TOP 6 RISKIEST EMPLOYEE PRACTICES THAT THREATEN A COMPANYS DATA SECURITY

According to The Human Factor in Data Protection" study, the most common causes of data loss is loss of laptops or other mobile devices, third party mishaps or flubs and system glitches. Only 8% of incidents were the result of outside actors.

Here are the most common examples of risky practices routinely adopted by employees:

1 Putting Company Data at Risk over Free Public Wi-Fi

60.9 % admit they will utilize any free Wi-Fi source they can find.

83% of respondents reported using their mobile device on public transportation.

95.6%

2 Not securing confidential information

37% store sensitive data on their laptops, smartphones, tablets and other mobile devices.

60% of employees steal company information when they leave or are fired.

3 Sharing passwords with others

52% of employees see no security risk in sharing passwords and logins.

54% fail to recognize the risk of sharing login details.

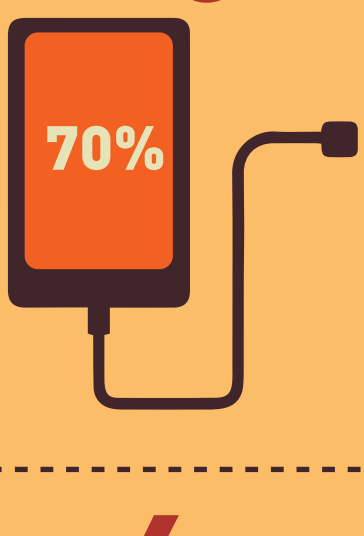
32% of those who have shared their password saying it was because their manager or boss asked.

4 Using the same name and password for different websites or online accounts

55% of users use the same password across more than one of their online accounts.

26% said that tend to use easy-to-remember passwords such as birthdays or their names.

5 Using generic USB to store confidential information



70% More than 70% of respondents say that they are absolutely certain that data breach was caused by sensitive or confidential information contained on a missing USB drive.

6 Leaving computer unattended while away from workplace

57% of workers dont have a laptop security device.

25% have left their laptop unsecured overnight.

52% dont lock their computer when theyre away from their desk.