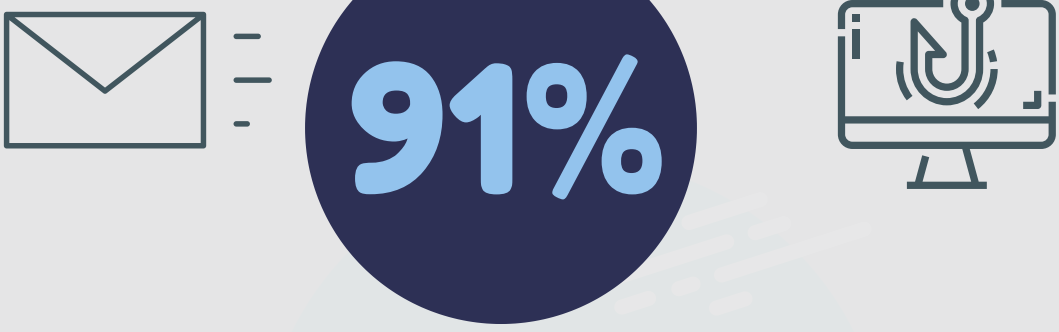
DON'T FALL FOR THE BAIT!

SOCIAL ENGINEERING & PHISHING

REVEALRISK
SECURE YOUR BUSINESS

According to a new report from PhishMe



of cyber attacks start with a phish

Phishing During COVID-19: Beware of. . .

- Access to testing and supplies
- Request for Money (Fundraising)
- Insurance Coverage
- Opportunity to invest in the company with the cure
- Fake Cures

QUESTIONS TO ASK YOURSELF IF APPROACHED WITH POTENITAL BAIT

- Why am I receiving this?
- Was I expecting this?
- Is this how they would communicate with me?

IF THE EMAIL LOOKS SUSPICIOUS

1. Open or preview the email carefully. Check full email address from the sender to see if it has been spoofed (not really the sender listed) Check their website.
2. Don't click the links or open attachments. Instead, login to your account or view typing the company URL into your browser.
3. Don't call phone numbers listed. Use the number from your address book or found on the company website.
4. Don't reply with any sensitive or login information. If you need to reset a password or login - use a trusted URL to change and never email password.
5. Contact Reveal Risk if your business needs assistance in workforce awareness programs and other cyber security improvement initiatives.