STRONG PASSWORD

How to Create and Manage Strong Password

Disusun oleh: Dhyta Caturani (PurpleCode Collective)

Facebook

@Dhyta Caturani

Twitter

@purplerebel

Instagram

@purplerebel
@purplecode_id

Password yang kuat dan aman adalah prioritas utama keamanan digital.

30 PASSWORD TERBURUK 2019

- 12345
- 123456
- 123456789
- test1
- password
- 12345678
- zinch
- g_czechout
- asdf
- qwerty.
- 1234567890
- 1234567
- Aa123456.
- iloveyou
- 1234
- abc123
- 111111
- 123123
- dubsmash
- test
- princess
- qwertyuiop
- sunshine
- BvtTest123
- 11111
- ashley
- 00000
- 000000
- password1
- monkey.

CONTOH PASSWORD DAN KEKUATANNYA

Sample password	Time to crack with an everyday computer	Time to crack with a very fast computer
bananas	Less than 1 day	Less than 1 day
bananalemonade	2 days	Less than 1 day
BananaLemonade	3 months, 14 days	Less than 1 day
B4n4n4L3m0n4d3	3 centuries, 4 decades	1 month, 26 days
We Have No Bananas	19151466 centuries	3990 centuries
W3 H4v3 N0 B4n4n45	20210213722742 centuries	4210461192 centuries Passfault

ELEMEN PASSWORD YANG KUAT

Agar tak bisa diretas

01

Dibuat sulit agar tak mudah ditebak oleh program komputer

02

Dibuat sulit agar tidak bisa ditebak oleh orang lain

03

Dibuat agar meminimalisir kerugian bila berhasil ditebak

01

brush overbuilt resonate acutely tactical
swiftness lustiness unluckily

PANJANG

Password yang kuat mensyaratkan harus panjang dengan minimum 25 karakter atau 5-6 kata random (passphrase). Password/passphrase yang panjang menyulitkan orang atau program komputer untuk menebak.

01

KOMPLEKS

V\z7UnZ@ut+GS [52"u2(94et:h {x[+;c:}h$

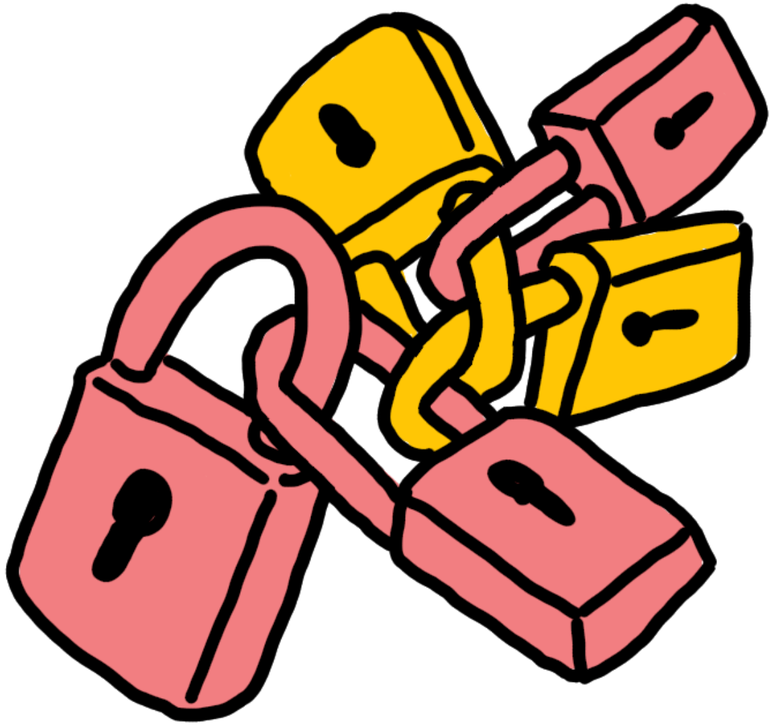
Buat password dengan menggunakan kombinasi huruf besar - huruf kecil, angka, simbol dan karakter khusus (seperti spasi).

02

JANGAN PERSONAL

Jangan gunakan informasi personal yang membuat passwordmu bisa ditebak oleh orang lain (terutama yang mengenalmu). Informasi personal termasuk namamu, nama orang terdekatmu, nama hewan peliharaan, tanggal lahir, nomor telepon, alamat, profesi, atau informasi personal lainnya.

02



RAHASIA

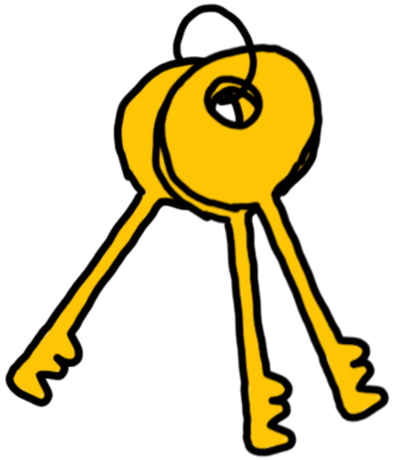
Jangan membagikan/memberitahukan passwordmu ke siapapun kecuali memang untuk keperluan mendesak!
Apabila karena satu alasan penting kamu harus membagikan passwordmu ke orang lain, segeralah mengganti passwordmu itu saat orang tersebut selesai mengakses akunmu.

02

PRAKTIS

Meskipun panjang dan kompleks, buatlah password yang praktis sehingga mudah diingat. Membuat kategorisasi, tingkat prioritas dan pola bisa membantu kita untuk mengingat. Namun otak manusia memang secara alami tidak mudah untuk mengingat, maka pelajari dan gunakan tool (app/software) Password Manager seperti KeepassXC.

03



UNIK

Jangan gunakan satu password untuk semua atau beberapa akun. Sebab bila satu password itu bisa didapatkan orang lain maka semua akunmu bisa diambil alih dan semakin banyak informasi yang bisa dicurinya darimu. Selain itu banyak ancaman keamanan dan kerugian lain apabila itu terjadi.

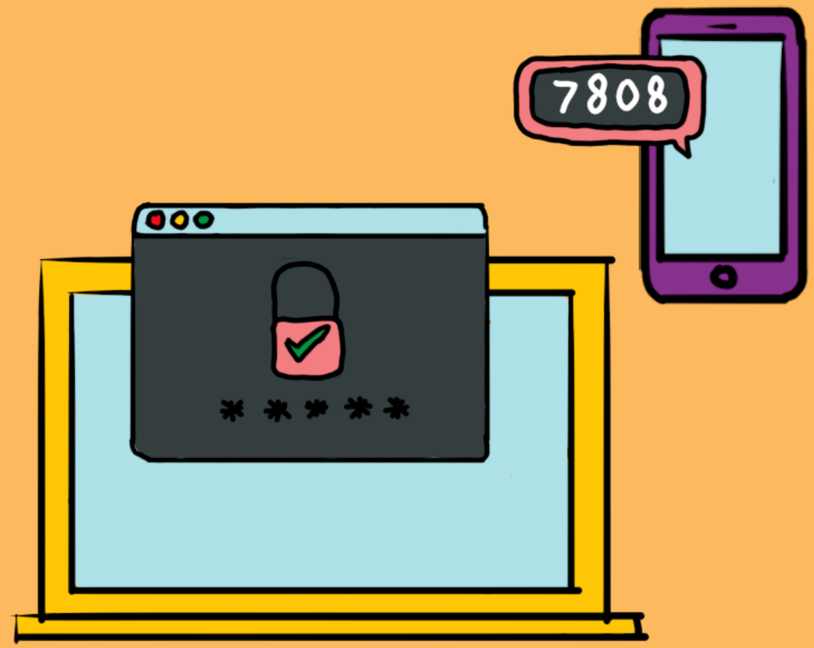
03

GANTI SECARA BERKALA

Ganti passwordmu secara berkala. Semakin lama kamu menggunakan password yang sama, semakin banyak waktu yang dimiliki orang lain untuk menebak dan mendapatkan passwordmu. Dan seandainya seseorang berhasil mendapatkan passwordmu dan dengan diam-diam ia mengakses akunmu, maka ia bisa semakin lama melakukannya.

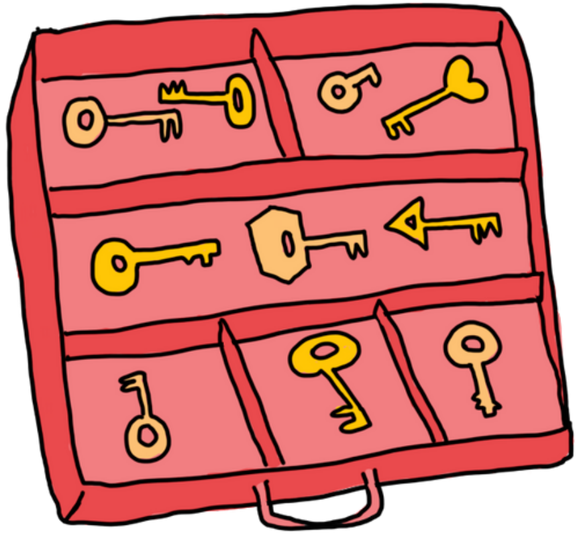
TWO FACTOR AUTHENTIFICATION

Kamu bisa menambahkan keamanan terhadap passwordmu dengan menggunakan Two Factor Aunthentification (2FA) atau Two Step Verification (2SV). Namun ingat: SMS Two Factor Authentifications is Dead! Jangan pernah menggunakan SMS sebagai moda 2FAmu karena SMS adalah sistem yang paling mudah diretas. Gunakan tools 2FA yang aman dan bisa dipercaya. Rekomendasinya adalah FreeOTP atau Authy.
Ada juga yang berupa hardware (disebut Token atau Dongle). Standar program yang digunakan biasanya Universal 2nd Factor (U2F).



PASSWORD MANAGER

Password manager bisa membantu kita untuk menyimpan, membuat dan mengelola password-password dengan aman (terenkripsi). Password Manager semakin berguna bila kamu memiliki banyak akun dengan password yang berbeda-beda.



KeePassXC

- KeePassXC adalah software Password Manager yang Open Source (bersumber terbuka) dan gratis
- Berfungsi sebagai penyimpan dan pengelola password dengan aman (terenskripsi)
- Berfungsi sebagai password generator
- Juga berfungsi untuk data keeper yang terenkripsi
- Dengan menggunakan KeepasXC kita hanya perlu mengingat 1 password saja, yakni password untuk membuka database dimana kita menyimpan semua password
- Bisa disimpan di external drive yang sebagai back up atau untuk digunakan di komputer manapun tanpa perlu untuk menginstal software dan mencopy database dalam komputer tersebut

KeePassXC

- Kelemahan KeePassXC yang merupakan konsekuensi dari keamanannya adalah mereka tidak menyimpan master key kita sehingga bila kita kehilangannya maka kita tidak bisa mengakses database password kita

- KeePassXC juga tidak menyimpan database kita, yang mana berarti jikalau kita menghapus database maka kita akan kehilangan database secara permanen

Konten disusun oleh: Dhyta Caturani

Ilustrasi oleh: Efi SH