5 WAYS EMPLOYEES CAN HELP PREVENT CYBER ATTACKS

SET POLICIES FOR SENSITIVE BUSINESS INFORMATION

Develop and communicate policies for protecting sensitive business information, such as passwords or certain company files. An example could be providing cybersecurity training to an employee before they can be granted access to a company computer.

REMIND THEM TO PRACTICE GOOD SECURITY

Remind your employees and communicate about good security practices, such as sending emails from unknown sources to them to observe if they react properly. If not, provide training for them and see the areas they can improve on.

SELECT STRONG PASSWORDS

By having a strong password, employees will be at a lesser risk of experiencing password attacks from cybercriminals. Ensure their passwords do not have personal information, such as nicknames or street they live in. Recommend them to include at least one number and special symbol in their passwords.

SPOTTING SUSPICIOUS EMAILS

Ensure your employees have the knowledge and skills to identify suspicious emails, such as phishing scams. Make sure their wary of any emails that contain grammatical or spelling errors, or asking them to click on a link or download an attachment.

INSTALLING OR UPDATING ANTI-VIRUS SOFTWARES

Having the latest anti-virus software can equip your device with the latest protection on new viruses. Some employees may forget to update their devices, so to ensure their device has the latest anti-virus software, aim to set up automatic updates.

PRESENTED BY osDORO