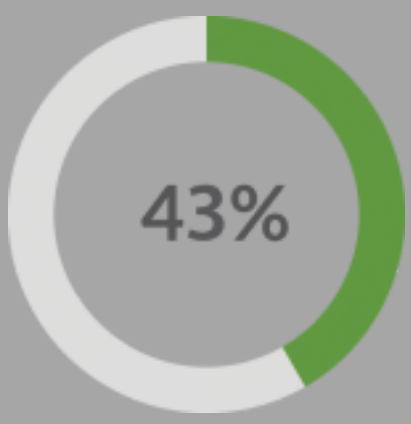
# GTS' PHISHING EMAIL TEST RESULTS

**Global Technology Solutions performed a simulated email phishing attack in December to assess how strong APS' defenses are when it comes to cyber security.**

## THE RESULTS WERE SHOCKING

In just two days, ***43% of APS employees*** clicked on and opened a message that was designed to look like a fake scam email from HR.

GTS completed the test this way because this is the exact approach hackers would take to breach out systems – and ***nearly half*** our population took the bait.




## WHAT HAPPENS IF APS GETS HACKED?

If we are hacked, this means that scammers can go into APS' systems and access your personal info, including:

- *Your social security number.*
- *Your banking and direct deposit info.*
- *Your address and phone number.*

## IT COULDN'T HAPPEN TO US...

That's what Bank of America, Netflix, Target, and Facebook said.

As a global leader, APS is a prime target for online criminals who want to cause data breaches.

Our approach to digital security has to change.

## HOW CAN YOU AVOID THE BAIT?

Remember the phrase hook, line, and sinker.

Hook, Line, & Sinker

### HOOK

Is the content of the email designed to hook you emotionally and reel you in somehow? Threats, coercion, and scare tactics are common in digital scams.

### LINE

Check the subject line of the email for the [EXTERNAL] tag and look for the yellow banner to remind you the email has originated from outside APS.

### SINKER

Verify the sender's email address by double-clicking the display name in Outlook to see if the real email address matches.

## BEST PRACTICES

- Watch the GTS Stream video on phishing.
- Turn on Message Preview in Outlook to get a sneak peek at suspicious emails before you click.

## DON'T CLICK, INSTEAD:

- **Right-click and delete.**
- **Call GTS immediately (ext. 2486).**

Right-Click & Delete