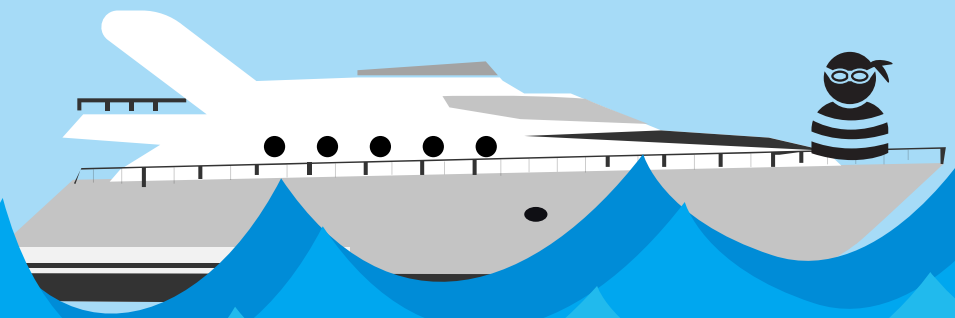
PHISHING FOR TROUBLE

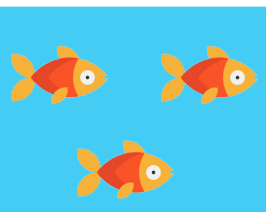
ATTEMPTS BY HACKERS TO TRICK YOU INTO GIVING OUT YOUR BANK ACCOUNT NUMBERS, PASSWORDS, CREDIT CARD NUMBERS. ETC.

2017
Reports of W-2 phishing emails increased 870%

2016
76% of organizations reported being victims of phishing attacks

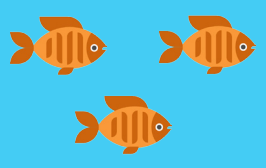


Types of Phishing



SPEARPHISHING
Directed at specific individuals, roles, or organizations

WHALING
Directed at executive officers or high-profile targets within a business or government



CATPHISHING
Hackers create fake dating profiles to seduce victims into fictitious online relationships

ANGLERPHISHING
Attackers leverage social media sites to create a fake brand presence

Signs of Phishing

POOR SPELLING

STRANGE SENDER ADDRESS

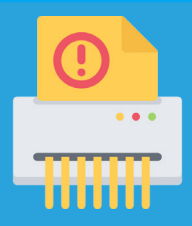
"TOO GOOD TO BE TRUE" OFFERS

LINKS TO FAKE WEBSITES

Ways to Avoid Phishing

Never access your bank or other sensitive websites by clicking links in emails. Always type the URL into your

Only enter sensitive data into secure websites that begin with *'https://'* and show a closed lock icon



Carefully discard/shred documents with personal identifiable information on it

Reputable organizations will never use email to request that you reply with your password, full Social Security number, or confidential personal information.

900 S Capital of Texas Hwy, Ste 350,
Austin, TX 78746

iLOCK360
Powered By experian.

Contact us at 512-600-5205
info@iLOCK360.com