FIELD GUIDE

TO SPOTTING PHISHING EMAILS

HABITAT • YOUR INBOX
RANGE • GLOBAL

DESCRIPTION

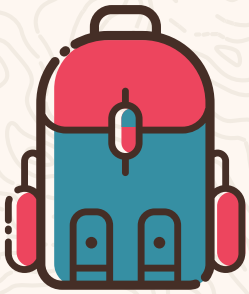
Phishing is a social engineering attack that lands in your inbox with the intention of stealing personal info. Often times, phishing emails appear to come from a known contact *(friends, family, co-workers)* or an organization such as a bank or credit card company. Attacks often feature malicious links or attachments that compromise the victim's device with malware.

POPULATION

The total number of reported phishing attacks in 2016 was 1,220,523. That is a 65% increase from 2015 and the highest number ever recorded.

APPEARANCE

You can identify phishing emails by a variety of distinct markings: bad spelling and poor grammar, odd phrasing or awkward sentence structuring, impersonal greetings such as *"Dear Customer"* instead of using your name, and web addresses that resemble a legitimate business but are slightly misspelled.



BEHAVIOR

Phishing emails typically come with a sense of urgency. They often claim that your account has been compromised or that a payment is overdue, accompanied with a call for action such as clicking on a link or downloading an attachment. Always remain skeptical of any emails that contain threatening language, and think before you click!

CONFUSION SPECIES

Spear phishing emails can masquerade as legitimate emails, tricking us into sending valuable information or clicking on malicious links. We may even suspect real emails sent by those we know, without any malicious motives, due to the sophistication of some phishing attacks.

SOURCES:
searchsecurity.techtarget.com/definition/phishing
blog.knowbe4.com/2016-exceeds-all-records-in-numbers-of-phishing-attacks