Familiarize yourself with phishing attacks

Marketing and Human Resources

What is phishing?

Phishing is a social engineering attack with the end goal of stealing your information. This information can range from account information to financial information.

You are sitting here because we “stole” your information 😈!

Learn to spot phishing emails

From: Mastercard Staff Rewards
To: employee@email.com
Subject: Black Friday Employee reward card

Hello <name>,

In recognition of your hard work throughout the year, we wish to reward you with a gift card to spend in the upcoming Black Friday sales as a small token of our appreciation. Please find attached your Employee reward card.

The balance of your card will be determined based on your role. To view the balance and activate your employee reward card, visit here.

For any questions or queries, please contact Staff Rewards support at: rewards-support@email.com.

From,
Staff Reward Services

On the left is the email that you all fell for. It is a well written email, but an important rule is to never click links on emails. Some other factors to look out for include:

- Messy organization/structure
- No points of legitimacy
- Suspicious looking source email address (we use our own address)
- Unfortunately, emails that offer an easy access for compensation are usually fake. If you are getting an award, it would have been wired to you already or you would have to physically pick it up
- Most importantly, anything that is asking for you to input your personal details

How do we stop getting phished?

- Never click links in emails! Usually does not have a good outcome.
- Enable the spam filter and report spam! Block phishing email addresses too.
- Don’t reply/open emails with suspicious headers.