

PLEASE REFRESH YOUR MEMORY ON THE BELOW CYBER SECURITY TIPS

- Do not click on links or attachments from senders that you do not recognize. Be especially wary of .zip or other compressed or executable file types.
- Do not provide sensitive personal information (like usernames and passwords) over email.
- Watch for email senders that use suspicious or misleading domain names.
- Inspect URLs carefully to make sure they're legitimate and not imposter sites.
- Do not try to open any shared document that you're not expecting to receive, simply DELETE.
- If you can't tell if an email is legitimate or not, please forward to IT.
- Be especially cautious when opening attachments or clicking links if you receive an email containing a warning banner indicating that it originated from an external source

Remember: 91% of successful data breaches started with a spear phishing attack. No matter how many controls we have in place to help protect our networks, we rely on every employee to be our first line of defense (Human Firewall). ** All it takes is 1 and according to our report we have more than 1 ☹. **.

Thanks for helping to keep our network, and our people, safe from these cyber threats.

Below are the results of phishing mistakes committed by department. Let's try to get the Police Department to ZERO. Thanks!

