

Findoc Finvest Private Limited Customer Awareness Module

Phishing

- Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details, by disguising as a trustworthy entity in an electronic communication.
- Phishing is typically carried out by email spoofing, and it often directs users to enter personal information at a fake website, the look and feel of which are identical to the legitimate one.

Preventive Measures

1. **NEVER** click on links provided within such emails.
2. **ALWAYS** type the website/URL of your bank in the browser by yourself.
3. **ALWAYS** check if the website prefix is https and not http. Legitimate website will have the https prefix.
4. **NEVER** enter your personal confidential information on any website that wants you to enter them for some random confirmation or verification.
5. **ALWAYS** update your anti-virus signatures and definitions to ensure that malware and spyware will be caught & taken care of by the anti-virus software before they do any actual damage.

Note: FFPL doesn't explicitly ask for Credit/Debit card details from their customers.

Report Fraud: Should you receive any such calls/messages requesting your personal financial information, hang up the phone and contact FFPL immediately at grievancenbfc@myfindoc.com.