The Art of Hacking Humans: Intro to Social Engineering

Dumpster Diving

Dumpster diving involves malicious attackers checking through garbage for sensitive data or information that was not properly discarded. Sensitive data can also easily fall into the hands of malicious attackers if they are left laying around carelessly, like invoices, receipts and storage media containing confidential data left carelessly about the place, employee data left in the same way, passwords on sticky note stuck on systems and devices that require such passwords to operate, and things like that.

Steve Hunt, a security industry analyst, decided to go through the garbage of a major bank and in within three minutes, he was able to find sensitive documents, and even a laptop (Goodchild, 2009). The documents included a copy of a cheque, documents showing financial transactions, and sensitive personally identifiable information of customers which in the hands of a malicious individual can constitute a major tragedy.

Dumpster diving takes advantage of victims' misplaced sense of security and negligence. There is usually a feeling that nobody will go through what has been discarded; hence effort not made to try obliterating what is contained in it.

To guard against dumpster diving, effort has to be made to ensure that documents, devices, instruments and anything containing data that is to be discarded are properly disposed off such that any sensitive data contained therein is irretrievable. Employees should be compelled to properly dispose any sensitive material or item that contains sensitive material, and they should be made to understand and appreciate why. They should also be made to understand that documents and systems should not be left about carelessly increasing risk of them getting compromised. Paper documents should be discarded by shredding both vertically and horizontally or completely burning to ashes as opposed to just dropping in bin, crumpling, or shredding in only one direction. Electronic media should be thoroughly destroyed physically such that recovery becomes impossible. Disk may be wiped and then formatted several times over to avoid possibility of data recovery from such disks or they may be demagnetized.

References:

Goodchild, J. (2013) *A Real Dumpster Dive: Banks Tosses Personal Data, Checks, Laptops* [Online]. Available from: https://www.csoonline.com/article/2123810/identity-theft-prevention/a-real-dumpster-dive--bank-tosses-personal-data--checks--laptops.html (Accessed: 29 October, 2017).