

Four

Tips to Identify Social Engineering Attempts Through Emails



GlobalCISOForum.com



One

Emails that contain links

Social engineers are confident in the power of friendship and the trust that comes with it. If they send a link to a victim's friend urging them to click, curiosity and trust will play a role in getting the new target to click the link.

The link could send one to a malicious website that installs malware on one's device. This malware could steal the stored login credentials in browsers or start logging the keys pressed on that machine for the purpose of collecting login credentials. The stolen information can be used to attack other friends in the same way.



Two

Emails that contain downloadable content

The possibility of a target downloading email attachments and opening them improves dramatically if they believe that they were sent by a trustworthy person.

PDFs named with enticing names will be downloaded and opened by oblivious users who believe that their friends can mean them no harm. Other file types can be used.

Zipped movies, documents, and audio files can still do the trick. When the target opens these files, malware is loaded onto their machine. In previous chapters, there was a discussion on some Metasploit exploits that have the capability to generate malicious files that are ready to be sent through email



Three

Emails requesting for urgent help

Urgency is a common indicator of social engineering. Social engineers never want to give a target enough time to process new information if this could expose their attack.

Therefore, whenever possible, urgency will be used. When engineers have control of an email address, they can easily use it to extort money from email users that have been in contact with the victim before.

They could request for money to be sent to a certain account immediately so that a bill can be paid, or some fines can be paid so that a friend is discharged or freed. It is only after the money has been sent that the hoax is unearthed.



Four

Emails requesting for donations

Sympathy is a weakness present and exploitable in most humans. Social engineers are experts at creating pretexts that evoke sympathy from people causing them to offer assistance without thinking twice.

Therefore, messages compelling one to donate to unknown charitable foundations or from unknown people asking for money to support some other charitable causes might turn out to be social engineering attempts.

Therefore, any donation requests, especially if they are urgent, must be treated with caution.



Don't forget to
follow our page
Global CISO Forum

Dr. Erdal Ozkayao

