CYBERSECURITY 101 FOR YOUR EMPLOYEES

RECOGNIZE AND REPORT PHISHING

October is Cybersecurity Awareness month and the theme is "See Yourself In Cyber." The month is dedicated to personal cybersecurity that we can all benefit from, especially employees who are often the first targets.

Employers should communicate effective cybersecurity hygiene beyond traditional security awareness training programs and each topic this month speaks well to that.

Week 3 is all about phishing.

THE TROUBLE WITH PHISHING

Phishing attacks have reached an all-time high in 2022 and employees are often the first to be targeted with the attacks. The best defense is to know how to spot one and to make sure they know how to report it.
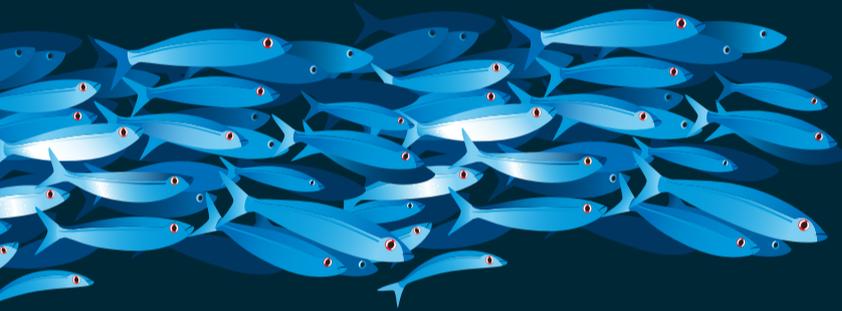
In the first quarter of 2022,

1,025,968

phishing attacks were detected!

HOW EMPLOYEES CAN SPOT A PHISHING EMAIL

Here's what to look for in a phishing email:

Sender address:
Most phishing attacks are impersonations and the sender address often isn't the company the email is pretending to be from.

Strange grammar:
Phishing emails might not be written in the original language and malicious hackers aren't proofreading with the same scrutiny as a real company's team.

Old logos and branding:
Some phishing emails haven't been updated in quite a while and may be using older branding.

A sense of urgency:
Many phishing emails try to get you to click on a link or download an attachment with unnecessary urgency. If you feel pressure, it may be a bad sign.

HOW TO COMMUNICATE TO EMPLOYEES

Not only is it important to tell employees how to spot phishing emails, you should also ensure that they're empowered to report any phishing emails. Remind them that they should never respond and that they can always reach out to whoever an email may be impersonating if it's an internal person.

If you do leverage any phishing simulations, make sure there's no shaming of any employee who may fall for a fake phishing attack. Practicing positive encouragement is likely to lead to better results.

To learn other ways to secure your organization, visit **solcyber.com**

SolCyber

solcyber.com