Identify and Avoid Phishing Scams

Last Modified on 06/15/2026 4:34 pm EDT

Overview | Spot a phishing email | What to do if you receive a suspicious email | What to do if you have already selected the link | Key takeaway

Overview

Cybercriminals frequently send emails that appear to come from trusted organizations to steal usernames, passwords, financial information, or other sensitive data. These phishing emails often use company logos, familiar branding, and urgent messaging to convince recipients to take immediate action.

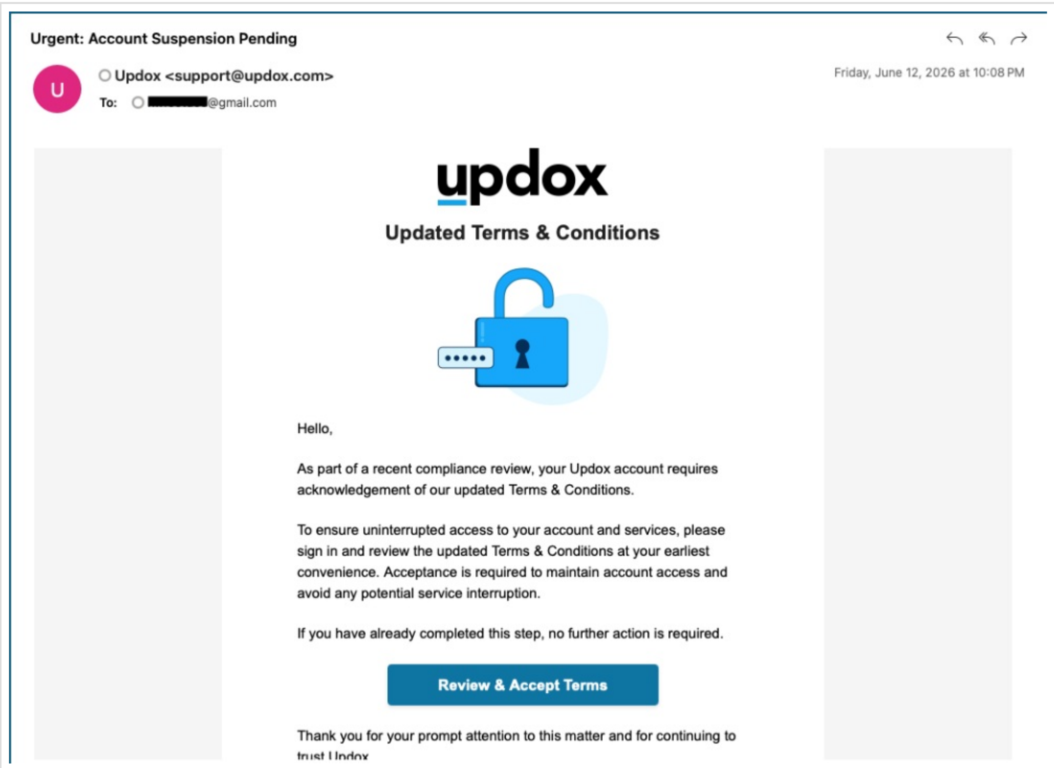
Understanding how to recognize phishing attempts can help protect your account and your organization from security incidents.

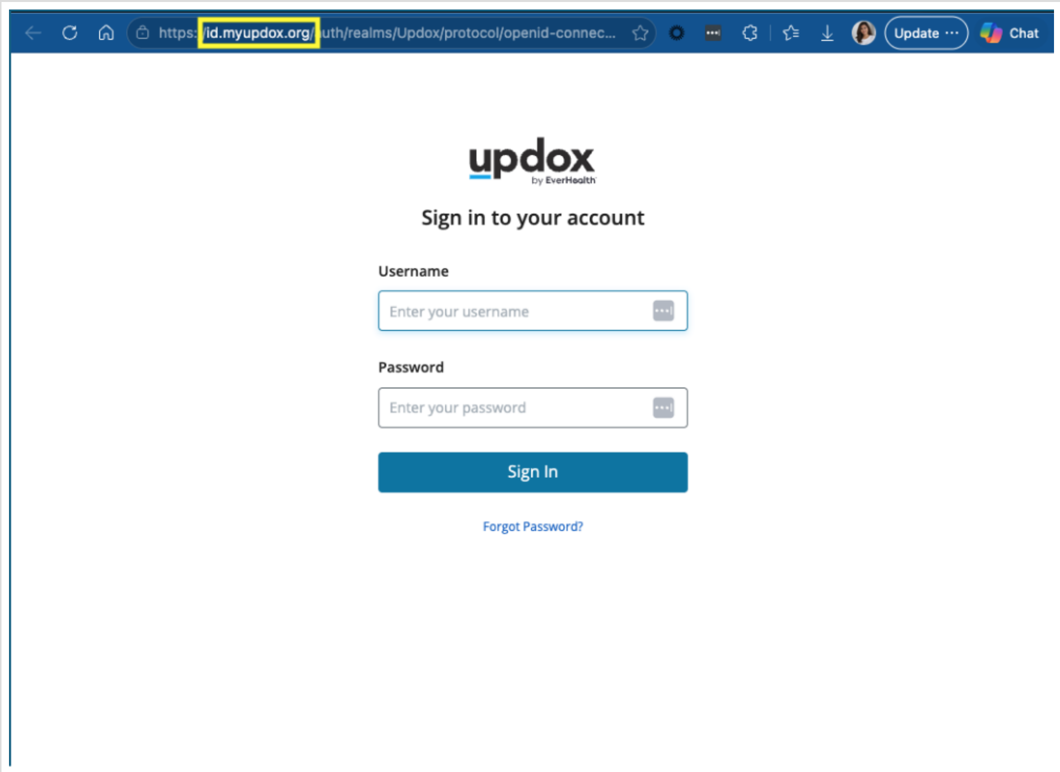
Example of a phishing email

A recent phishing email appeared to be sent by Updox and included:

- Official Updox branding and logos
- Professional formatting
- A request to review updated Terms & Conditions
- Urgent language suggesting account access could be interrupted
- A button labeled **Review & Accept Terms**

At first glance, the email looked legitimate. However, selecting the button revealed that the destination website was not an official Updox website.





Important

The only domains owned and operated by Updox are:

- updox.com
- myupdox.com

If a link takes you to any other domain, including domains that look similar to Updox, do not enter your credentials or provide any information.

Spot a phishing email

1. Check the destination URL before selecting it, and verify that the destination domain is:
    - updox.com - our main site
    - myupdox.com - our login site

    Always hover your mouse over links and buttons before selecting them.

    Be suspicious of links that:

    - Use unfamiliar domains
    - End in unexpected extensions such as .org, .net, or other domains not owned by Updox
    - Include misspellings or additional words that mimic legitimate websites

2. Be wary of urgent requests.

    Phishing emails often create a sense of urgency. Attackers use urgency to encourage users to act before verifying the email.

    Examples include:

- "Account suspension pending"
- "Immediate action required"
- "Verify your account now"
- "Your access will be terminated"

3. Verify requests through official channels. If an email asks you to:

    - Update account information
    - Reset your password
    - Accept new terms
    - Verify your identity

    Do not use the link provided in the email. Do this instead:

    a. Open a new browser window.
    b. Go directly to:
        - https://www.updox.com/
        - https://id.myupdox.com
    c. Sign in through the official website.

4. Inspect the sender carefully

    The displayed sender's name may look legitimate, while the actual email source may be different.

    Always verify:

    - The sender's address
    - The domain sending the message
    - Whether the message was expected

5. Never enter credentials on untrusted sites.

    If you select a link and the website address is not an official Updox domain:

    - Do not enter your username or password.
    - Close the browser window immediately.
    - Report the email to your IT or security team.

What to do if you receive a suspicious email

- Do not select any links.
- Do not download any of the attachments.
- Take a screenshot if possible.
- Report the message to your security or IT team.
- Delete the email after reporting it.

What to do if you have already selected the link

If you selected a suspicious link or entered your credentials:

- Change your password immediately. Create a strong and unique password.

    > Passwords must be at least 10 characters long (16+ recommended) with at least one uppercase letter, one lowercase letter, and one number or special character.

- Notify your security or IT team.
- Monitor your account for unusual activity.
- Enable multi-factor authentication (MFA) if available.
- For accounts with MFA available, refer to How To: Setting Up Multi-factor Authentication (MFA) for more information about how an account holder can enable MFA.

Key takeaway

A professional appearance doesn't guarantee that an email is legitimate. Always verify the destination website before selecting any link. For Updox-related communications, only trust websites hosted on:

- updox.com
- myupdox.com

If a link directs you anywhere else, treat it as suspicious and report it immediately. If you need assistance resetting your password or need more information on MFA and whether it’s currently available for your account, contact support via live chat or email support@updox.com.