The Three Ws of

Investigating Phishing Emails

WHO?

- Do I know the sender?
- Is this someone I usually communicate with?
- Is the email sent to an unusual group of people?
- Is the email spelled correctly? Look for even the smallest typo.
- Does the email address match the email in the signature?

WHAT?

- What action does the sender want you to take?
- Does the email contain bad grammar, odd styling, or typos?
- Is the email written in a style consistent with the sender?
- Is the action something you'd expect from the sender?
- Is it an urgent request? This is a big red flag!

WHY?

- Why do they want you to click on a link, download an attachment, or send information?
- Are they presenting a sense of urgency?
- What is the consequence they are threatening if you do not act? Is it something you would expect?
- Have they presented an unusual situation? Is it something you would expect?

If ANY of these questions point to a suspected phishing email what do you do?

- Report the email as phishing or mark it as "Junk."
- Call the sender directly to verify, do not email.
- Do not take action until you verify it is not phishing!

SBS CyberSecurity

WWW.SBSCYBER.COM