Social engineering exmples:

A recent phishing campaign used LinkedIn branding to trick job hunters into thinking that people at well-known companies like American Express and CVS Carepoint had sent them a message or looked them up using the social network, wrote [ThreatPost](https://threatpost.com/massive-linkedin-phishing-bot-attacks-hungry-job-seekers/178476/" \t "_blank). If they clicked on the email links, recipients found themselves redirected to pages designed to steal their LinkedIn credentials.

pretexting relies on building a false sense of trust with the victim. This requires building a credible story that leaves little room for doubt in the mind of their target. It also involves choosing a suitable disguise. For example, an attacker might say they’re an external IT services auditor so that the organization’s physical security team will let them into the building.

The first sampple is about phishing happened in myself a few days ago. I am selling some stuff throught tori.fi. One guy showed his interest on a jacket and first cut the price down a little bit and then confirmed to buy and he said he will use a safe payment through posti. Soon I received a link and I opened it and request me to input the numbers of credit card. I showed a little dout because I think for receiving a payment more look like input the bank number. So, I just rejected the payment and after that my husband told me that’s a scam. I was in tori.fi sometimes buy sometimes sell for many years, some small order like a few euro, some bigger ones like a few hundreds euro. Before that, I didn’t face any question with any order. People are so trustful and reliable about the payment and delivery. But whatever, still some scam could happen on line.

So in the daily live either in the school or working we could carefully live safe in the complicated world.

Do not open any emails from untrusted sources. Contact a friend or family member in person or by phone if you receive a suspicious email message from them.

Do not give offers from strangers the benefit of the doubt. If they seem too good to be true, they probably are.

Lock your laptop whenever you are away from your workstation.

Purchase anti-virus software. No AV solution has a 100% detection rate, but they can help to defend against campaigns that use social engineering tactics.

Read your company’s privacy policy to understand under what circumstances you can or should let a stranger into the building.