Re: Securing your systems – cyber-attacks and fraudulent financial transactions during COVID-19

Dear Colleagues,

The scale and intensity of cyber-attacks and fraudulent financial transactions are growing fast in the current crisis. With exponential growth of online activity, criminals are finding more ingenious ways to intercept vital information and divert financial transactions.

Even a minor deviation from the standard due-diligence in the payment/disbursement processes could unintentionally lead to a significant financial loss.

Following the Global Fund's guidance note on information sharing and data management issued last April, PRs have been requested to implement the necessary updates to their internal processes and confirm when this has been actioned.

As a reminder of good practice for PRs, SRs and CCM Funding recipients, should adhere to the following best practices:

- Adopt the "**Never trust, always verify**" attitude on all financial transactions. The most dangerous requests are often those that appear to come from an address or phone number that we know well. In some cases, hackers are using genuine accounts, but diverting information. Any unsolicited requests that involve a financial transaction should be handled with extreme caution.
- Ensure your **antivirus** is updated with the latest version.
- Consult with your banks for updates on making your **online payment software** more secure.
- Request **additional due-diligence if the bank account** of a supplier or recipient differs from the supplier's location or there is a change in the country where the bank account is hosted. You can request a duly signed letter from the supplier or recipient to confirm the authenticity of the bank account.
- Request additional confirmation by having a phone call.
- Create additional back-end verifications for payments being done to new bank accounts.
- Work with your IT departments to have refresher trainings for staff to improve awareness of these issues. In particular, train CCM leadership, CCM Secretariat staff and PR staff on "phishing" email.