Phishing happens to organizations when cyber criminals think there is personal information they can get from users that they can use to get money or use it for bad intentions, and they tend to use different tools and subtle ways that users will not easily suspect.

Bellow are different scenarios/ examples used by scammers and recommendations people can use to avoid getting scammed

Phishing email example (for awareness purposes)

Alerts@fnb-secure.co.za

Account verification required immediately

We detected suspicious activity on your account. Please verify your identity to avoid account restriction.

Verify now:
http://fnb-verify-login[.]co/account

Phishing email sample 1 (bank-themed)

Source: Public phishing email sample (used for security awareness and training purposes)

Subject: Account verification required immediately

From: alerts@fnb-secure.co.za
This domain does not match the one of the FNB bank, and it needs to be verified using headers

The link: http://fnb-verify-login.co/account
The link is not HTTPS, the domain is not official, it uses "verify-login" which is the wrong wording and the link will likely redirect you to the outside official banking platform where your information will be stolen

Email summary:

The email claims that suspicious activity was detected on the recipients bank account and urges the user to verify their identity immediately using a provided link. The message uses urgent language and fear based tactics to pressure the recipient into acting quickly.

Identified Phishing Indicators

- Urgent subject line designed to pressure the recipient
- Sender email domain does not match the legitimate bank domain
- Vague description of suspicious activity without specific details
- Unprovoked requests for identity verification

Suspecious external link directing users to outside official banking platforms

Risk classification

Risk level: Phishing

Reason:
The email contains multiple phishing indicators including spoofing (attackers are imitating a trusted source which is the FNB bank), urgency where users are rushed into taking a command, fear based messaging, and a malicious verification link designed to harvest user credentials

Simple explanation of the attacks

- This email attemps to impersonate a legitimate bank to track users into clicking a fake link. If the user clicks the link, they may be redirected to a fraudulent website that steals login credentials or personal information

User awareness tip

- Legitimate banks do not request users to verify their identity through email links. Users should access banking services only through official mobile applications or official websites

How phishing attacks work

- Phishing attacks happen when scammers send emails that pretend to come from organizations people already trust, such as banks, Online services, or delivery companies

- These emails usually claim that something is wrong with your account and try to scare you into acting quickly. They might say your account will be blocked, suspended or compromised if you do not respond immediately
- The email often includes a link or an attachment. You might be taken to a fake website that looks real and asks you to enter details or personal information. Once you do this, the attacker steals your information and can use it to access your accounts or commit fraud
- Phishing attacks work because they rely on human emotions like fear, urgency and trust rather than advanced technical skills

Do's and don'ts to avoid phishing attacks

What to do

- Check the senders email address carefully. Make sure the domain matches the organizations exactly

- Be cautious with urgent or threatening messages. Take a moment to think before you act. Scammers want you to panic

- Hover over links before clicking. If the link looks strange or unfarmiliar, do not click it

- Use official apps or websites

access accounts by typing the website address yourself or using official apps

- Report suspicious emails

If something feels off, report it to IT or security instead of engaging with it

- Delete confirmed phishing emails immediately

This prevents accidental clicks

What you should never do

- Do not click on suspicious links

Especially if the email is unexpected or urgent

- Do not download unknown attachments

Attachments can contan malware

- Do not share passwords, personal information or your OTP with anyone.

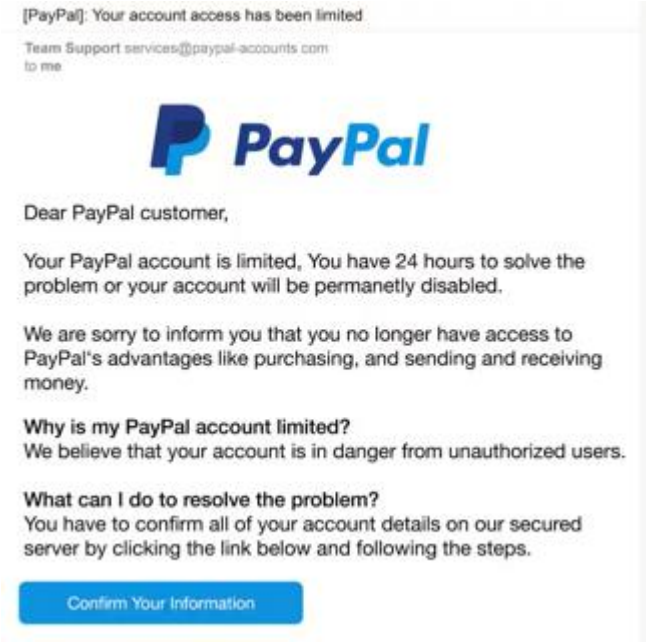
Legitimate organizations do not ask for this

- Do not respond to phishing emails

Replying confirms that your email address is active

- Do not trust emails because they look professional

Phishing emails are designed to look real


[PayPal]: Your account access has been limited

Team Support services@paypal-accounts.com
to me

PayPal

Dear PayPal customer,

Your PayPal account is limited, You have 24 hours to solve the problem or your account will be permanetly disabled.

We are sorry to inform you that you no longer have access to PayPal's advantages like purchasing, and sending and receiving money.

Why is my PayPal account limited?
We believe that your account is in danger from unauthorized users.

What can I do to resolve the problem?
You have to confirm all of your account details on our secured server by clicking the link below and following the steps.

Confirm Your Information

Subject: Your PayPal account is limited. You have 24 hours to solve the problem or your account will be permanently disabled.

From: service@paypal.com
This email claims to be from PayPal, but we must verify it using headers and link checks because attackers can spoof display names or make emails look legitimate

Link shown: confirm your information
The email includes a call-to-action link ('confirm your information'). these links often lead to to fake login pages designed to steal credentials

Message summary:
The email claims the user has lost access to PayPal services such as purchasing, sending, or receiving money due to account limitations and possible unauthorized activity. The message creates fear and urgency to push the user into clicking the provided link.

Phishing Indicators Identified

- Urgent deadline (24 hours) to pressure the user
- Threat of permanent disablement
- Fear-based wording suggests danger or unauthorized access
- Attempts to make the user act quickly without verifying the message

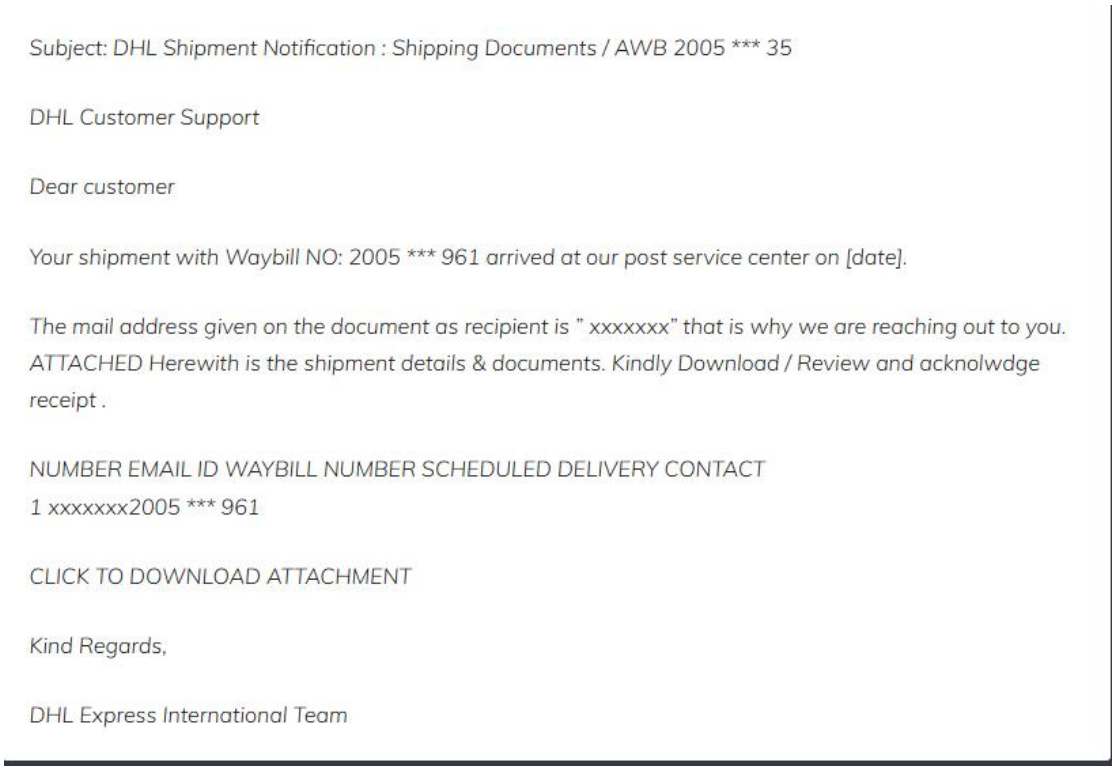
Risk classification
Risk level: Phishing/ Highly Suspicious

Reason:
The email uses urgency, fear, and a verification link to pressure the user into confirming information. These are common phishing behaviors and may lead to credential theft or fraud.

Simple Explanation (for users)

This email tries to scare PayPal users into clicking a link “confirming information”. if the page leads to a fake PayPal login page, attackers can steal your login details and access your account.

Phishing email sample 2 (delivery / parcel scam)



Subject: DHL Shipment Notification : Shipping Documents / AWB 2005 *** 35

DHL Customer Support

Dear customer

Your shipment with Waybill NO: 2005 *** 961 arrived at our post service center on [date].

The mail address given on the document as recipient is " xxxxxxx" that is why we are reaching out to you. ATTACHED Herewith is the shipment details & documents. Kindly Download / Review and acknolwdge receipt .

NUMBER EMAIL ID WAYBILL NUMBER SCHEDULED DELIVERY CONTACT
1 xxxxxxx2005 *** 961

CLICK TO DOWNLOAD ATTACHMENT

Kind Regards,

DHL Express International Team

Subject: DHL Shipping Notification: Shipping Documents / AWB 2005***961

From: DHL Customer Support
The sender name displays as DHL Customer Support (sender name appears t be legitimate, but the legitimacy must be verified using the full email address and headers). Attackers can spoof names easily.

Link shown: Click to download
may lead to:

- A malicious file download (malware)
- A fake login page (credential for theft)

Both are very common

Message summery:
The email claims that the shipment with a waybill number has arrived at a service center, but the address information is incorrect. The receipt is instructed to download and review attached shipping documents and acknowledge receipt. He message uses a generic greeting (Dear Customer) and encourages the user to click a downloading link, which may deliver malware or redirect to a phishing page.

Phishing indicators identified

- Trusted brand impersonation (DHL)
- Generic greeting (Dear Customer)

- Call-to-action link encouraging a download
- Attachment/document bait commonly used for spreading malware
- Message appears unusual and not professionally written

Risk classification
Risk level: phishing

Reason
This email uses a common phishing technique where attackers impersonate delivery services and trick users into clicking a download link. This can lead to malware infection or credential theft.

Simple Explanation (for users)

This email pretends to be from DHL and asks you to download shipping documents. Phishing emails like this often contain harmful downloads or fake pages that steal information. If you were not expecting a parcel, do not click anything and report the email.

Summery Table

Email sample	Theme/brand	Phishing indicators	Risk classification
Sample #1	Bank (FNB)	Urgent verification request,fear-based message, suspecious sender dormain, suspicious link, vague “suspicious acivity”	Phishing
Sample #2	PayPal	24-hour pressure, threat of permanent disablement, fear tactics, “confirm your information”, call-to-action link	Phishing / Highly suspicious
Sample #3	DHL Delivery	Fake shipping notification, generic greeting, “click to download” bait, attachment/document lure, unprofessional format	Phishing