

Summary Report for Lab Draft Robert Gabriel

Introduction

The effect of Facebook and social engineering is a growing area for hacking and gaining personal information of that for victims.

What the report says is the effect sharing information online can have side effects.

With the Facebook effect, people are adding, and sharing more information online not knowing about the dark side of doing this. The younger generation is sharing more and more online, adding people they don't know and taking these online quizzes that seem to be friendly (more on this later).

Quizes

People sharing photos, statuses about family, pets, movies and music they like. All these can tell us a lot about a person and you can build an idea of a person like their favorite color, where they live, who their friends are and much more

Looking at the overview of everything a person online, there is one area that it all leads back to. That's the email and with most email accounts there is a password restart feature. Where you have to answer a personal question. This question can be anything from favorite color, first name of mother and much more. How would a "hacker" gain this information? Well from the research paper, it's all about getting the information the user gives away on those Facebook quizzes. The user answers, information that seems friendly and safe, but in the background they build a profile of the user, who they are, what's their favorite movie and more.

With the use of APIs of Facebook, the Quiz/app developer (hacker) can ask for permission to the Facebook user's personal information (email, name, address, friends, location and more).

Most users will not read what permissions the app asks for, so in short by answering short questions about who are you most like from a character. Will paint a picture of who you are as a person and this can open a can of worms. Where with this information the hacker can now answer the password restart email question. Giving them access to everything you have online, bank, social media, personal accounts and more into the great theft of gain and identity theft

Attack Types

What the report is summarised that as you post information openly online by using the “harmless at first glance” cases it gives cracker and hacker more information about you to help gain access to your accounts for financial gain. This can be used in the attacks below

The different types of social engineering are

- In-Person Attack or Scam (Face to face attacks)
- Impersonation & Identity Theft (Pe tending to be them)
- Spear Phishing (sending personal emails , trying to trick them to download software by saying stuff they like and know)

Finish

To finish on this quote from the report

“Social engineering is like putting together a puzzle. As the social engineer gathers the little bits and pieces of seemingly unimportant information, a much larger picture starts to emerge.”