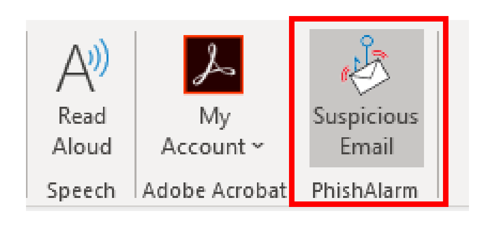
You fell for a phish

But don't worry, this was just a test!

Next time, use the PhishAlarm button in Outlook to report a suspicious email.
Information Security and your colleagues are staying vigilant to keep the Enterprise safe;
Join them by using PhishAlarm to stop phishing attacks before they happen.
You might be recognized Enterprise-wide for your efforts!



If your PhishAlarm button doesn't work, please change your settings:

Open Internet Explorer, click on the gear at the top right, click on Internet Options, click on the Security tab, click Internet in the top box and make sure that Enable Protected Mode is checked.

This type of phish is known as a *Link Attack*. The hacker tricked you into clicking on a link.

Here are some things to watch out for:

DO look out for unexpected gifts, free items, or coupons. If it

DON'T click on links that don't match URL destination. Hover

DON'T act quickly! These emails use threatening language to

DO verify the address of the sender. All external emails have a seems too good to be true, it probably is!

over the link- does it match up with a legitimate site?

trigger an emotional response. If you feel uneasy about an email, **report it immediately**.

CAUTION banner and internal emails come from an address with extension **<Company Domain>**

Please do not share your experience with colleagues, so they can learn too.

Got it! Thanks!

Click to acknowledge and close