EMAIL DO AND DON'TS

DO

1. Use strong passwords on all your emails accounts, strong passwords contains at least eight characters long,contains the mixture of numbers,lowercase letters,uppercase letters, punctuation and symbols.

2. Turn on the junk mail filtering system that is offered by your email client. This will send spam into a separate folder you can check through and then empty. When a junk message slips through to your in box, always mark it as Spam to try and prevent it happening again.

3. Regularly change your password for accessing you email accounts.

4. Use long and complicated emails address to make your email address difficult to guess by Spamers as possible.

5. Install firewall, anti-Spam and anti-virus software and keep them up to date to protect yourself against hackers who can get access to your computer as use it as Spam source.

DON'TS

1. Don't post your email address on a social network site, chat room or web page. Criminals use software to trawl these sites and identify email addresses, which they then harvest and turn into lists they sell on.

2. Don't reply to Spam emails and ask to be removed. All this does is let the people sending it know your address is live and active. This will only lead you to get more Spam and junk in your in-box.

3. Don't use simple words or phrases as your email password. It means your account could easily be hacked by automated systems that try millions of different combinations of letters. Mix up your passwords and use numbers and special characters too. This will make them hard to identify.

4. Don't pass on junk mail. What might seem a harmless joke, poem, chain letter or funny story will simply clog up the Internet and in-boxes. Receiving so many of these types of messages are what cause people to be caught off-guard when a more sinister Spam email arrives.

5. Don't trust any email asking you for your password. This is known as Phishing and should never ever be replied to. Report it to the bank or organization it claims to be from so they can alert other users and customers.

6. Don't believe everything you read. Spam emails will often have a false subject line to try and trick you into opening the message. It may be a tempting offer, or the promise of something for nothing, but there will always be a catch. That could leave you open to all sorts of problems.

7. Don't open email attachments containing the following file extensions: **.exe, .bat, .reg, .scr, .dll, or .pif. Or** with two file extensions for instance**: resume.doc.pif or Love-letter-for-you.txt.vbs**.

8. Don't open attachments with emails from unfamiliar sources,with attachment that has no text messaging explaining what attachment is about.

9. Don't use the following because your email will be seen as spam,

    a. Words like free, guaranteed, credit card, sex etc

    b. Use red color in your texts

    c. Use all capital letters especially in subjects and body

    d. Using excessive punctuations such as !!!!!!??????

    e. Excessive use of CLICK HERE especially in capitals

    f. Excessive use of $$$$ and other symbols

    g. Sending image/graphic only emails

Prepared by NOC
Habari Node Ltd
Internet Provider with a Difference.
Www.habari.co.tz