

* Sonu Jehra

* Bsc IT (58)

* 1022768 (58)

Problem Statement 3 :- Describe password management using free online tools.

Objective :- To understand the concept of creating strong passwords and how to manage password using different criteria.

Activity :- Create a strong password by using practical tips.
a) Use online website "have i been pwned" for password and email id hacking purpose.

⇒ purpose of this site.

This site serves two primary purpose. firstly it observably provide a service to the public. Data breaches are rampant and many people don't appreciate the scale or frequency with which they occur. By aggregating the data here it not only help victims learn of compromises of their accounts but, also highlights the security of the risk.

Secondly, the site provide an excellent use case for putting a number of technologies through their paces and hand on skills somewhat current.

Sonu

⇒ Don't get out your password :- This is an obvious piece of advice. but on that bears revisiting, with the exception of some school services, you shouldn't even have a provider a ~~site~~ site administrator with your password for them to access your account.

⇒ change your passwords often :- In addition to keep your password a secret, you should change the password on your various accounts and devices at least once every six months.

⇒ Use two factor authentication ⇒ two factor identification requires you to enter a code send to you in a text message or another services to access your account after the enter your ~~use~~ user name.

⇒ Create complex password :- your password to access your account on app or website should consist of a combination of account on app, number, uppercase & special characters.

Saru

→ checking for few website you know that were breached also write compromised data.

① Adobe.

In Oct. 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, encrypted password and a password hint in plain text.

② Avast :- the avast anti-virus form was hacked & 423 K member record were exposed. The simple machines based form included usernames, email, and password hashes.

③ Yatra :- In Sep 2013, In Indian booking website known as Yatra had 5 million record exposed in a data breach. The data contained email and physical addresses. on th Vigilanted.jp

⇒ creating few website for checking your checking password

1) <https://password.kaspersky.com/>

2) <https://free.safety.intel/>

3) <https://password-check.online-domain-tools.com/>

1. Sonu