Phishing Email Examples

This guide provides examples of common phishing emails with detailed analysis of their warning signs. Use these examples to help identify suspicious messages in your own inbox.

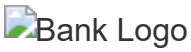
> **Study these examples to become familiar with phishing tactics.** Real phishing attempts may be more sophisticated than these examples, but will often contain similar warning signs. Always verify unexpected communications through official channels.

Example 1: Bank Account Alert

From: Bank-of-America-alerts@secure-banking-center.com

To: Valued Customer

Subject: URGENT: Your Account Has Been Temporarily Limited



Dear Valued Customer ,

We have detected unusual activity on your account . For your security, we have temporarily limited access to your online banking.

To restore full access to your account, you must verify your information immediately by clicking the link below:

VERIFY ACCOUNT NOW

If you do not verify your information within 24 hours , your account access will remain limited and may result in permanent suspension.

Thank you for your immediate attention to this matter.

Sincerely,
Bank of America Security Team

This email contains sensitive information . If you did not request a verification, please contact us immediately at 1-800-555-0123 or reply to this email.

Warning Signs Analysis

Warning Sign #1: Suspicious Sender Address

The email appears to be from "Bank-of-America-alerts@secure-banking-center.com" instead of an official bankofamerica.com domain. Legitimate banks always use their official domain names in email addresses.

Warning Sign #2: Generic Greeting

The email uses "Dear Valued Customer" instead of your actual name. Legitimate bank communications typically address you by name.

Warning Sign #3: Urgency and Threats

The email creates a false sense of urgency with "URGENT" in the subject line and threatens account suspension if you don't act within 24 hours. Scammers use urgency to pressure you into acting without thinking.

Warning Sign #4: Request for Personal Information

The email asks you to "verify your information" by clicking a link, which would likely lead to a fake website designed to steal your login credentials.

Warning Sign #5: Suspicious Link

The "VERIFY ACCOUNT NOW" button would link to a fraudulent website, not the official bank website. Always hover over links to see the actual destination before clicking.

How to Respond

If you receive an email like this:

1. Do not click any links in the email
2. Do not call any phone numbers provided in the email
3. If you're concerned about your account, open a new browser window and type in your bank's official website directly, or use their official mobile app
4. Report the phishing attempt to your bank through their official channels
5. Delete the email

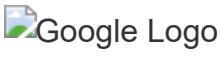
Example 2: Account Password Reset

From: secure-team@googledocs.serviceaccount.com

To: [Your Email]

Subject: Security Alert: Your Google Account password needs reset

---



Dear User,

We detected a sign-in attempt from a new device located in Lagos, Nigeria .
If this wasn't you, your password may be compromised.

Date and Time : May 17, 2025, 2:34 AM EST

Device : Android 12.0

Location : Lagos, Nigeria

IP Address : 197.255.XXX.XXX

For your account security, please reset your password immediately by clicking the link below:

Reset Password

The reset link will expire in 1 hour for security reasons.

If you believe this was a mistake, simply click here to confirm it was you and we'll update our records.

Thank you,
Google Security Team

Warning Signs Analysis

Warning Sign #1: Suspicious Sender Address

The email claims to be from Google but uses "googledocs.serviceaccount.com" instead of an official google.com domain. This is a clear red flag.

Warning Sign #2: Generic Greeting

The email uses "Dear User" instead of your name, which Google would typically include in official security communications.

Warning Sign #3: Creates Urgency

The email mentions the reset link will expire in 1 hour, creating pressure to act quickly without proper verification.

Warning Sign #4: Suspicious Links

Both the "Reset Password" button and the "click here" link would likely direct to a fraudulent website designed to capture your Google credentials.

Warning Sign #5: Discourages Alternative Verification

The "Please do not reply" instruction attempts to prevent you from seeking verification through other channels.

How to Respond

If you receive an email like this:

1. Do not click any links in the email
2. Access your Google account directly by typing accounts.google.com in your browser
3. Check your account security settings to see if there were actually any suspicious sign-in attempts
4. If you're concerned, change your password directly through Google's official website
5. Consider enabling two-factor authentication if not already active
6. Report the phishing attempt to Google

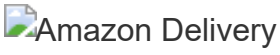
Example 3: Package Delivery Notification

From: delivery-notification@amaz0n-shipping.net

To: [Your Email]

Subject: ACTION REQUIRED: Your package delivery #39827465 is pending

---



Hello,

We attempted to deliver your package today, but we need additional delivery information to complete the delivery.

Package ID : #39827465
Status : Delivery Pending
Last Attempt : May 18, 2025

Your package will be returned to the sender in 24 hours if we do not receive the required information.

UPDATE DELIVERY INFO

If you did not expect a delivery , please disregard this message .

Thank you,
Amazon Delivery Services

Warning Signs Analysis

Warning Sign #1: Suspicious Sender Address

The email comes from "amaz0n-shipping.net" (note the use of "0" instead of "o") rather than amazon.com, which is Amazon's official domain.

Warning Sign #2: Generic Greeting

The email uses "Hello" instead of your name, which Amazon would typically include in official communications.

Warning Sign #3: Creates Urgency

The email claims your package will be returned to the sender within 24 hours, creating a false sense of urgency to act quickly.

Warning Sign #4: Vague Package Information

The email provides a generic package ID without specific details about what you ordered, unlike legitimate Amazon shipping notifications which include product information.

Warning Sign #5: Request for Information

The email asks you to update your delivery information, which would likely lead to a fake website designed to collect personal and financial data.

How to Respond

If you receive an email like this:

1. Do not click any links in the email
2. Log in to your Amazon account directly by typing amazon.com in your browser
3. Check your orders to see if you have any pending deliveries
4. If you're expecting a package, track it through your account's order history
5. Report the phishing attempt to Amazon's customer service
6. Delete the email

Example 4: Tax Refund Notification

From: irs-tax-refund@irs-govs.org

To: [Your Email]

Subject: IRS: You have a tax refund pending

IRS Logo

Dear Taxpayer ,

After the last annual calculations of your fiscal activity , we have determined that you are eligible to receive a tax refund of $783.80 USD .

To receive your refund , you must submit a refund request and provide additional verification .

Please submit your refund request within 7 days by clicking the button below:

CLAIM YOUR REFUND NOW

For security reasons, we will need to verify your identity and banking information before processing your refund.

Your refund may be delayed if you fail to verify your information within the specified timeframe.

Regards,
Internal Revenue Service
Refund Department

Warning Signs Analysis

Warning Sign #1: Suspicious Sender Address

The email comes from "irs-govs.org" rather than irs.gov, which is the official IRS domain. The IRS always uses the .gov domain for official communications.

Warning Sign #2: Generic Greeting

The email uses "Dear Taxpayer" instead of your name, which is a common trait of phishing emails.

Warning Sign #3: Requests Banking Information

The email states it needs to verify your banking information. The IRS never requests financial or personal information via email.

Warning Sign #4: Creates Urgency

The email claims you must submit your refund request within 7 days, creating a false sense of urgency.

Warning Sign #5: Unexpected Refund

If you haven't filed taxes recently or aren't expecting a refund, an unexpected refund notification is highly suspicious.

How to Respond

If you receive an email like this:

1. Remember that the IRS does not initiate contact with taxpayers by email, text, or social media to request personal or financial information
2. Do not click any links or open any attachments
3. If you're concerned about your tax refund status, visit the official IRS website directly at irs.gov
4. Forward the email to phishing@irs.gov then delete it

5. Report the phishing attempt to the FTC at reportfraud.ftc.gov

---

Remember: Official Organizations Will Not:

- Send emails from non-official domain names
- Create false urgency to pressure you into acting quickly
- Ask for your password, PIN, or full Social Security Number via email
- Send unpersonalized messages with generic greetings
- Include suspicious attachments or links to external websites
- Threaten negative consequences if you don't provide information

When in doubt, go directly to the official website by typing the address in your browser, or call the organization using a phone number you know is legitimate (from your credit card, statement, or official website).