How to prevent your IITR id from becoming a vehicle for generating spams

Rule of Thumb

- Avoid clicking on a link in an e-mail message unless it is from a trusted source.

- Do not reply to e-mails soliciting personal information

WARNING SIGN #1

Soliciting Personal Information by E-Mail

Financial institutions and reputed online retailers do not send e-mails asking for any personal information. Any e-mail that claims to be from a credible source, but asks for such data is most likely a Phishing expedition.

WARNING SIGN #2

Badly Written E-Mail

Read the message closely. A professional company such as e-Bay or Amazon will not issue any communication containing basic grammatical and spelling errors. A high proportion of phishing e-mails contain such fundamental errors.

WARNING SIGN #3

Hidden Addresses & Sources

Phishing attacks redirect you somewhere other than where they claim to be going. Check to see if the link in the e-mail is legitimate by resting or hovering over the link. It should be the same web address as the displayed link and be the web address of the company allegedly sending the e-mail.

WARNING SIGN #4

Threatening Legal Sounding Messages

From a customer service perspective, no reputable company would send their customers a threatening e-mail. If you receive a threatening e-mail, it almost certainly isn't legitimate. If you think it may be, telephone or send a new e-mail to the legitimate company. Under no circumstances should you respond directly with a return e-mail to the message you just received.

At the least

TWO essential password rules to consider when creating a password

1. **Length**
2. **Complexity**

- **Your password length should be at least 8 characters long**
- **Your password should use a combination of lower case letters, upper case letters, numbers, and special characters.**

Thank You !

for further support email to
email-support@iitr.ac.in