PHISHING ATTACKS

Did you know that there were over 500 million phishing attacks reported in 2022? And that is just the number reported. So there were even more phishing attacks in 2022.

While we cannot stop phishing attacks, we can provide you with tips to help you not fall victim to one.

1. **Is the email from public email domain? (e.g., @gmail.com, @yahoo.com)**

   It is unlikely that a legitimate company will use a public email domain.

2. **Does the email have inconsistencies?**

   The sender's name does not match the email address (e.g., the sender's name is Kevin Smith but the email address says Karl Smith).

   The sender purports to be from your bank, but the email address is @gmail.com

3. **Is the domain name misspelled?**

   If the email claims to be from your bank, but the email is being sent from another email domain like gmail.com it's probably a scam. Also be watchful for very subtle misspellings of the legitimate domain name. For example @wellsforgo.com instead of @wellsfargo.com

4. **Does the email contain a suspicious link or attachment?**

   Before clicking on a link, make sure that the domain associated with the link matches the sender. If the email is from your bank, when you hover over the link, the domain should be from your bank.

   Does the attachment have an unfamiliar extension or one that often associated with malware (.zip, .exe, .scr, etc.).

5. **Is the email asking you for personal information, payment information, or login credentials?**

6. **Is the email asking you to act urgently?**

Why are phishing attacks so popular?

BECAUSE THEY WORK.