Spoofed domain name

Authentication failures (SPF, DKIM, DMARC)

Foreign IP address unrelated to PayPal

Urgent subject line to induce panic

Another sample of phishing mail

Subject: Urgent: Verify Your Account Now to Avoid Suspension

From: PayPal Support security@paypa1.com

To: you@example.com

Dear Valued Customer,

We have noticed unusual activity on your account. For your security, we have temporarily limited your access.

To restore your account, please verify your information immediately by clicking the link below:

👉 https://paypal.com.secure-login-verify.com

Failure to do so within 24 hours will result in permanent account closure.

Thank you for your prompt attention.

Sincerely, PayPal Account Security Team

I Analyze suspicious links or attachments

Sender address is security@paypa1.com instead of the official paypal.com.

Link text looks like PayPal: https://paypal.com.secure-login-verify.com

Real domain is secure-login-verify.com, which is not owned by PayPal — an example of subdomain spoofing.

Look for urgent or threatening language in the email body

We have temporarily limited your access" — creates fear of account loss

Verify your information immediately" — demands instant action

Failure to do so within 24 hours will result in permanent account closure" — strong threat to force compliance

🔗 Note any mismatched URLs

Displayed link: https://paypal.com.secure-login-verify.com

Real dmain: secure-login-verify.com

❓ Why suspicious:

The real PayPal domain is paypal.com

In this link, “paypal.com” is just part of a subdomain (paypal.com.secure-login-verify.com) owned by the attacker

Everything before the last two dots in a domain can be faked — the real ownership is determined by the last two segments (secure-login-verify.com)

✅ Learning Outcome

I am able to detect some of phishing emails.

Understand the phishing email headers.

Analyze the sucipious link by hover my coursor on the linkSpoofed domain name

Authentication failures (SPF, DKIM, DMARC)

Foreign IP address unrelated to PayPal

Urgent subject line to induce panic

Another sample of phishing mail

Subject: Urgent: Verify Your Account Now to Avoid Suspension

From: PayPal Support security@paypa1.com

To: you@example.com

Dear Valued Customer,

We have noticed unusual activity on your account. For your security, we have temporarily limited your access.

To restore your account, please verify your information immediately by clicking the link below:

👉 https://paypal.com.secure-login-verify.com

Failure to do so within 24 hours will result in permanent account closure.

Thank you for your prompt attention.

Sincerely, PayPal Account Security Team

I Analyze suspicious links or attachments

Sender address is security@paypa1.com instead of the official paypal.com.

Link text looks like PayPal: https://paypal.com.secure-login-verify.com

Real domain is secure-login-verify.com, which is not owned by PayPal — an example of subdomain spoofing.

Look for urgent or threatening language in the email body

We have temporarily limited your access" — creates fear of account loss

Verify your information immediately" — demands instant action

Failure to do so within 24 hours will result in permanent account closure" — strong threat to force compliance

🔗 Note any mismatched URLs

Displayed link: https://paypal.com.secure-login-verify.com

Real domain: secure-login-verify.com

❓ Why suspicious:

The real PayPal domain is paypal.com

In this link, "paypal.com" is just part of a subdomain (paypal.com.secure-login-verify.com) owned by the attacker

Everything before the last two dots in a domain can be faked — the real ownership is determined by the last two segments (secure-login-verify.com)

✅ Learning Outcome

I am able to detect some of phishing emails.

Understand the phishing email headers.

Analyze the sucipious link by hover my coursor on the linkvSpoofed domain name

Authentication failures (SPF, DKIM, DMARC)

Foreign IP address unrelated to PayPa

Urgent subject line to induce panic

Another sample of phishing mail

Subject: Urgent: Verify Your Account Now to Avoid Suspension

From: PayPal Support security@paypa1.com

To: you@example.com

Dear Valued Customer,

We have noticed unusual activity on your account. For your security, we have temporarily limited your access.

To restore your account, please verify your information immediately by clicking the link below:

👉 htts://paypal.com.secure-login-verify.com

Failure to do so within 24 hours will result in permanent account closure.

Thank you for your prompt attention.

Sincerely, PayPal Account Security Team

I Analyze suspicious links or attachments

Sender address is security@paypa1.com instead of the official paypal.com.

Link text looks like PayPal: https://paypal.com.secure-login-verify.com

Real domain is secure-login-verify.com, which is not owned by PayPal — an example of subdomain spoofing.

Look for urgent or threatening language in the email body

We have temporarily limited your access" — creates fear of account loss

Verify your information immediately" — demands instant action

Failure to do so within 24 hours will result in permanent account closure" — strong threat to force compliance

🔗 Note any mismatched URLs

Displayed link: https://paypal.com.secure-login-verify.com

Real domain: secure-login-verify.com

❓ Why suspicious:

The real PayPal domain is paypal.com

In this link, "paypal.com" is just part of a subdomain (paypal.com.secure-login-verify.com) owned by the attacker

Everything before the last two dots in a domain can be faked — the real ownership is determined by the last two segments (secure-login-verify.com)

✅ Learning Outcome

I am able to detect some of phishing emails.

Understand the phishing email headers.

Analyze the sucipious link by hover my coursor on the link