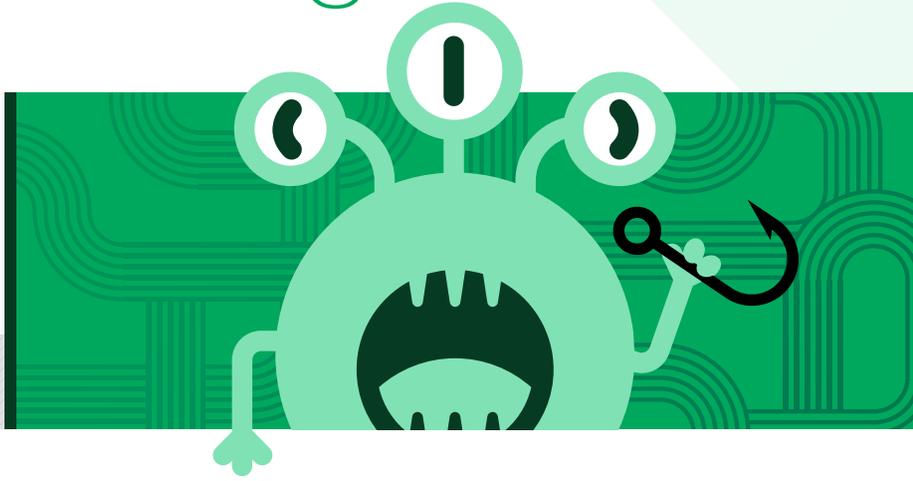# expel®

SOC SNAPSHOT #2: Q1/2022
What we're seeing:

Phishing trends

Phishing lowdown visual

10% of all Q1 incidents of phishing emails submitted to our team for review were malicious.

Only **12%** of the employees who had their credentials stolen via a phishing attack had forwarded the email to our analysts for further review.

The subject line most used for malicious emails is a blank entry. This is often used when attackers are trying to develop a relationship with the target to carry out an attack at a later date.

What other subject lines did we see?
Check out the full Q1 2022 Threat Report

Download report
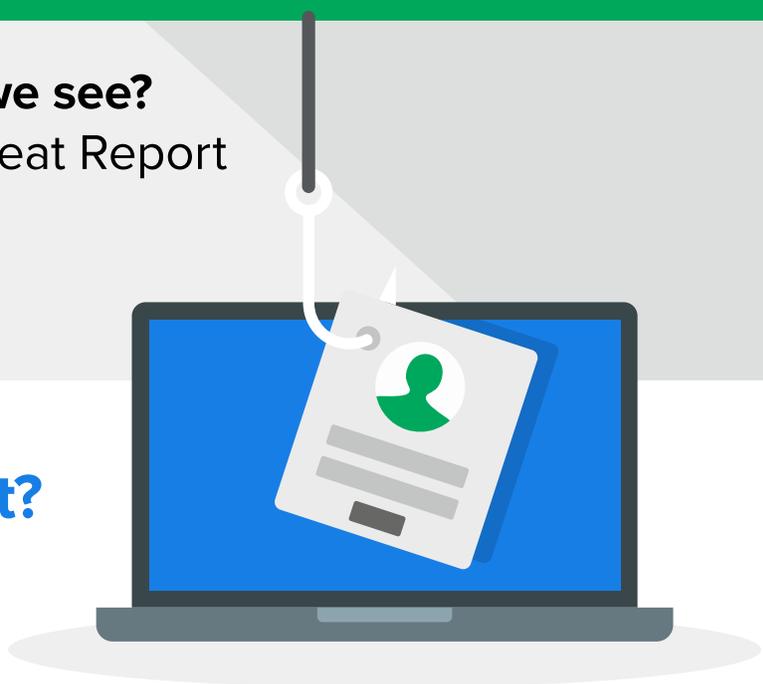
What can you do about it?

Make sure you're running MFA wherever possible using phish-resistant FIDO security keys to significantly reduce risk associated with credential theft.

Invest in training so employees learn to recognize potential red flags associated with phishing emails when they land in their inbox.

Educate specific business units on the phishing campaigns that might target them.

Get phishing remediation help

View the phishing demo

www.expel.com