# Social Engineering - Trust but Verify

**Author :** Cat

**Date :** January 20, 2019

What’s the easiest way steal something that is kept securely behind a lock? Get ahold of the key. Or even better, just have someone let you in. Sounds preposterous but this is the number one way tech criminals get access to personal identities and private company information; the users are tricked into handing it over.

Social Engineering is the *science* of manipulating someone to get what you want. By using our natural tendency to trust along with gathering extra information, a criminal can bypass both physical security (locked doors) and technical security (passwords, firewalls, internal servers) mainly with information shared freely on the internet. It is a psychological means to a technical end.

This is why the mentality of “I have nothing to hide” online is flawed. Here are five examples of techniques social engineers can use to fool you into giving away info.

## Using Personal Knowledge Against a Target

Social networks and forums online are full of information a criminal can use to learn about someone's interests. One great example from expert Social Engineer Christopher Hadnagy starts with a targeted attack at a user, often called spear phishing. The hacker in question found the user's work email listed on forum for rare stamps. He then set up a fake website hosting images of rare stamps that he claimed he own. The hacker reached out to the target via his work email and asked him if he was interested in seeing his stamps for sale. He provided the link. The target *clicked the malicious link from within his company firewall*, and that's all it took to gain access to the internal servers of the company. The target would not have even known it had happened.

## Using Personal Knowledge About a Contact to Gain Trust

The simpler and more effective method to gain trust is by using information on a secondary subject. Especially if a request is coming from someone higher up at a company or an authority figure. One example would be gather anything from a planned vacation or business trip. This again can be done via social network posts, destination forums, conference attendee lists, or airport WiFi connections. The criminal then contacts an assistant or subordinate to the target and says that they "know" that the target is on a flight right now but they really need them to take this immediate action on behalf of the target. After including several more personal details on the target (kids names, location they are travelling to etc), they gain the trust of the person they have called *to do whatever they have asked*. Millions of dollars were lost last year from people transferring money from this scam.

## USB Key Drops

The thing about USB keys is that you can't tell what is on them until after you've plugged them in. Which is why is it so effective to drop a key in a public lobby or by the bathrooms inside a company office. There are numerous programs online that will allow you to create secret malware that you can place on that key. Add a few random vacation photos and you've got an unsuspecting way to get *access to a person's computer just by having someone plug it in*, again without the user having any idea they've done it.

### Spoofing

These are emails that appear to be from someone but they are not. It is actually very easy to change the *reply to* address or display name on a message. We are all so busy that we rarely check the actual email addresses. Using public sources, like the contact page on a company site or linkedIn. Hackers can easily spoof an internal address. For personal address books, people frequently give downloaded apps ‘access to their contact lists’ *which gives hackers a list of known contacts* to which they can spoof emails, typically requesting money for an emergency.

### Phishing

This is an email or text that takes you to screen that *looks* like a login to something to use. When you *enter your credentials (email and password), the hacker takes them* and then reroutes you to the actual site so you do not know you have been compromised.

## How to Avoid Getting Taken In

As you have read, the human link is the weakest link to your personal and professional cyber security networks. The most critical step to take is to train yourself and your employees to be in the lookout for all of these events.

Here are some further actions you can take right now:

- Use Privacy Settings on all social networks

- Be wary what public information is available and where you are sharing contact information (Google yourself and your email address)
- Have a personal and corporate policy not to plug in unverified USB keys
- Double check return addresses before clicking on or downloading anything suspicious
- Remember that no reputable service will have you login in from an email

For a better better understanding of the types of scams criminal use, check out our complete Glossary of Internet Fraud and Scam Terminology.

## Trust, but verify.