Phishing Attacks And How To Avoid Them

Phishing is a form of cyber attack in which scammers/attackers make Internet users divulge with sensitive information about their bank accounts and personal details. E-mail can be used to obtain sensitive information from unsuspecting users. The information may be passwords for websites, credit card information, and online financial information such as bank account numbers. The attackers are able to target Internet users due to some inherent weakness in web browsers and other technical aspects of the Internet. All the internet users are requested to adopt/practice the following guidelines to avoid such attacks, as prevention is always better than cure.

- Be suspicious of any email with urgent requests for personal financial information and do not react to such suspicious e-mails.

- The credentials of the sender should be verified before making any transaction on the received e-mail message. Please contact the Bank to verify the genuineness of the e-mail.

- Don't use the links/hyper links in an email to get to any web page, if you suspect the message might not be authentic.

- Avoid filling out forms in suspicious email messages that ask for personal financial information. Personal information like passwords, PIN, credit/debit card numbers not to be provided to any entity in response to e-mail request.

- Always ensure that you're using a secure website when submitting credit card or other sensitive information via your Web browser.
  a) To make sure you're on a secure Web server, check the beginning of the Web address in your browsers address bar - it should be "https://" rather than just "http://".
  b) Whenever a user connects to a secure website (https), the web browser alerts the user. In normal practice users ignore this warning message and do not verify the server certificates while making online transaction with the financial institution. The users should verify credentials of such web-sites before making any financial transaction.
  c) Please look for the correct URL address of the Bank and also the SSL lock symbol at the bottom of the browser. By double clicking at the lock symbol, you can view the certificate that verifies this web site's identity. This is to ensure that the lock symbol is not a hard coded image and it represents the genuine site.

- Regularly check your bank, credit and debit card statements to ensure that all transactions are legitimate.

- Ensure that your browser is up to date and security patches applied and use latest versions of browsers to connect to Internet as they could provide higher levels of security.

- If you happen to receive any such suspicious e-mails, please report the same immediately to this e-mail id: **(complaints@kccb.in)** .