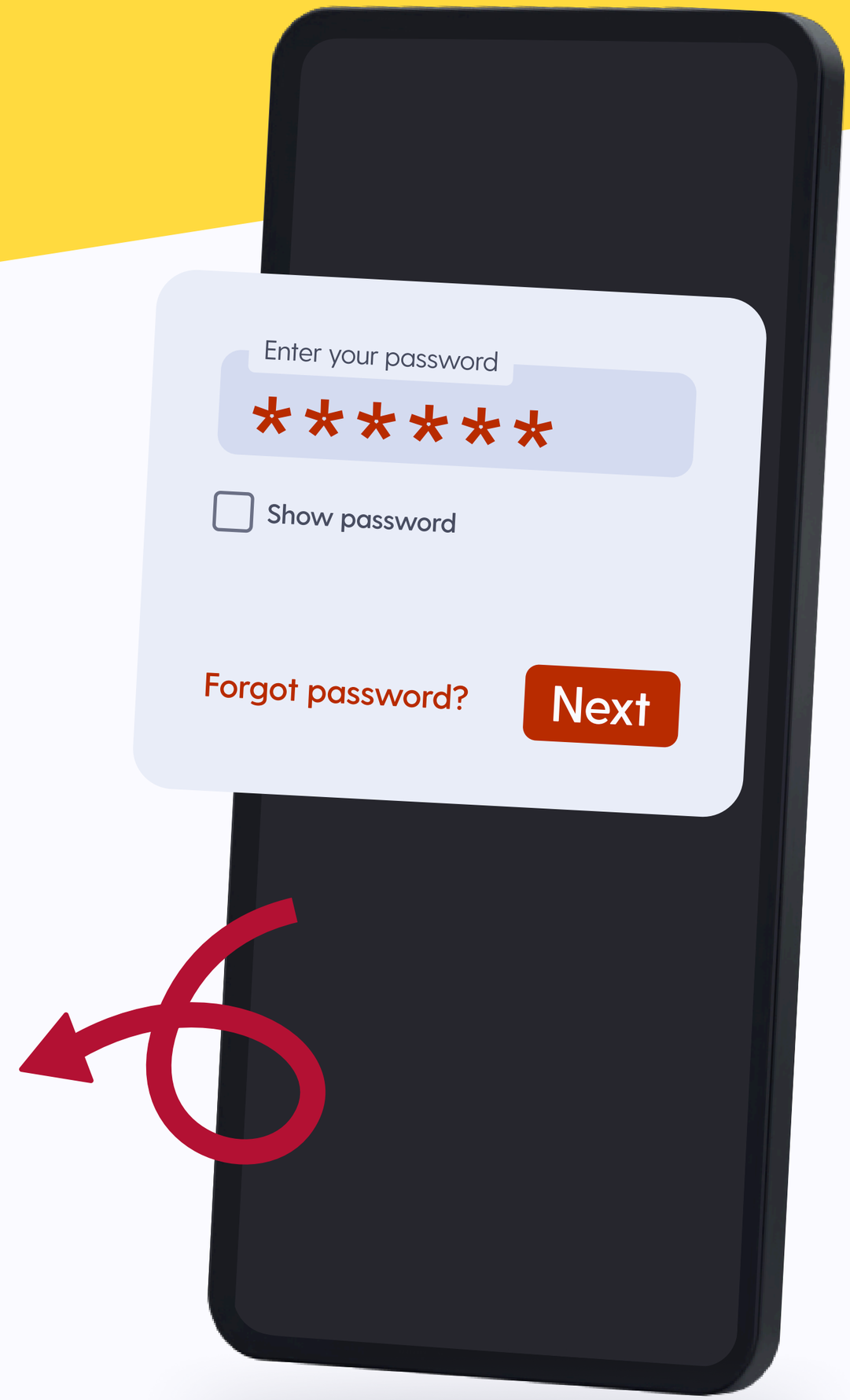


Slow down and verify any unexpected and urgent requests.

If a link directs you to log in: **STOP.**

TIP

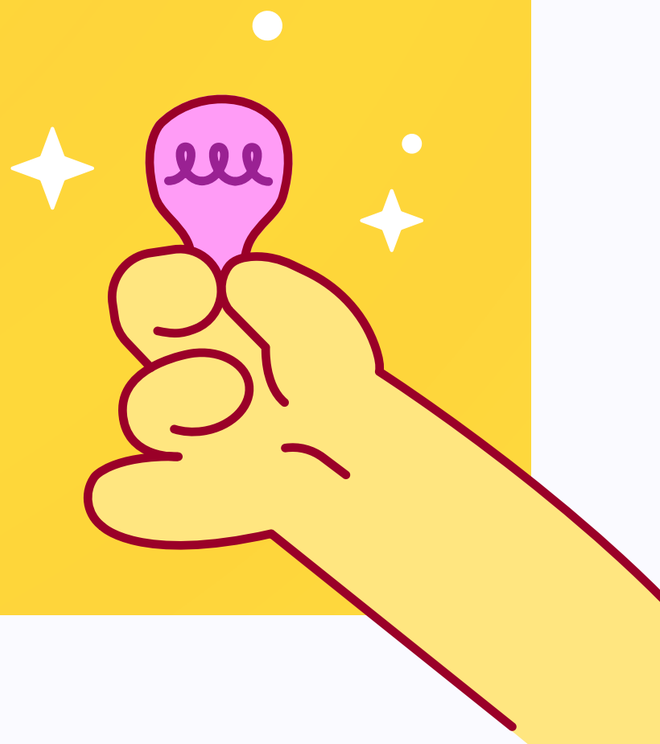
These typically are fake log in pages designed to steal your account info. Avoid signing in to a service with a link. Instead navigate directly through your app.



Stay Safe:

- **Be suspicious of urgent messages** asking you to log in, regardless who it says it's from.
- **Don't click links** in unexpected emails or texts. Go directly to the site instead.
- If something feels off, **don't be afraid** to contact your direct manager **to verify.**

Better safe than hacked!



Security Awareness Simply Explained

wizer-training.com