

Beware of Suspicious Emails / SMS

Security Advisory

You may be receiving many Emails / SMS / WhatsApp messages claiming to be from Bank, advising to click on links provided in the mail / message to update / activate banking services. But be cautious. They may be malicious links which can infect your device with malware or steal sensitive information like account number, Internet Banking user id, passwords etc.

Sample Mail

From: UCO Bank Team [xyz@abcmail.com]

Dear Customer,

Your Internet Banking password has not been updated since last 90 days. Kindly update your Internet Banking password at <http://ucodigitalbanking.com> to continue the service.

Regards
UCO Bank Team

Do not fall prey to these tricks.

Best Practices:

- Do not click on links received through emails / SMS from unknown senders. Always check sender email address apart from display name to ensure genuineness of email.
- Always login to your Internet Banking Account by directly typing the URL in the browser.
- Always remember, UCO Bank will never ask for OTP, Internet Banking password, Mobile Banking PIN, debit card details, OTP, CVV and other confidential information over email / SMS or phone calls.
- Do not install unknown apps, if someone tells over phone to do so.

Protect One | Protect All | Protect India

Chief Information Security Officer
CISO Office, UCO Bank