PHISHING SAFETY TIPS

It is important to safeguard yourself and others against all phishing attacks and not cause damage to others inadvertently. Here are some best practices that will help you achieve this:

WHAT YOU SHOULD DO

- Open attachments only if it is from a known source and if you are expecting it.
  - If you are expecting it, call the concerned party and verify the mail before opening.
- If an email threatens you with dire consequences, verify it through a different channel.
- Before clicking any link, hover the mouse over the link and read the complete URL to verify the link is genuine.
- Type links directly into the browser instead of clicking them.
- Verify the sender of suspicious emails, even if the email is from a known person.
  - The domain of such emails would not be a genuine one.

WHAT YOU SHOULD AVOID

- Avoid opening unknown emails with attachments, clickable links, reward mails, panic mails and threat mails.
  - More attractive the reward = more is the possibility of an attack.
  - Ignore such mails unless you have been expecting a reward.
- Avoid visiting suspicious looking websites.
- Do not intentionally use, distribute, or create viruses, worms, or other malicious software.
- Do not interrupt or change the settings of the auto virus scan scheduled on your desktop/laptop.

- Beware of unknown emails that indicate urgency or immediate actions.
  - Verify such emails with IT/security teams.
- Look for issues such as:
  - Bad email formatting
  - Blurry logos/banner
  - Bad spelling/grammar
  - Generic greetings/messages

- Refrain from sharing personal or ABI-related sensitive information on emails or web forms.
- Avoid opening emails marked as spam.
  - ABI has tools to filter and mark communication as spam.

Always remember to promptly report the following:

- Suspicious emails
- Virus/malware incident

Always report any such phishing activity to

soc-support@ab-inbev.com.