Email Phishing

June 24, 2025

1 Summary

Conducted an assessment on a phishing email. The message body featured an urgent and threatening language and notable grammar errors.

2 Technical Details and Evidence

2.1 Sender Email Address

The sender email address (trust.ameribank7.com) is not an official domain of Bank of America. Official domain of Bank of America "bankofamerica.com".

From: authenticationmail@trust.ameribank7.com
To: johnsmith@email.com
Subject: **A new login to your bank account**

2.2 Email Headers

Here the sender mail address and the reply-to are same.Return-Path:(authenticationmail@trust.ameribank7.com exact copy of the sender, as the sender domain is not official the repy-to also re-directing to the attacker. The email source hostname is malicious.

2.3 Suspicious Link

Malicious link on the body of the email that to reset password using the link given. The link not seem to have the domain name or anything related to the Bank of America, making it suspicious.

If this was not you, please reset your password immediately with this link:

https://trust.ameribank7.com/reset-password

2.4 Language

The language used in this context is highly unprofessional. Urges the user to reset their password immediately. There is a clearly visible spelling mistake in the body of the email, such as 'divice' instead of 'device', which further indicates it is not a legitimate message.

> Dear account holder,
>
> There has been a recent login to your bank account from a new divice:
>
> IP address: 192.168.0.1
>
> Location: Miami, Florida
>
> **4 new transactions have been made with this account since your last login.**

3 Impact

Attacker have access to your system. Loss of credentials and personal data. Loss of money or assets.

4 Remediation Advice

- Verify the sender, Attackers mostly use similar domains for the attack. Hover over links to ensure the URL matches the supposed sender.
- Never download or open attachments from an untrusted sender.
- Do not click the button that redirects to any untrusted site.