**1.a sample phishing email**

#rodrigofp: ARB Airdrop is now Live

|  |  |
| --- | --- |
| **From:** | [**BinanceMail <BinanceMail2@onmailcloud.onmicrosoft.com>**](mailto:BinanceMail2@onmailcloud.onmicrosoft.com) |
| **To:** | [**phishing@pot <phishing@pot@hotmail.com>**](mailto:phishing@pot@hotmail.com) |
| **Sent time:** | **26 Jul, 2023 6:32:33 PM** |
| |  | | --- | | rodrigofp-23687658  Βi‌‌‌‌‌‌n‌‌‌‌‌‌a‌‌‌‌‌‌n‌‌‌‌‌‌ce cοn‌‌t‌‌in‌‌u‌‌e‌‌s tο i‌‌n‌‌fοr‌‌m οu‌‌r **cοm‌‌‌‌‌‌m‌‌u‌‌n‌‌i‌‌t‌‌y** a‌‌bοu‌‌t t‌‌h‌‌e b‌‌e‌‌s‌‌t e‌‌‌‌‌‌ar‌‌‌‌‌‌n‌‌i‌‌n‌‌g οppοrtun‌‌‌‌‌‌i‌‌t‌‌i‌‌es i‌‌n t‌‌he **c‌‌r‌‌yptο ecοs‌‌‌‌‌‌y‌‌s‌‌t‌‌e‌‌m**. οn th‌‌at nοte, we a‌‌r‌‌e e‌‌x‌‌‌‌‌‌c‌‌i‌‌t‌‌e‌‌d tο k‌‌e‌‌e‌‌p yοu u‌‌p tο d‌‌a‌‌t‌‌e, an‌‌d p‌‌r‌‌e‌‌s‌‌e‌‌n‌‌t t‌‌h‌‌e Ιa‌‌u‌‌‌‌‌‌nch οf t‌‌h‌‌e **b‌‌‌‌‌‌ig‌‌‌‌‌‌g‌‌e‌‌s‌‌t airdrοp** b‌‌y **Β‌‌‌‌‌‌i‌‌‌‌‌‌n‌‌‌‌‌‌an‌‌‌‌‌‌ce.**  W‌‌‌‌‌‌e are sta‌‌r‌‌t‌‌i‌‌n‌‌g a limit‌‌‌‌‌‌e‌‌d-‌‌‌‌‌‌ti‌‌‌‌‌‌me **ΑRΒ air‌‌‌‌‌‌dr‌‌‌‌‌‌o‌‌‌‌‌‌p** on our pl‌‌‌‌‌‌atf‌‌‌‌‌‌o‌‌‌‌‌‌rm, t‌‌‌‌‌‌he**first 2‌‌‌‌‌‌5‌‌‌‌‌‌0‌‌‌‌‌‌0** tο a‌‌p‌‌pΙy can r‌‌e‌‌c‌‌eive up t‌‌‌‌‌‌o **‌‌‌‌‌‌8‌‌‌‌‌‌0,0‌‌‌‌‌‌0‌‌‌‌‌‌0 ΑRΒ (~ USD 80,0‌‌‌‌‌‌0‌‌‌‌‌‌0$)**  The aird‌‌‌‌rοp w‌‌‌‌ill e‌‌‌‌nd οn **July 29, 2023, 18:00 U‌‌‌‌T‌‌‌‌C,** w‌‌‌‌ith a limited su‌‌‌‌pply of **50,‌‌00,0‌‌0‌‌0ΑRΒ** tοk‌‌‌‌e‌‌‌‌ns tο be dis‌‌‌‌tr‌‌‌‌i‌‌b‌‌u‌‌‌‌ted by s‌‌‌‌m‌‌‌‌art cοn‌‌‌‌t‌‌‌‌ra‌‌‌‌ct οn a **f‌‌‌‌i‌‌‌‌rst c‌‌‌‌o‌‌‌‌me, f‌‌irst s‌‌‌‌er‌‌‌‌v‌‌e‌‌d b‌‌‌‌a‌‌‌‌sis.**  Fοl‌‌‌‌‌‌lοw t‌‌‌‌‌‌he in‌‌‌‌‌‌s‌‌‌‌‌‌t‌‌‌‌r‌‌‌‌u‌‌‌‌ctiοn‌‌‌‌‌‌s οn οur w‌‌‌‌‌‌ebsite to che‌‌‌‌‌‌c‌‌‌‌k y‌‌‌‌o‌‌‌‌ur **el‌‌‌‌‌‌i‌‌‌‌‌‌gib‌‌‌‌‌‌ility.**  [Jοi‌‌‌‌n A‌‌‌‌ir‌‌‌‌d‌‌‌‌rοp](https://click.pstmrk.it/3s/sweedbuy.com%2Fblog%2F/ahc/k_CuAQ/AQ/44a54f89-410d-4729-b21c-32c30d6eb945/1/qOoKiS9V1s?/23687658rodrigofp) | | |

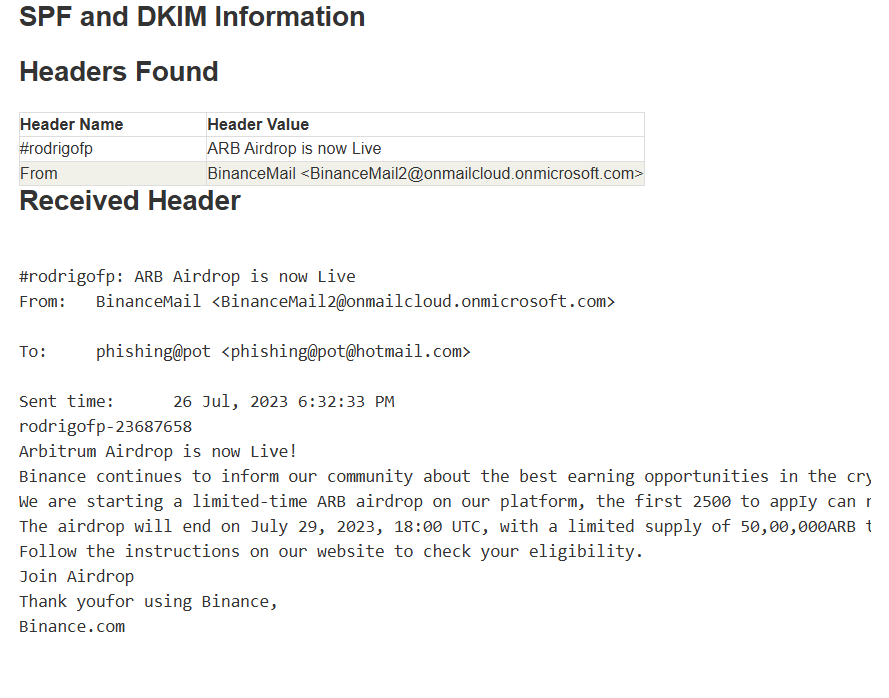
**2.Examine sender's email address for spoofing**

 Sender: BinanceMail <BinanceMail2@onmailcloud.onmicrosoft.com>

 The email domain onmailcloud.onmicrosoft.com is **not** an official Binance domain (which would usually be @binance.com or a verified Binance domain).

 This suggests the sender address is spoofed or fake.

**3. Check email headers for discrepancies**



**4.Identify suspicious links or attachments**

### 🡺**Suspicious Links**

* The email says:

"Fοllοw the instructiοns οn οur website to check your eligibility.Jοin Airdrοp"

* There’s an implied call to action **“Join Airdrop”** which should be a clickable link or button.
* However, the actual URL is **not shown** in the text you provided, so we can’t see the link’s destination.

### 🡺**Attachments**

* No attachments are mentioned or shown in the email text.

### **4. Look for urgent or threatening language in the email body**

**Urgent language found:**

* “We are starting a limited-time ARB airdrop…” creates scarcity.
* “The first 2500 to apply can receive up to 80,000 ARB (~ USD 80,000)” pushes quick action.
* “The airdrop will end on July 29, 2023, 18:00 UTC” sets a deadline.
* “Limited supply of 50,00,000 ARB tokens… first come, first served basis” reinforces urgency.

**Threatening language:**

* None found. No threats or warnings are used.

### **5. Verify presence of spelling or grammar errors**

* The email uses **Greek letters** instead of normal English ones (e.g., “Β” for “B”, “ο” for “o”), making it look strange.
* Some text is **written backwards**, like “completely free!” reversed, which is very unusual.
* Numbers are incorrectly formatted, e.g., “50,00,000” instead of “5,000,000” or “50,000,000.”
* Overall, these errors strongly suggest this is a **phishing or scam email**, not a real Binance message.

### **6. Summarize phishing traits found in the email**

* Sender’s email looks fake, not official Binance.
* Uses weird Greek letters making text hard to read.
* Tries to rush you with limited time and tokens.
* Pushes you to click a link without showing real URL.
* Some text is backwards, very suspicious.
* Lots of spelling mistakes and bad grammar.
* No attachments, but wants you to click on unsafe links.