Common Threats and Solutions

Password Managers

Irfan Kanat

Department of Digitization
Copenhagen Business School

May 24, 2021

In this video we will learn how to use a password manager.

A Strong Password

Possibilities...

A Strong Password
Possibilities...

A Strong Password

Possibilities...

$l = abc...xyz = 26$

A Strong Password
Possibilities...
$l = abc...xyz = 26$

A Strong Password

Possibilities...

$I = abc...xyz = 26$

$III = 26 \times 26 \times 26 = 17576$

A Strong Password
Possibilities...
$I = abc...xyz = 26$
$III = 26 \times 26 \times 26 = 17576$

A Strong Password

Possibilities...

$I = abc...xyz = 26$

$III = 26 \times 26 \times 26 = 17576$

$IIII = 26 \times 26 \times 26 \times 26 = 456976$

A Strong Password
Possibilities...
$I = abc...xyz = 26$
$III = 26 \times 26 \times 26 = 17576$
$IIII = 26 \times 26 \times 26 \times 26 = 456976$

A Strong Password

Possibilities...

$I = abc...xyz = 26$

$III = 26 \times 26 \times 26 = 17576$

$IIII = 26 \times 26 \times 26 \times 26 = 456976$

$L = abc...zAB...XYZ = 52$

A Strong Password
Possibilities...
$I = abc...xyz = 26$
$III = 26 \times 26 \times 26 = 17576$
$IIII = 26 \times 26 \times 26 \times 26 = 456976$
$L = abc...zAB...XYZ = 52$

A Strong Password

Possibilities...

$I = abc...xyz = 26$

$III = 26 \times 26 \times 26 = 17576$

$IIII = 26 \times 26 \times 26 \times 26 = 456976$

$L = abc...zAB...XYZ = 52$

$LLL = 52 \times 52 \times 52 = 140608$

A Strong Password
Possibilities...
$I = abc...xyz = 26$
$III = 26 \times 26 \times 26 = 17576$
$IIII = 26 \times 26 \times 26 \times 26 = 456976$
$L = abc...zAB...XYZ = 52$
$LLL = 52 \times 52 \times 52 = 140608$

A Strong Password

Possibilities...

$l = abc...xyz = 26$

$lll = 26 \times 26 \times 26 = 17576$

$llll = 26 \times 26 \times 26 \times 26 = 456976$

$L = abc...zAB...XYZ = 52$

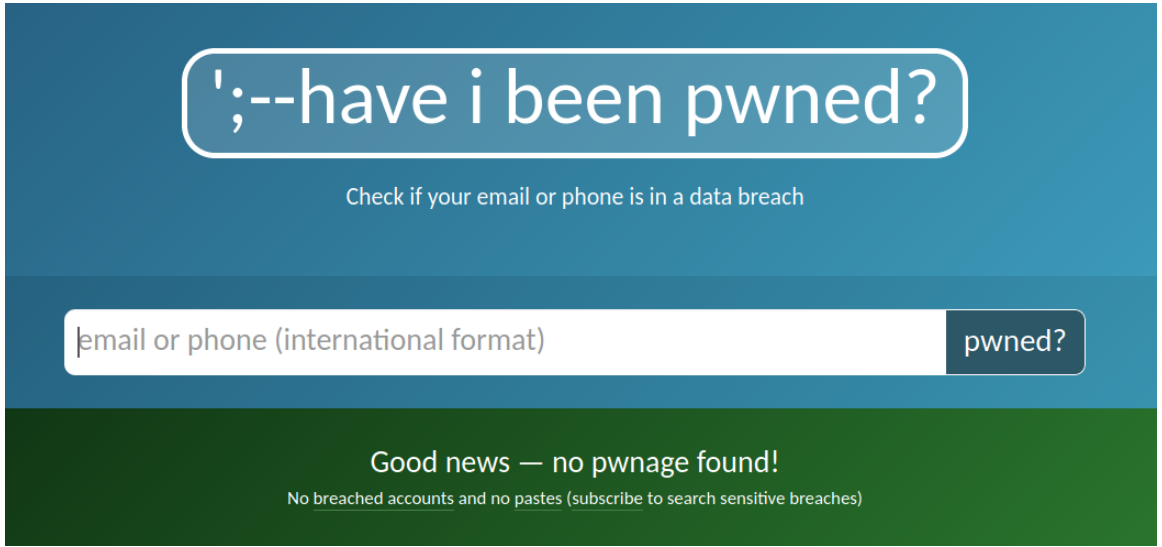
$LLL = 52 \times 52 \times 52 = 140608$

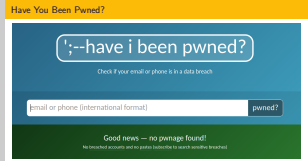
Upper, lower case characters, numbers, special symbols...

A Strong Password
Possibilities...
$l = abc...xyz = 26$
$lll = 26 \times 26 \times 26 = 17576$
$llll = 26 \times 26 \times 26 \times 26 = 456976$
$L = abc...zAB...XYZ = 52$
$LLL = 52 \times 52 \times 52 = 140608$
Upper, lower case characters, numbers, special symbols...

The strength of the password can be estimated by how many possible tries it would take to guess the password. This is what a computer trying to **bruteforce** the password.
So two ways to increase the strength of the password. Size of the character set, and digits. So longer passwords made up of different types of characters (letters, numbers, symbols) are harder than shorter passwords made up of just one type of character.
Bruteforce is not the only way to crack a password. Trying all words in a dictionary, and combinations of words has also been done in the past. This is known as a **dictionary attack**. So don't use words in your password.
You can also just guess the password by using information about the person. So don't use personal facts as password.

Have You Been Pwned?





One way adversaries may get access to your accounts is by using your known passwords on other accounts.
So if your password was revealed in a data breach, all your other accounts using the same password is also in danger.
I highly recommend you go and check your e-mail address on `haveibeenpwned.com`

Good Password

Long

Character Types

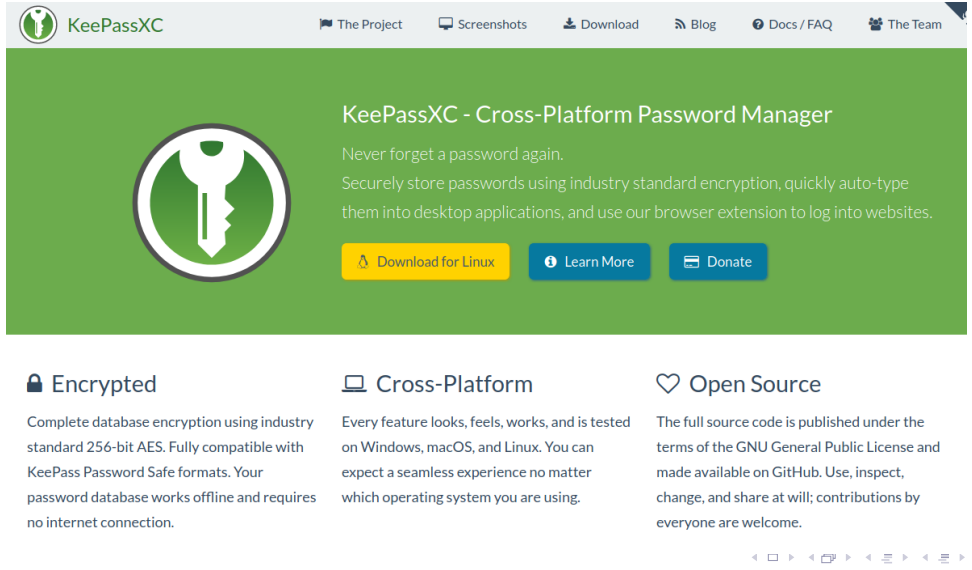
No Words

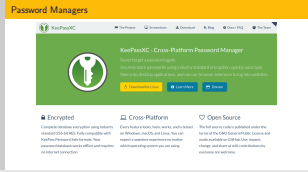
No Personal Facts

Don't Reuse

Good Password
Long
Character Types
No Words
No Personal Facts
Don't Reuse

Password Managers





A good password is not only hard to guess, it is also hard to remember for humans. So it is imperative you use a password manager.

There are various password managers out there. The most convenient ones are cloud based services like lastpass or 1password. Unfortunately these type of services run the risk of becoming paid after the fact. Last pass for example changed the terms of its free tier in 2020, putting their users in a difficult situation.

Therefore I recommend open source solutions. They are not as convenient, but it gives you more control.