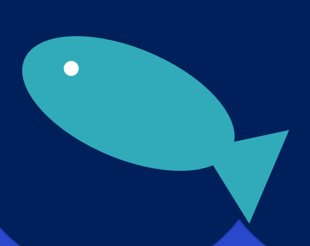
Banner Health®

PHISHING: HOW TO AVOID GETTING HOOKED

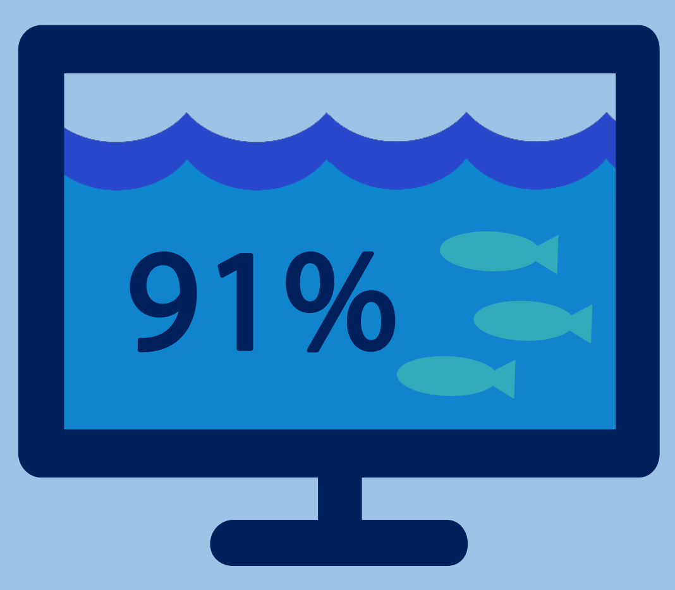


WHAT IS PHISHING?

Phishing occurs when emails or malicious websites solicit you to enter personal information by posing as a trustworthy source

The goal of a phishing attempt is to trick you into providing sensitive information, such as log in credentials, so that the cyber criminal can access your data and potentially the corporate system

91% OF CYBERATTACKS START WITH A PHISH*



AND END WITH MALWARE, RANSOMWARE, OR OTHER INTRUSIONS INTO YOUR SYSTEM

WHAT DO CYBER CRIMINALS WANT?

- PASSWORDS
- FINANCIAL INFORMATION
- IDENTITY
- PROTECTED HEALTH INFORMATION
- MONEY

WHY DO WE FALL FOR PHISHING ATTACKS?

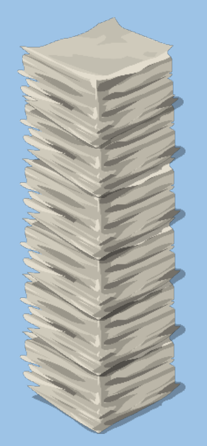
- LACK OF AWARENESS
- CURIOSITY
- FEAR
- URGENCY
- DESIRE TO PLEASE

WHAT IS THE IMPACT?

ACCORDING TO THE OFFICE FOR CIVIL RIGHTS, IN 2015** THERE WERE:

253 HEALTHCARE BREACHES

1 MILLION + INDIVIDUALS IMPACTED IN 6 LARGEST BREACHES



LOSS OF OVER 112 MILLION RECORDS

WHAT CAN I DO?

IF YOU SUSPECT AN EMAIL IS A PHISHING ATTEMPT, REPORT IT BY EMAILING:

reportphishing@apwg.org ☜

*2016 Enterprise Phishing Susceptibility and Resiliency Report, PhishMe

**Department of Health and Human Services' Office for Civil Rights HIPAA Statistics: 2015

For more information, please visit https://education.apwg.org