Subject: Important Security Notice: Protect Yourself from Fraudulent and Phishing Emails

Dear Valued Upwardor Customer,

We hope this email finds you well and safe. We are writing to inform you about a crucial matter that requires your attention and vigilance.

In recent times, there have been an increasing number of fraudulent masking emails and phishing attempts targeting unsuspecting customers like yourself. These malicious activities aim to deceive and manipulate recipients into divulging sensitive information, such as login credentials, financial data, or personal details.

As your trusted partner, we take your security and privacy very seriously. We want to ensure that you remain protected against these threats. Here are some essential steps you can take to safeguard yourself from fraudulent and phishing emails:

1. **Verify Email Sources**: All official communications from Upwardor will always come from email addresses ending with our default domain, "upwardor.com." If you receive any emails claiming to be from Upwardor but using a different domain, please treat them with suspicion and report them immediately to our team.

2. **Exercise Caution with Links**: Avoid clicking on links or downloading attachments from unknown or suspicious sources, even if they appear to be from our domain. If you are uncertain about the legitimacy of a link, contact our support team for verification.

3. **Do Not Open Attachments from Malicious Emails**: As part of our email communication policy, Upwardor will not send unsolicited attachments. If you receive an unexpected attachment from an email claiming to be from us, refrain from opening it and report to our support team immediately.

4. **Beware of Urgency and Threats**: Fraudulent emails often use urgent language or threats to create a sense of panic and rush you into taking action. Always remain calm and verify the authenticity of such communications through official channels.

5. **Do Not Share Personal Information**: Upwardor will never ask you to provide sensitive information, such as passwords or financial details, via email. If you receive any such requests, do not respond and inform our support team promptly.

6. **Enable Multi-Factor Authentication (MFA):** Whenever possible, enable MFA for your Upwardor accounts to add an extra layer of security.

7. **Keep Software Updated**: Ensure that your operating system, antivirus software, and web browsers are up to date with the latest security patches. Regular updates help protect your devices from known vulnerabilities.

8. **Report Suspicious Emails**: If you receive any emails that appear to be fraudulent or phishing attempts, please report them immediately to our support team. We will investigate and take appropriate action to protect our customers.

As a cautionary example, we want to share some suspicious email addresses that you should be wary of:
- info@upwarrdor.com
- info@upwardo.com
- info@up.wardor.com
- info@upwa.rdor.com
- info@upwardot.com

Please be assured that all our communication with you will strictly adhere to our default domain, "**upwardor.com**"

Your security is our top priority, and we are committed to maintaining a secure environment for all our customers. If you have any questions or concerns regarding email security or any other matter, please don't hesitate to contact our support team. We are here to assist you in any way we can.

Thank you for your attention and cooperation in this critical matter.

Stay safe and secure.

Best regards,
Upwardor Inc.