Familiarize yourself with phishing attacks

Retail Team

Sushanta Poudel

What is phishing?

Phishing, one of those sneaky tricks. Just imagine someone coming to you, putting on an act as if he or she were your friend, and trying to get you to share secrets. Online, the bad guys pretend to be someone you would trust, such as your bank, or work, or hospital, in order to trick you into sharing important information, such as a password, personal information, or even money. It is very important for one to be cautious and not to share one's personal informations with strangers online!

Learn to spot phishing emails

- **Check the sender's Email address:** Sender's email address often looks similer to but aren't exactly the same as the real one. If our legitimate email is itsupport@yourcompany.com it migh come us as itsupports@yourcompany.com.

- **Beware of "Uregnt" or threatening language:** Sometimes the scammerts may implement urgent or intimidating language to make you take immediate action. Examples can be ""Your work account would be will be restricted if you don't follow the link."

- **Looks for generic greeting, and grammar mistakes:** Phishing emails often greet without using your name i.e. dear employee, or dear co-worker, and contain noticeable grammar errors.

Learn to spot phishing emails

- **Hover over the links:** Hovering your mouse over the link before clicking on any it will display the actual URL. If the URL looks suspicious or doesn't match the sender, don't click it.
- **Be cautious with attachments:** Attachments and documents can contain malware. Opening an attachment from someone you don't know and don't trust can infect the system and can cause data loss, effect reputation and cause financial loss.
- **Always, verify the information:** If the email asks for your personal information or money, contact the sender directly using trusted method to verify the request.

How do we stop getting phished?

Enable multi-factor authentication: This adds additional security to make it much harder for anyone to get into your accounts simply by knowing only your password.

Watch out for emails: Never click on links or download attachments from an unknown or suspicious email, even if it may look valid. Make sure the sender's email is correct.

Learn and inform: Take a little time to learn what the general phishing signs are, then share this with family and friends.

Report phishing attempts. If you get a phishing email, or if you are unsure about the email, report it to your company's IT team.