Phishing Email Detection &Awareness Assessment Report

Prepared by

kakumanu Jaya Dharani

Future Interns Internship

Task-2 Phishing Detection &Awareness Assessment

Objective

The objective of this task is to analyze a phishing email sample, identify malicious indicators, classify associated risks, and provide awareness guidelines to help users
recognize and prevent phishing attacks

Phishing Email Sample

The analyzed email claims to be from SBI (State Bank of India) and informs the recipient about “unusual activity” detected in their bank account. The message warns that the account will be permanently suspended within 24 hours unless immediate verification is completed through a provided link.

The email creates a sense of urgency and fear to pressure the recipient into clicking the verification link. However, the sender’s email address and the provided URL do not match the official SBI domain, indicating a likely phishing attempt.

This type of email is commonly used in credential harvesting attacks, where attackers attempt to steal sensitive information such as banking usernames, passwords, and OTPs by redirecting victims to a fake login page that mimics the official bank website.

Email Header Analysis

The sender email address support@sbi-verification-alert.com does not match the official SBI domain (sbi.co.in). This indicates domain spoofing. The verification link uses HTTP instead of secure HTTPS, which is unsafe for banking services. The domain contains extra words like “verification” and “alert,” which are commonly used in phishing emails to appear legitimate.

Domain & Link Inspection

The sender domain sbi-verification-alert.com does not match the official SBI domain sbi.co.in, indicating a spoofed or fake domain.

The verification link http://sbi-secure-login-alert.com/verify uses HTTP instead of secure HTTPS and redirects to a non-official website.

The domain name contains extra words like “secure” and “alert,” which are commonly used in phishing websites to appear legitimate

Phishing Indicators Identified

1. Fake Sender Domain – The email domain sbi-verification-alert.com does not match the official SBI domain (sbi.co.in).
2. Suspicious Link – The verification link redirects to a non-official website and uses insecure HTTP.
3. Urgency Tactic – The email pressures the user by stating the account will be suspended within 24 hours.
4. Generic Greeting – The message starts with “Dear Customer” instead of the user’s registered name.
5. Request for Verification – The email asks the user to verify account details, which legitimate banks do not request via email.

Risk Classification

Classification: HIGH RISK – PHISHING EMAIL

The email is classified as high risk because it contains a fake sender domain, a suspicious verification link, and urgency tactics designed to pressure the user into revealing sensitive banking information. If the user clicks the link and enters credentials, it may lead to financial fraud, unauthorized transactions, and identity theft.

Attack Explanation

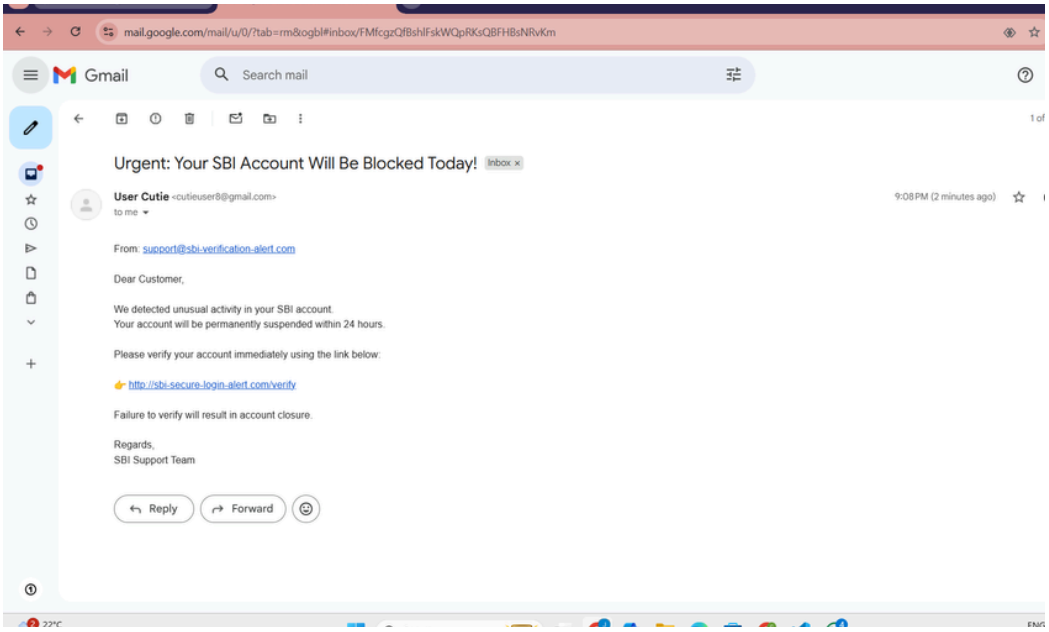
This email represents a phishing attack where the attacker impersonates SBI to trick the user into revealing sensitive banking credentials

.

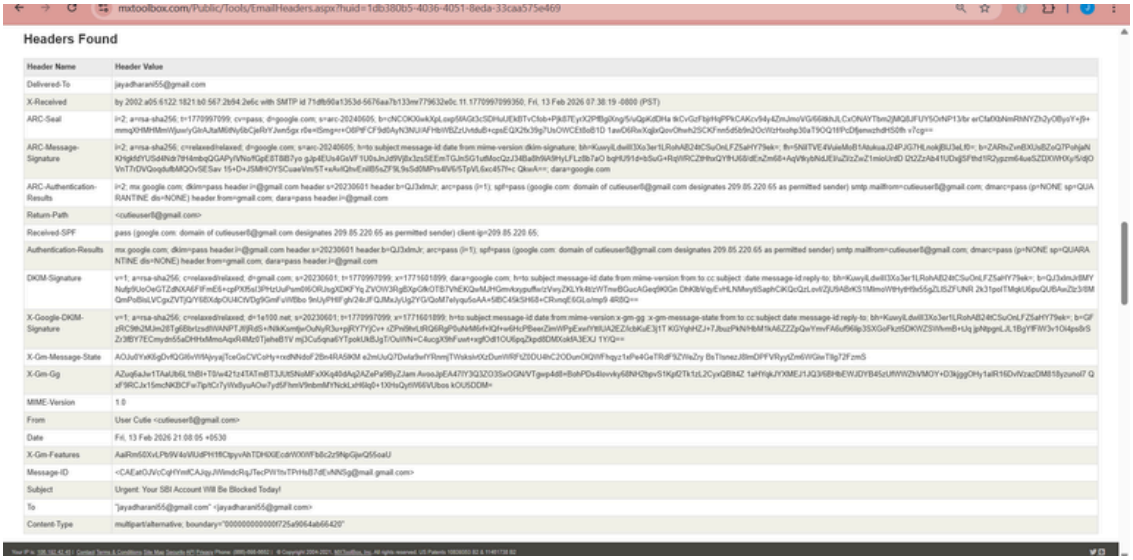
The attacker sends a fake email containing a malicious verification link. When the user clicks the link, they are redirected to a fraudulent website that looks like the official bank login page. If the user enters their username, password, or OTP, the information is captured by the attacker.

The attacker can then use the stolen credentials to access the victim’s bank account and perform unauthorized transactions.

Phishing Email Sample

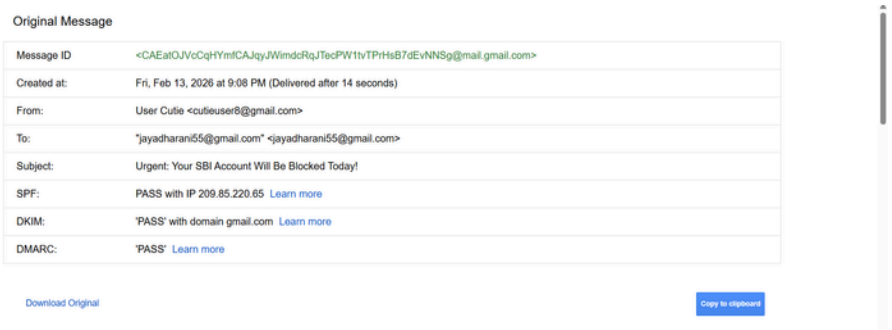


Email Header Analysis



Headers Found

Header Name	Header Value
Delivered-To	jayadharani55@gmail.com
X-Received	by 2002:a05:6122:1821:b0:567:2b94:2e6c with SMTP id 71dfb90a1353d-5676aa7b133mr779632e0c.11.1770997099360; Fri, 13 Feb 2026 07:38:19 -0800 (PST)
ARC-Seal	i=2; a=rsa-sha256; t=1770997099; cv=pass; d=google.com; s=arc-20240605; b=cNCOKGkwkXpLoxp5fAGt3cSDfHuJEkBTvCfob+PjkBTEyrX2PBfgGXng/5/uQpKdDHa tkCvGzFbjrHqPPkCAKcv94y4ZmJmoVrG/668khJLCxONAYTbm2jMQBJFUYSOrNP13/br erCfaKKkNmRhNYZh2yOBysY+jfp+ mmqXHMHMmWjuwlyGtrAJtaM6tNy6bCjeRrYJwn5gx r0e+tSmg==+O8PtFCF9d0AyN3NUAFHbWBZzUv4duB+cpsECjX2fx39g7UsOWCEtbo81D 1awD6RwXqjkrQovOhwh2SCKFnm5d5b9n2OcWzthxohp30aT9OQ1tlPcDfjemxzhdH50fh v7cg==
ARC-Message-Signature	i=2; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20240605; h=to:subject:message-id:date:from:mime-version:dkim-signature; bh=KuwyILdwll3Xo3er1LRohAB24tCSuOnLFZ5aHY79ek=; b=ZARbvZvnBXUsBZwQ7PohjaN KHgk6tYU5d4Nck7tH4mbqQGAPyfVNofRqpEE8BBJ7yo gJp4EUs4GaVF1U0sJnJd9VjBx3zsSEEmTGJn5G1utMocQzJ34Ba8hI9A5HyLFLzSb7aO bqHU91d+bSuG+RqWRCZtHtxQYBHJ6SIdEnZm68+AqVlKybNdJEIiuZIzZwZ1mioUrdD t2tZzAb41UDxjl5Fthd1R2ypzm64ue5ZDXWHXly5/djO VnTrDVQoqdulbMQOvSESav 15+D+JSMHOYSCuaeVm/5T+xAxlQhvEnl85sZF9L9s5d0MPra4fV6/5Tp/VL6xc457l+c QkwA==; dara=google.com
ARC-Authentication-Results	i=2; mx.google.com; dkim=pass header.i=@gmail.com header.s=20230601 header.b=QJ3xlmJr; arc=pass (i=1); spf=pass (google.com: domain of cutieuser8@gmail.com designates 209.85.220.65 as permitted sender) smtp.mailfrom=cutieuser8@gmail.com; dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com; dara=pass header.i=@gmail.com
Return-Path	<cutieuser8@gmail.com>
Received-SPF	pass (google.com: domain of cutieuser8@gmail.com designates 209.85.220.65 as permitted sender) client-ip=209.85.220.65;
Authentication-Results	mx.google.com; dkim=pass header.i=@gmail.com header.s=20230601 header.b=QJ3xlmJr; arc=pass (i=1); spf=pass (google.com: domain of cutieuser8@gmail.com designates 209.85.220.65 as permitted sender) smtp.mailfrom=cutieuser8@gmail.com; dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com; dara=pass header.i=@gmail.com
DKIM-Signature	v=1; a=rsa-sha256; c=relaxed/relaxed; d=gmail.com; s=20230601; t=1770997099; x=1771601899; dara=google.com; h=to:subject:message-id:date:from:mime-version:from:to:cc:subject :date:message-id:reply-to; bh=KuwyILdwll3Xo3er1LRohAB24tCSuOnLFZ5aHY79ek=; b=QJ3xlmJrBMY Nufg9UsOeGTZdNXA6FIFmE6+cpPX6sI3FHzUuPsm0l6ORJtqXDKFYqZVOW3RgBXpGfkOTBTVhEKQxMJHGmvkxypuffwlzVwyZKLYk4tzWTmwBGucAGeqfkKGn DhK8kVqyE+HLNMwy6SaphCiKQcQzLov6ZjUlABdK51MmoWHyH9b55gZL8SZFUNR 2k31poITMqkU6puQUBAwZb3/8M QmPoBIsLVCgxZVTjQiY6EKdpOU4CIVDgl3GmFuIVBbo 9nUyPHIFgh/2ibJFQJMxJyUgZYG/QoM7elyqu5oAA+5lBC45k5H68+CRvmqE6GLo/mp9 4RBQ==
X-Google-DKIM-Signature	v=1; a=rsa-sha256; c=relaxed/relaxed; d=1e100.net; s=20230601; t=1770997099; x=1771601899; h=to:subject:message-id:date:from:mime-version:x-gm-gg :x-gm-message-state:from:to:cc:subject:date:message-id:reply-to; bh=KuwyILdwll3Xo3er1LRohAB24tCSuOnLFZ5aHY79ek=; b=GFzRC99h2MJm28Tgl6Bbr1zsdlWANPTJ9jRdS+/NlkKomfjwOuNyR3u+pjRYTYjCv+ rZPw9hrLtRQ6RgPSuNM6f+KQHw6HcPBeerZimWPpExwhYtlUA2EZJlcbKuE3j1T KGYqHHZJ+7JbuzPkN/HbM1hA6ZZZpQwYmvFA6uf96lp3SXGoFkzt5DKWZSIWhmB+Uq jpNtpgnL/L1BgYIFW3v1OI4ps8rSZr3BY7ECmydn55aDHHxMmoAqxR4Mz0TjehwBTV mj3Cu5qna6YTpokUkBJgT/OuWN=C4ucgX9hFvwt+xgfOd1OU6pqZkpd8DMXokflA3EXJ YYQ==
X-Gm-Message-State	AOJu0YxK6gDvRQG6vWfAjrya|TceGsCVCoHy+rxdNNdoF2Bn4RA5iKM e2mUuQ7Dwla9wfYRnmjTWskslvXzDunWRFlZ0DU4hC2ODumOlQIWFhqyz1xPe4GeTRdF9ZWaZry BsTisnezJ8ImDPFVRyyZm6WGiwTi9g72FzmS
X-Gm-Gg	AZuq6aJe1TAaUb6L1hBI+T9/w421z4TATmBT3JUtSNsMFxXKq40dAq2AZePa9ByZJam AvooJpEA47lY3Q3ZO3SxOGNVTgwp4d8+BohFDs4lovvky68NH2bpvS1KpfZTk1zL2CyxQBtMZ 1aHYqkJYXMEJ1JG3/6BHbEWJDYB45zUtWWZhVMOY+D3kjggGHy1aIR16DvWzacDM818yzunol7 QxF9RCJx15mcNKBCFw7lp/fCx7yWx8yuAOw7yd5FhmV9nbmMYNckLxH6lq0+tXHsQyfiW66VUbos kOU5DDM=
MIME-Version	1.0
From	User Cutie <cutieuser8@gmail.com>
Date	Fri, 13 Feb 2026 21:08:05 +0530
X-Gm-Features	AaiRm52XvLPb9V4oVlUdPH18CtpyvAhTDHX0ECcdrW0XWFb8c2z9NpGjuvQ55oaU
Message-ID	<CAEatOJVcCqHYmfCAJqyJWimdcRqJTecPW1tvTPrHsB7dEvNNSg@mail.gmail.com>
Subject	Urgent: Your SBI Account Will Be Blocked Today!
To	"jayadharani55@gmail.com" <jayadharani55@gmail.com>
Content-Type	multipart/alternative; boundary="0000000000000725a9064ab66420"



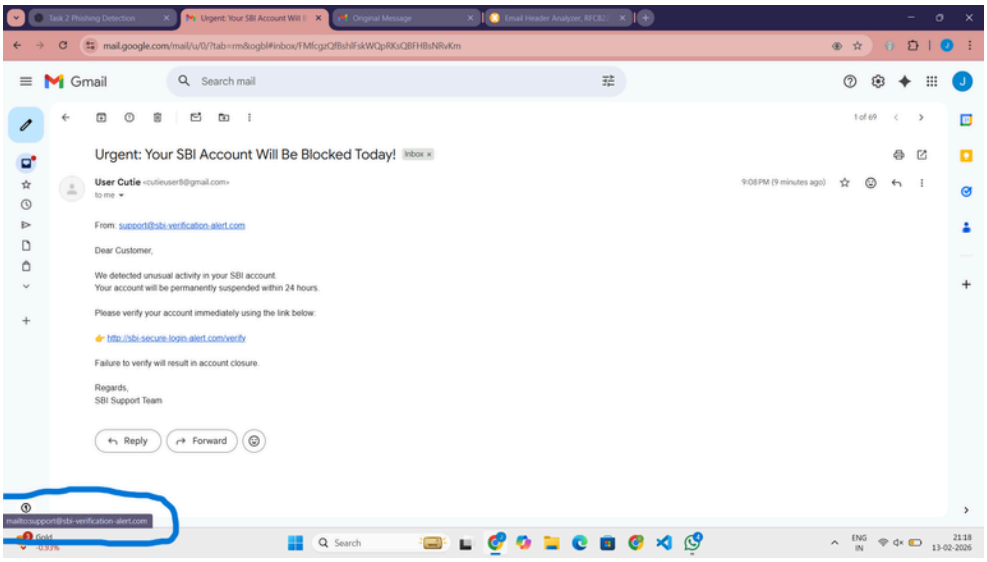
Original Message

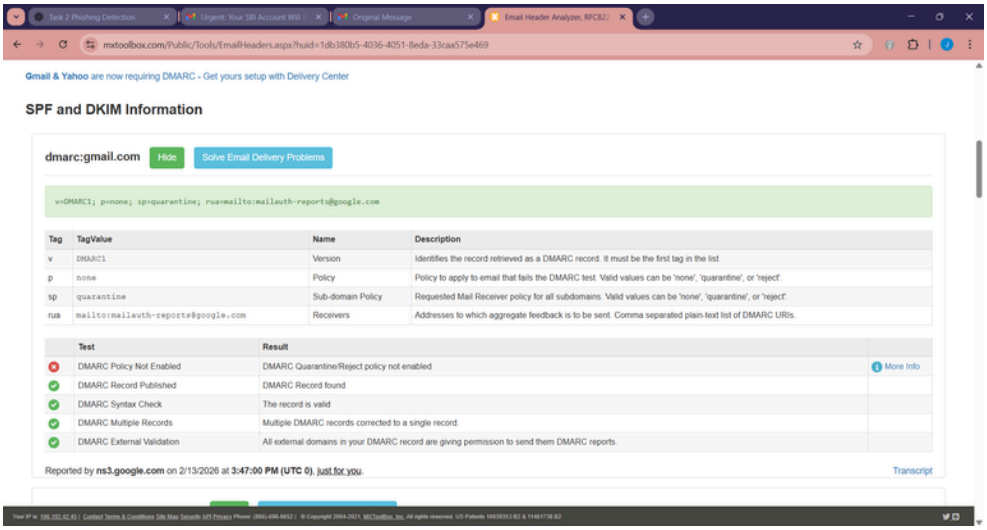
Message ID	<CAEatOJVcCqHYmfCAJqyJWimdcRqJTecPW1tvTPrHsB7dEvNNSg@mail.gmail.com>
Created at:	Fri, Feb 13, 2026 at 9:08 PM (Delivered after 14 seconds)
From:	User Cutie <cutieuser8@gmail.com>
To:	"jayadharani55@gmail.com" <jayadharani55@gmail.com>
Subject:	Urgent: Your SBI Account Will Be Blocked Today!
SPF:	PASS with IP 209.85.220.65 Learn more
DKIM:	'PASS' with domain gmail.com Learn more
DMARC:	'PASS' Learn more

Download Original

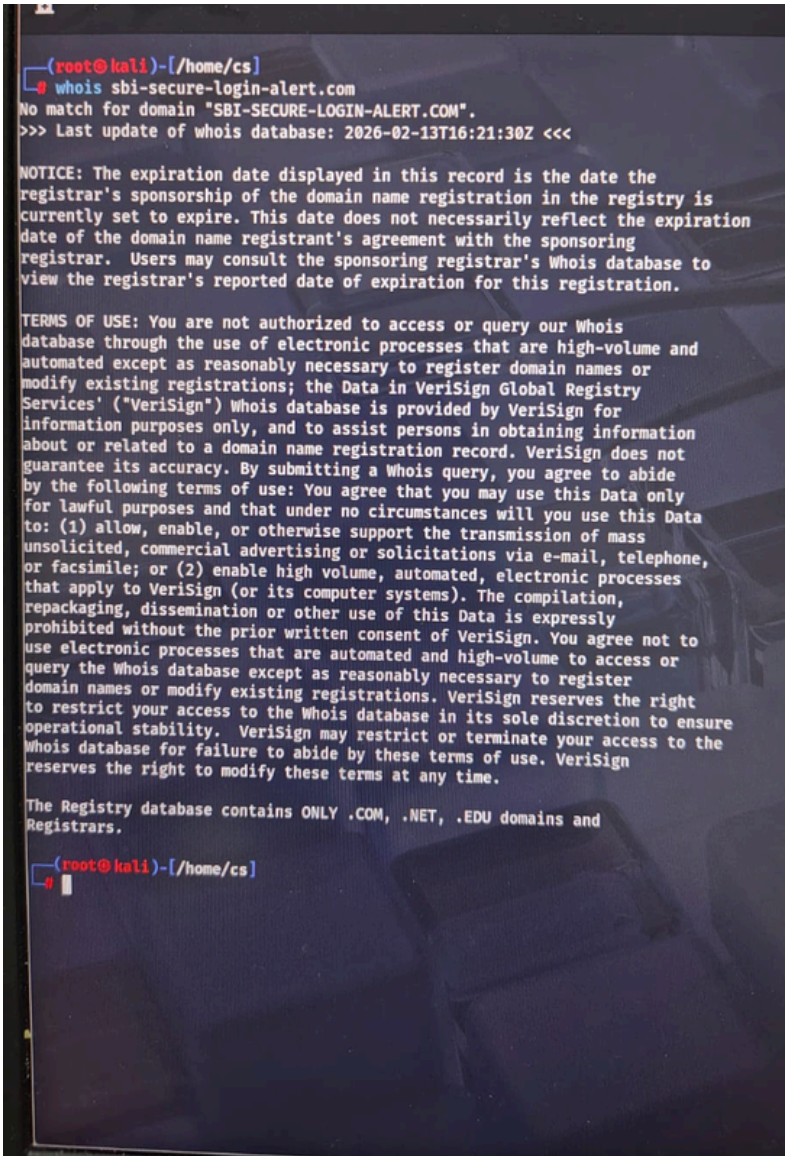
Copy to clipboard

Domain and Link Inspection






(root@kali)-[/home/cs]
ping sbi-secure-login-alert.com
ping: sbi-secure-login-alert.com: Name or service not known
(root@kali)-[/home/cs]
#


(root@kali)-[/home/cs]
whois sbi-secure-login-alert.com
No match for domain "SBI-SECURE-LOGIN-ALERT.COM".
>>> Last update of whois database: 2026-02-13T16:21:30Z <<<
NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar. Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.
TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability. VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.
The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
(root@kali)-[/home/cs]
#

Prevention Guidelines

Always verify the sender’s email domain before trusting the message.
Do not click suspicious links in emails or messages.
Type the official bank website URL manually in your browser.
Ensure the website uses HTTPS before entering sensitive information.
Never share passwords, PINs, or OTPs via email.
Enable Two-Factor Authentication (2FA) for added security.
Report suspicious emails to the bank or cybersecurity team immediately.

conclusion

The analyzed email is a clear phishing attempt impersonating SBI. It uses a fake domain, malicious verification link, urgency tactics, and generic greetings to deceive users into revealing sensitive banking information.

Domain and link inspection, header analysis, and phishing indicators confirm that the email poses a high security risk. User awareness, careful verification of email sources, and strong security practices are essential to prevent financial fraud and protect personal information.