# WHAT'S THE DIFFERENCE BETWEEN SPAM AND PHISHING EMAILS?

Spam is unsolicited email that typically attempts to sell you something. The spammer has no intention of spreading malware or stealing sensitive information.

## TYPES OF SPAM:

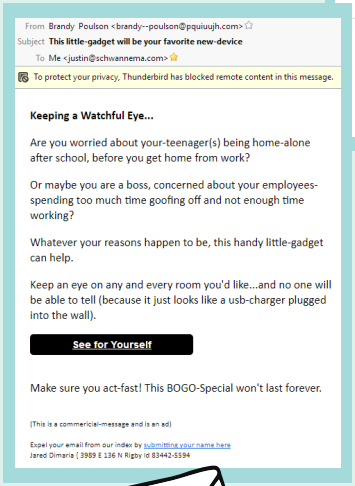
**Intentional** – spammers who gain access to bulk email lists and solicit products.

**Unintentional** – spam that originates from infected computers.

**Spim** – spam over instant messages.

**Spit** – spam over telephony.

## EXAMPLES OF SPAM:


## HOW TO AVOID SPAM:

1. Keep your email address private. Don't store it in plain text on a blog or website, and only give it to trusted sources.

2. Don't click on any links or pictures in spam emails.

3. Use filters. Most email clients allow you to adjust filters based on content to block spam.

4. Register with dmachoice.org to get off commercial email lists. https://www.ims-dm.com/cgi/optoutemps.php

Phishing is a social engineering tactic designed to steal information or money, often via malicious links or attachments.

## TYPES OF PHISHING:

**Generic** – the typical email that features poor grammar and claims you've won the lottery.

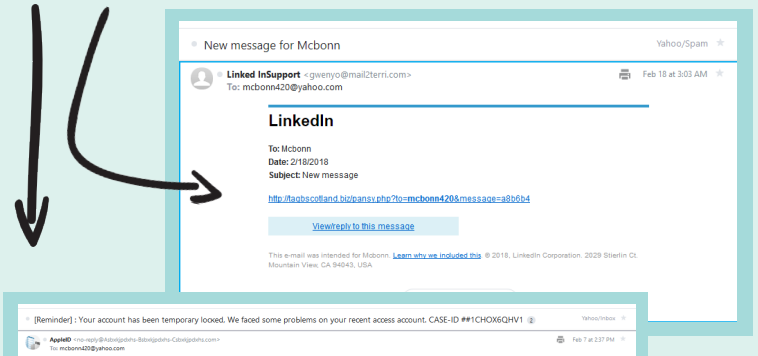
**Spear** – more sophisticated phishing attacks that target specific organizations or individuals. Spear phishers use a technique known as spoofing, which forges the email "from" address, so it appears to come from someone you know.

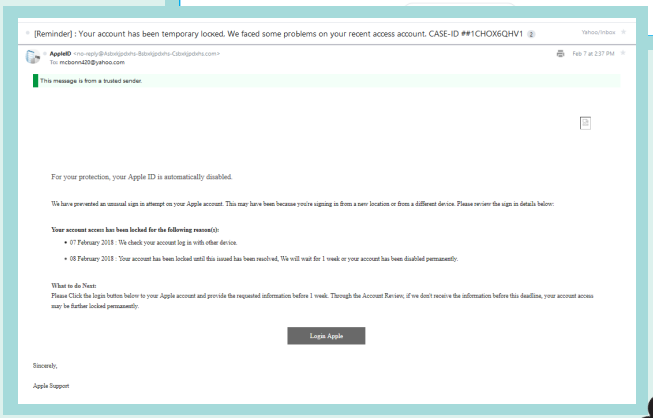
**Whale** - phishing that targets high profile individuals like CEOs and celebrities.

**Smishing** - phishing via SMS.

**Vishing** - phishing via phone calls.

## EXAMPLES OF PHISHING:




## HOW TO AVOID GETTING PHISHED:

1. Be skeptical of all unsolicited emails.

2. Never click on links or download attachments from strangers.

3. Verify the sender's email address before clicking or responding.

4. Remember that offers too good to be true are usually scams.