Phishing Email Summary:

- Sender: ia0pr02mb9779.namprd02.prod.outlook.com, info-yagcfgyuze@boonsupply.com, [no.reply.alerts@chase.com](mailto:no.reply.alerts@chase.com)

- Header: Domain not found in SPF, DMARC Quarantine/Reject policy not enabled

- Link: Hover reveals phishing domain (<https://dsgo.to/CQECQECnpqY3NDSGtODt9ft2qtxzcXGUveTV5fRYmtYAZsQCnpqY3NDSGtODt9ft2qtxzcXGUveTV5fRYmtYAZsQCQECnpqY3NDSGtODt9ft2qtxzcXGUveTV5fRYmtYAZsQ>)

- Attachment: jpge file

- Language: "Your Bank Account has been blocked due to unusual activities CASE# T53-H32-C10-C83"

Conclusion: Attackers embed a legitimate-looking webpage (like a game or social media page) within an [iframe](https://www.google.com/search?sca_esv=d5e847b1dc31b2cb&rlz=1C1ONGR_enIN1104IN1105&sxsrf=AE3TifMji3thquRGaATgVOtwsCwVBNrtog%3A1754415436796&q=iframe&sa=X&sqi=2&ved=2ahUKEwjwg5jnmvSOAxXWRmwGHUBTBmoQxccNegQIMBAB&mstk=AUtExfD9JlyTpUkX-EQsHnKpulGXn0vKeQw5D18Uq739_B-U452UdoDNf45Vw-PFLoyrRH_kDbkE755fSxcXcf2FLQzB-TuPaw8B3aac136GOlpTI96M6HolxF7CKTbFOmlv9wiF42tMxfWHwU2q9fNBuhx2NTCI18AcRAxU4gN6HyBKHuC0XCwjxVKzI33-Lxme3TACqy1d---_3JVUzHTe7H3XKq2kcakdCQcv3jycVXwOAYjvAjOXQ_GiHzDIwKf5noFN-j3EYlNsKpUALAYQrSCy&csui=3" \t "_blank), and then overlay it with a seemingly harmless, but actually malicious, page.

* The user interacts with the visible, decoy page, but their clicks are actually registered on the hidden, malicious page underneath.

**Header Analyzed -sample-5.eml**

**Delivery Information**

* Problem Icon [DMARC Compliant (No DMARC Record Found)](https://mxtoolbox.com/dmarc/problem/dmarc-record-published)

The **sender's domain has no DMARC record** published.

Because there's no DMARC policy to check, the email is **marked “compliant” by default**.

Red **flag** – legit domains (like banks or companies) should have DMARC to prevent spoofing.

This could indicate a **phishing or spoofed email**.

* + Problem Icon [SPF Alignment](https://mxtoolbox.com/Public/Tools/EmailHeaders.aspx?huid=41683d8e-f34a-48a9-8004-5369a88d1930)

checks if the email was sent from an IP authorized by the domain's DNS.

If SPF Alignment Passes: The domains match → likely legitimate.

* + Ok Icon [SPF Authenticated](https://mxtoolbox.com/Public/Tools/EmailHeaders.aspx?huid=41683d8e-f34a-48a9-8004-5369a88d1930)

PF **Authenticated** means the email **was sent from an IP address that’s allowed** by the domain's SPF record.

The sending server **passed the SPF check**, verifying it's **authorized** to send on behalf of the domain.

* + Problem Icon [DKIM Alignment](https://mxtoolbox.com/Public/Tools/EmailHeaders.aspx?huid=41683d8e-f34a-48a9-8004-5369a88d1930)

DKIM **(DomainKeys Identified Mail)** uses a digital signature to verify the email wasn’t altered and came from an authorized sender.

DKIM **Alignment** means the **domain in the DKIM signature matches the “From” address domain** (or is a subdomain).

* + Problem Icon [DKIM Authenticated](https://mxtoolbox.com/Public/Tools/EmailHeaders.aspx?huid=41683d8e-f34a-48a9-8004-5369a88d1930)

DKIM **Authenticated** means the **email has a valid DKIM signature**.

The signature was verified using the **public key** published in the sender's DNS.

This proves the **email was not tampered with** in transit and was **authorized by the signing domain**.