EMAIL: GOOD VS BAD

5 Ways to Protect your Network

Tips to help you decipher if the email you are about to read is valid or set to unleash a malicious attack on your company's network with just a single click.

1.

Subject to attack.

Take a good look at the subject line. Does it seem unusual or out of character when you consider the sender? Were you expecting this type of email from this particular sender? If no, it is best to err on the side of caution and leave it alone – or better yet, delete it altogether.

New Email, who's this?

Look at the "from" line of the sender versus the domain of the link within the email. Do they match? No? This could be a potential malicious email.

2.

3.

Check for Mistakes?

Look for grammatical errors, misspellings and/or odd spacing. Most emails from reputable sources will not contain these types of errors.

Greetings Earthling.

Many phishing scams will start with very generic greetings such as "Dear Customer" or "Dear Sir/ Madam." Don't fall for it.

4.

5.

You want me to go where?

Before clicking on that hyperlink in the email, hover over it to see the destination URL. Does it match the rest of the email? Does it look like a legitimate URL? Can't safely decipher where that link will take you? If so, delete... delete... delete.

appriver.com/good-vs-bad

appriver®