

1. Introduction

This paper will discuss

- Phishing attacks
 - what they are
 - Why they are effective
 - Human factors
 - many different factors, in this paper three will be discussed:
 - lack of knowledge and Memory failure
 - Faulty Reasoning or Judgment
 - Casual Values and Attitudes About Compliance
 - Chosen for individual risk and chaining abilities, which increases risk.
 - Possible use cases combining phishing techniques with human factors
 - Outcomes if attackers are successful

2. Phishing

- can be through
 - websites
 - emails
 - voice calls
 - in-person
 - insider or outsider
- utilized for
 - sensitive data extraction
 - codes, routing numbers, documents, etc.
 - stealing credentials
 - employee credentials
 - banking credentials
 - third party credentials
 - elevated of privilege
 - access to sensitive information
 - access to administrative employees
 - access to services and networks
- Can be single- or multi-stage attack
 - see Figure 1/Table 1 & Figure 2/Table 2
 - figure 1: workflow pattern – single stage
 - Table 1 – corresponding definitions
 - figure 2: workflow pattern – multi-stage
 - Table 2 – corresponding definitions

Phishing attacks would be not be successful if human factors did not present opportunities for manipulation.

3. Human Factors

- factors which play into social engineering/phishing

3.1 Lack of Knowledge and Memory Failure

- common characteristics
- weaknesses

- dangers

3.2 Faulty Reasoning and Judgment

- common characteristics
- weaknesses
- dangers

3.3 Casual Values and Attitudes about Compliance

- common characteristics
- weaknesses
- dangers

4. Attack Cases

Attack classes:

- Attack participant
- Attack Media
- Attack Artifacts

4.1 Sensitive Data

attack case: memorizing bank transfer codes left on a sticky note (class diagram, interaction view)

4.2 Stealing Credentials

attack case: a bogus email asking for bank login credentials (class diagram, interaction view)

4.3 elevation of privilege

attack case: e.g. MiTM website inserts malware onto target system, is able to phish admin accounts (class diagram,)interaction view

5. Attack Outcomes

- infrastructure damage
- personnel damage
- monetary damage
- reputation damage

6. Conclusion

(Will wrap the whole thing up)