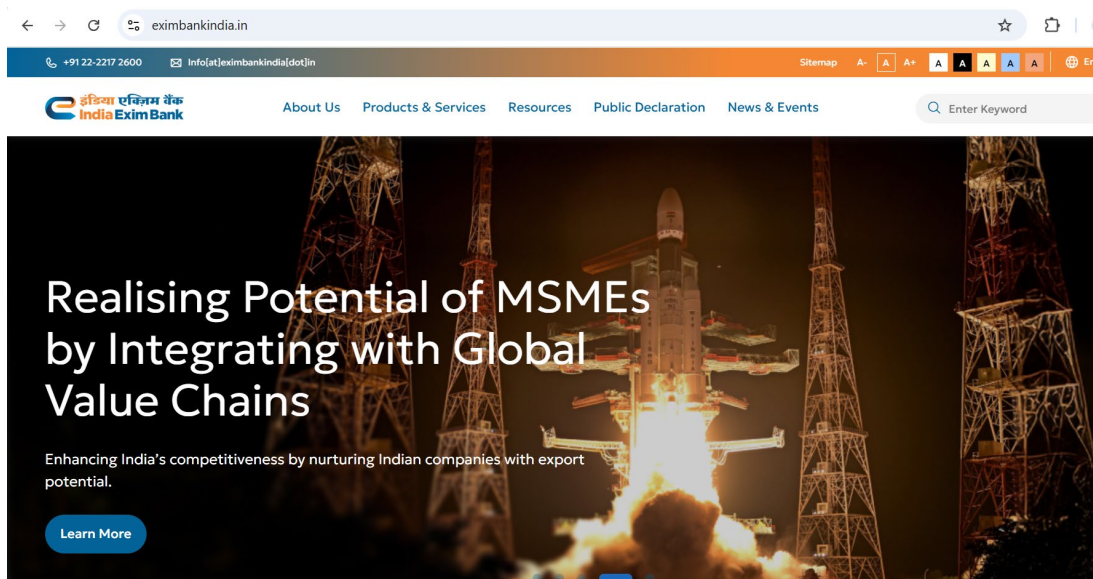


Website-Security Tips

Official Website: www.eximbankindia.in



To protect yourself from fraud, phishing, and cyber threats, please follow the guidelines below when accessing the official website of Export-Import Bank of India (Exim Bank).

Important Notice:

Exim Bank does not offer retail or individual banking services.

We do **not maintain savings, current, or personal accounts** for individuals. Any communication claiming otherwise is **fraudulent**.

Website & Email Security Guidelines

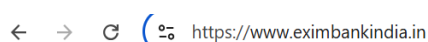
1. Always Manually Enter the Official URL

Access the bank's website by **typing** <https://www.eximbankindia.in> **directly into your browser**. Do not trust links from emails, text messages, or third-party websites. Fraudulent websites often contain typos or added words designed to deceive users.

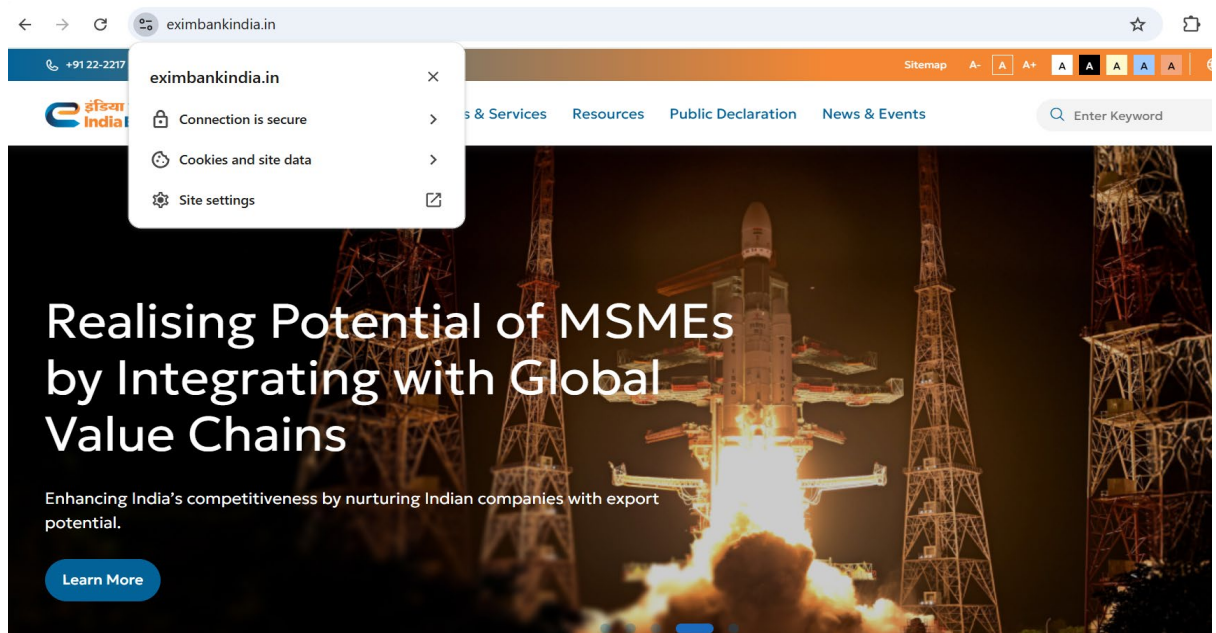
2. Look for HTTPS & Padlock Symbol

Ensure the website URL begins with **https://** and displays a **padlock icon** in the browser's address bar. This confirms a secure and encrypted connection.

https://

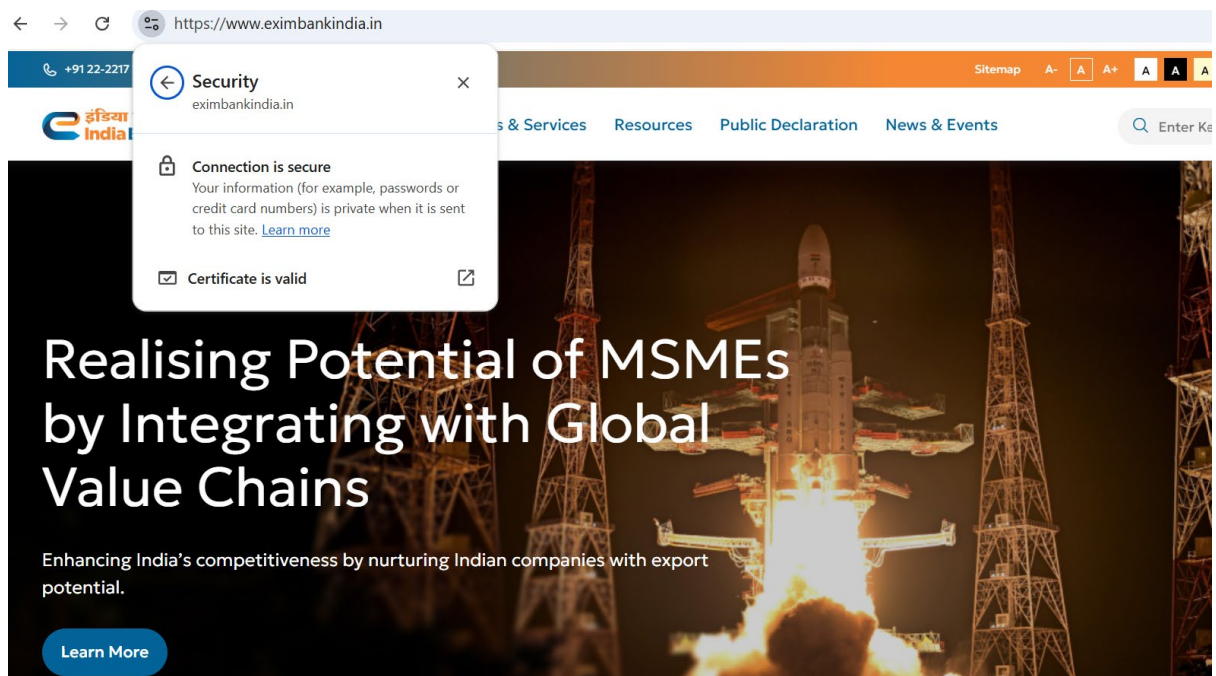


Padlock (connection Secure)



3. Verify the Digital Certificate

Click the padlock icon → View.Certificate → ensure it is **issued to www.eximbankindia.in** and **signed by DigiCert**. This confirms you are connected to the genuine website.



4. Check Email Domain Authenticity

All official communications from Exim Bank originate from **@eximbankindia.in**. Be cautious of emails from lookalike domains or free email services.

5. Stay Within the Secure Website

After accessing the website, ensure that **all internal navigation continues under <https://www.eximbankindia.in>**. Unexpected redirects may indicate a compromised session.

6. Review the Privacy Policy

Before submitting any information via the website, review our official **Privacy Policy** to understand how your data is collected and protected.

7. Use Updated Web Browsers

Access the website only through **latest versions** of supported browsers such as Microsoft Edge, Google Chrome, Mozilla Firefox, Safari, or Opera. Outdated browsers may be vulnerable to security threats.

8. Protect Your Devices from Malware

Keep your systems and devices protected with **updated antivirus and anti-malware software**. Regularly scan for potential threats like Trojans, spyware, or ransomware.

9. No Auto-Downloads or Pop-ups

Exim Bank's official website **will never initiate automatic downloads** or prompt pop-ups requesting sensitive personal information. Avoid downloading files unless explicitly verified.

10. Report Fraudulent Websites or Messages

If you come across any **fraudulent websites or suspicious communications** claiming to represent Exim Bank, report them to: iso@eximbankindia.in

11. Avoid Public Wi-Fi for Sensitive Browsing

Do not access or attempt to engage with bank-related websites over public Wi-Fi. Use secure and private internet connections.

12. Avoid Saving Passwords on Shared or Public Devices

Never save your login credentials on shared or public computers. Always log out after your session to prevent unauthorized access.

13. Clear Browser Cache and Cookies Regularly

Regularly clear your browser's cache and cookies to remove any stored sensitive data and minimize the risk of session hijacking or data leakage.

14. Be Cautious of Browser Extensions

Only install trusted browser extensions or add-ons, as malicious extensions can compromise your security by intercepting data or injecting harmful scripts on websites.

15. Verify Website Content for Authenticity

Be alert to unusual website content such as poor grammar, low-quality images, or inconsistent branding. These may indicate a fake or compromised website.

16. Stay Informed on Cybersecurity Trends

Educate yourself on common cyber fraud tactics such as phishing, spoofing, and social engineering. Stay vigilant and verify before acting on unsolicited messages or calls.

17. Report Suspicious Activity Immediately

If you receive suspicious communication or identify a fake website impersonating the Bank, report it without delay to:

Information Security Group – iso@eximbankindia.in