Tips for NGOs to reduce the potential of fraud and scamming

Help protect your organization, your beneficiaries and your donors.

- Favor e-payment solutions
  Use PayPal or credit card payments through reliable providers and ensure that donors can easily find the details of such solutions and their policies.

- Train your staff
  Protect your funding by raising awareness of your staff on CEO fraud attacks and ensure staff know how and to whom to report suspicious activity.

- Register your NGO
  Donors will check if you are a legitimate organization on charity registration sites.

- Inform donors about scams
  Communicate about the risk of scammers and fraud using your NGO identity as bait and remind donors how to donate securely to your NGO.

- Protect critical data
  Implement basic cyber hygiene to protect your donors, beneficiaries, staff and operational data, as cybercriminals seek to steal data and sell it.

- Avoid publishing your IBAN
  The number can be altered if your website is not well protected.

- Watch out for fake fees
  Never pay money to receive a donation or grant as this is most likely a scam.

- Beware of phishing emails
  Don’t click on links in unsolicited emails or social media messages mentioning donations as they can contain malware. Delete and do not share unsolicited emails or messages with others.

- Avoid gift cards and cryptocurrencies
  These can be difficult to manage, easy to steal and are often used by scammers.

- Minimize data collection
  Do not ask donors for data you don’t need such as Social Security number, date of birth or bank account number.

CyberPeace Builders is a network of volunteers providing free cybersecurity assistance to Humanitarian Non-Governmental Organizations. If you need our help, email us at assistance@cyberpeaceinstitute.org

The CyberPeace Institute is a neutral and independent NGO whose mission is to reduce the harms from cyberattacks on people’s lives worldwide. More on cyberpeaceinstitute.org