**Social Engineering (via Mail)** 

Social engineering is the art of manipulating people so they give up their confidential information. The types of information these criminals are seeking can vary, but when individuals are targeted the criminals are usually trying to trick you into giving them your passwords or bank information, or access your computer to secretly install malicious software–that will give them access to your passwords and bank information as well as giving them control over your computer. One of the ways Social Engineering can affect you is through mails.

**Email from a friend -** If a criminal manages to hack or gain access to one person’s email password they have access to that person’s contact list and because most people use one password everywhere, they probably have access to that person’s social networking contacts as well. **Once the criminal has that email account under their control, they send emails to all the person’s contacts or leave messages on all their friend’s social pages, and possibly on the pages of the person’s friend’s friends as well.**

* **These messages may use your trust and curiosity:**
* **Contain a link that you just have to click** because the link comes from a friend and you’re curious, you’ll trust the link and click. This may be infected with malware so the criminal can take over your machine and collect your contacts info and deceive/cheat them just like you were.
* **Contain an attachment to download–pictures, music, movie, document, etc.,** that has malicious software in it which is unknown to you. If you download which you are likely to do since you think it is from your friend you become infected. Now, the criminal has access to your machine, email account, social network accounts and contacts.
* **These messages may create a convincing story :**
* **Urgently ask for your help** – your ’friend’ is stuck in country X, has been robbed, beaten, and is in the hospital. They need you to send money so they can get home and they tell you how to send the money to the criminal.
* **Asks you to donate to their charity, or some other cause** – with instructions on how to send the money to the criminal.

**Don’t become a victim!!!**

We can adopt the following methodologies for saving us from falling a prey to these predators.

* **Slow down**. Spammers want you to act first and think later. If the message conveys a sense of urgency, never let it affect you.
* **Research the facts**. If the email looks like it is from a company you use, do your own research. Use a search engine like google, yahoo etc. to go to the real company’s site, or a phone directory to find their phone number and verify the details.
* **Delete any request for financial information or passwords.**If you get asked to reply to a message with personal information, it’s a fraud.
* **Reject requests for help or offers of help**. Legal companies and organizations do not contact you to provide help.
* **Curiosity leads to careless clicking**. If you don’t know what the email is about, clicking links is a poor choice. Similarly, never use phone numbers from the email; it is easy for them to trick you.
* **Beware of any download.**If you don’t know the sender personally and they ask you to download a file they have sent, downloading anything is a mistake.
* **Set your spam filters to high.** Every email program has spam filters. To find yours, look under your settings options, and set these high–just remember to check your spam folder periodically.
* **Secure your computing devices.** Install [anti-virus](https://www.webroot.com/in/en/home/products/av) software, firewalls, email filters and keep these up-to-date. Set your operating system and smartphone to automatically update.

**Though we can’t 100% get rid of cyber-crimes as cyber criminals are always at the look-out for a loop hole to attack us in this digital world, we can always take the necessary precautions so that if not completely get rid of the damage from being caused, we can still reduce the impact drastically.**