MENINGKATKAN KESADARAN

KEAMANAN INFORMASI

Kata Pengantar

Keamanan informasi merupakan upaya untuk mengamankan aset informasi dari berbagai ancaman yang mungkin timbul. Sehingga keamanan informasi secara tidak langsung dapat menjamin kelanjutan pemerintahan. Semakin banyak informasi yang disimpan semakin besar pula resiko yang akan dihadapi seperti kehilangan data, terekspos nya data kepihak yang tidak berkepentingan.

Keamanan informasi ditujukan untuk mendapatkan kerahasiaan, ketersediaan serta integritas pada semua sumber daya informasi. Masalah keamanan merupakan salah satu aspek penting bagi sebuah sistem informasi, sayang sekali masalah ini kurang mendapatkan perhatian dari pemilik dan pengelola sistem informasi.

Buku ini dibuat dalam rangka meningkatkan keamanan informasi pada Dinas Kesehatan Kabupaten Bantul. Semoga Buku ini bisa menambah wawasan pembaca tentang Keamanan Informasi.

Bantul, 3 April 2023

Yogyakarta, 3 April 2023

Mengetahui,

dr. Agus Triwidiantara,MMR

NIP. 197008312002121003

Management Representative

DAFTAR ISI

Apa itu data ?

- Data adalah nilai yang mendeskripsikan dari suatu objek atau kejadian.
- Data adalah sesuatu yang belum mempunyai arti bagi penerimanya dan masih memerlukan adanya suatu pengolahan.
- Data merupakan bentuk jamak dari datum, berasal dari bahasa Latin yang berarti ‘‘sesuatu yang diberikan’’

Informasi ?

- Informasi adalah hasil dari pengolahan data dalam bentuk yang lebih berguna dan lebih berarti bagi penerimanya yang menggambarkan suatu kejadian-kejadian sehingga akan berguna untuk pengambilan keputusan.
- Informasi adalah sebagai data yang sudah diolah, dibentuk, atau dimanipulasi sesuai dengan keperluan tertentu.
- Informasi adalah data yang disimpan, diproses, atau ditransmisikan.
- Informasi adalah hasil pengolahan dari data yang dapat memberikan gambaran lebih jelas terhadap sesuatu.

Jenis-jenis Data

- Data teks, citra, audio, dan video.
- Data yang terformat adalah data dengan suatu format tertentu. Misalnya, data yang menyatakan tanggal atau jam, atau menyatakan nilai mata uang.
- Teks adalah sederetan huruf, angka, dan simbol-simbol khusus .
- Audio adalah data dalam bentuk suara. Instrumen musik, suara orang atau suara binatang, gemericik air, detak jantung .
- Video menyatakan data dalam bentuk sejumlah gambar yang ber•gerak dan bisa saja dilengkapi dengan suara.

Ciri-ciri Informasi (Davis, 1999):

- Benar atau salah. Dalam hal ini, informasi berhubungan dengan kebenaran terhadap kenyataan. Jika penerima informasi yang salah mempercayainya, efeknya seperti kalau inforrrasi itu benar.
- Informasi benar-benar baru bagi si penerima.
- Informasi dapat memperbarui atau memberikan peru•bahan terhadap informasi yang telah ada.
- Korektif Informasi dapat digunakan untuk melakukan koreksi terhadap informasi sebelumnya yang salah atau kurang benar.
- Informasi dapat mempertegas informasi yang telah ada sehingga keyakinan terhadap informasi semakin meningkat.

Keamanan informasi

Keamanan informasi menurut G. J. Simons adalah bagaimana usaha untuk dapat mencegah penipuan (cheating) atau bisa mendeteksi adanya penipuan pada sistem yang berbasis informasi, di mana informasinya sendiri tidak memiliki arti fisik. Aspek-aspek yang harus dipenuhi dalam suatu sistem untuk menjamin keamanan informasi adalah informasi yang diberikan akurat dan lengkap (right information), informasi dipegang oleh orang yang berwenang (right people), dapat diakses dan digunakan sesuai dengan kebutuhan (right time), dan memberikan informasi pada format yang tepat (right form).

Dalam membuat program keamanan informasi ada prinsip dasar yang harus dipenuhi agar sistem tersebut handal. Prinsip dasar tersebut adalah:

1. Kerahasiaan artinya informasi dijamin hanya tersedia bagi orang yang berwenang sehingga pihak yang tidak berhak tidak bisa mengakses informasi. Contoh kerahasiaan adalah seorang administrator tidak boleh membuka atau membaca email milik pengguna. Selain itu kerahasiaan harus menjamin data-data yang harus dilindungi penggunaan dan penyebarannya baik oleh pengguna maupun administrator, seperti nama, alamat, tempat tanggal lahir, nomor kartu kredit, penyakit yang diderita, dan sebagainya.

2. Integritas artinya informasi dijaga agar selalu akurat, untuk menjaga informasi tersebut maka informasi hanya boleh diubah dengan izin pemilik informasi. Virus trojan merupakan contoh dari informasi yang integritasnya terganggu karena virus telah mengubah informasi tanpa izin. Integritas informasi ini dapat dijaga dengan melakukan enkripsi data atau membuat tanda tangan dijital (digital signature).

3. Ketersediaan artinya adanya jaminan ketika pihak berwenang membutuhkan informasi, maka informasi dapat diakses dan digunakan. Hambatan dalam ketersediaan ini contohnya adalah adanya Denial of Service Attack (DoS). DoS merupakan serangan yang ditujukan ke server, di mana banyak sekali permintaan yang dikirimkan ke server dan biasanya permintaan tersebut palsu yang menyebabkan server tidak sanggup lagi melayani permintaan karena tidak sesuai dengan kemampuan sehingga server menjadi down bahkan error.

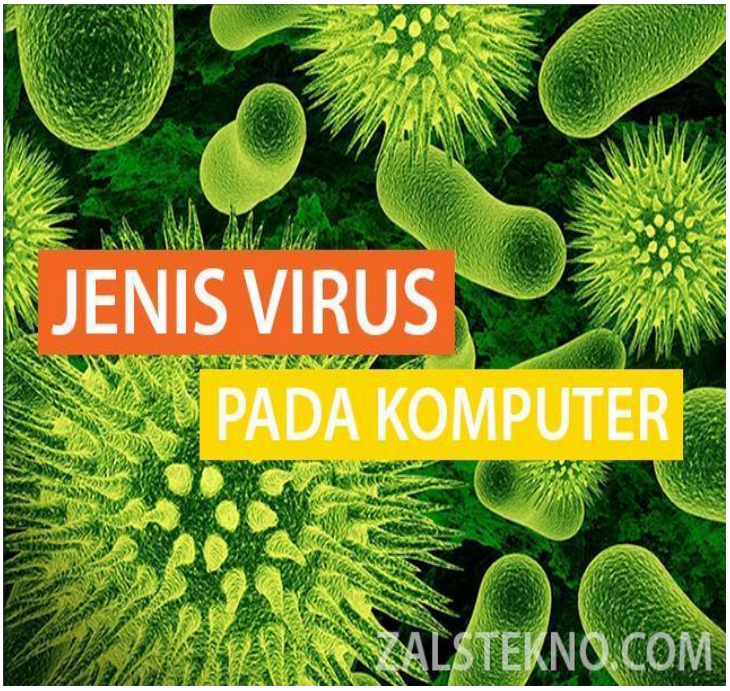
Apa yang termasuk ancaman keamanan sistem informasi ?

Ancaman keamanan sistem informasi adalah sebuah aksi yang terjadi baik dari dalam sistem maupun dari luar sistem yang dapat mengganggu keseimbangan sistem informasi.Ancaman terhadap keamanan informasi berasal dari individu, organisasi, mekanisme, atau kejadian yang memiliki potensi untuk menyebabkan kerusakan pada sumber-sumber informasi.

Ancaman dalam keamanan sistem informasi ini bukan hanya berasal dari luar perusahaan seperti lawan bisnis atau individu dan kelompok lain tapi juga dapat berasal dari dalam perusahaan.

Sebuah ancaman dalam keamanan akan dilanjutkan dengan adanya serangan, dalam kesempatan kali ini akan kami bahas mengenai serangan seranga yang dapat mengancam keamanan sistem informasi :

1. Virus



Tentunya kita sudah tidak asing lagi dengan Virus. Pada dasarnya, virus merupakan program komputer yang bersifat "malicious" (memiliki tujuan merugikan maupun bersifat mengganggu pengguna sistem) yang dapat menginfeksi satu atau lebih sistem komputer melalui berbagai cara penularan yang dipicu oleh otorasisasi atau keterlibatan "user" sebagai pengguna komputer. Kerusakan yang dapat ditimbulkan pun bermacam-macam mulai dari yang mengesalkan sampai kepada jenis kerusakan yang bersifat merugikan dalam hal finansial

2. Worms

Worms merupakan program malicious yang dirancang terutama untuk menginfeksi komputer yang berada dalam sebuah sistem jaringan. Perbedaan prinsip yang membedakan worms dengan virus adalah bahwa penyebaran worm tidak tergantung pada campur tangan manusia atau pengguna. Worms merupakan program yang dibangun dengan algoritma tertentu sehingga mampu untuk mereplikasikan dirinya sendiri pada sebuah jaringan komputer tanpa melalui bantuan maupun keterlibatan pengguna.

Karena karakteristiknya yang tidak melibatkan manusia, maka jika sudah menyebar sangat sulit untuk mengontrol atau mengendalikannya. Usaha penanganan yang salah justru akan membuat pergerakan worms menjadi semakin liar tak terkendali untuk itulah dipergunakan penanganan khusus dalam menghadapinya.

3. Trojan Horse

Istilah Trojan Horse atau Kuda Troya adalah sebuah taktik perang yang digunakan dalam penaklukan kota troy yang dikelelilinggi benteng yang kuat. Pihak penyerang membuat sebuah patung kuda raksasa yang di dalamnya memuat beberapa prajurit yang nantinya ketika sudah berada di dalam wilayah benteng akan keluar untuk melakukan peretasan dari dalam. Ide ini mengilhami sejumlah hacker dan cracker dalam membuat virus.

Malware, adalah salah satu hal yang paling ditakuti bagi mereka yang sering bekerja menggunakan komputer, laptop, notebook dan gadget lainnya. Malware bukanlah nama orang namun nama ini sangat populer di dunia teknologi dan harus kita hindari. Malware adalah suatu program yang diciptakan untuk merusak sistem komputer tanpa pemberitahuan terlebih dulu pada pemiliknya. Program ini mengistal sendiri tanpa Anda ketahui dan program ini sangat dtakuti oleh pengguna internet dan pengguna kompute. Banyak diantara mereka yang telah mengalami kerugian karena malware. Program ini bisa mencuri data kemudian mengirimkannya kepada pusat malware.

Malware bisa menyebabkan komputer bekerja terlalu berat, hal ini menimbulkan komputer menjadi lebih cepat panas dan lambat saat digunakan. Saat Anda menggunakan koneksi internet, malware bisa menyebabkan bandwidth menjadi lebih banyak digunakan dan jumlah tagihan intersnet Anda menjadi lebih besar. Malware banyak jenisnya dan salah satu jenis malware yang paling ditakuti adalah keylogger karena bisa merekan aktivitas Anda pada keyboard saat bertransaksi online menggunakan kartu kredit. Ada cukup banyak jenis malware yang harus dicegah karena semuanya memang sangat berbahaya dan bisa menimbulkan kerugian financial bagi Anda.

Dalam dunia internet, malware adalah hal yang berbahaya karena antivirus yang kita pasang pun tidak mampu mendeteksinya. Jika malware masuk dalam komputer kita, malware bisa mencuri data yang penting pada perangkat komputer kita. Tapi,jangan khawatir karena Anda bisa mencegah malware agar tidak mengacak-acak data di komputer Anda.

Jenis-jenis Virus pada Komputer

1. Ransomware
2. Trojan
3. Worm
4. Spyware
5. Memory Resident Virus
6. Multipartite Virus
7. FAT Virus
8. Directory Virus
10. Boot Sector Virus
11. Overwrite Virus
12. Web scripting Virus
13. Polymorphic Virus

Beberapa cara mencegah masuknya virus malware pada komputer

Sering update aplikasi

Salah satu mencegah masuknya malware pada komputer adalah sering mengupdate perangkat dan juga aplikasi yang ada misalnya saja update OS, software antivirus dan juga browser yang menjadi cara tempat masuknya malware.

Memasang antivirus

Sangat penting bagi kita yang memiliki komputer atau laptop untuk memasang antivirus ataupun internet security. Anda bisa memilih antivirus yang handal seperti Avast da Norton atau antivirus lainnya yang terpercaya dan berkualitas.

Selektif saat mendownload aplikasi

Kadang kita suka mendownload aplikasi gratisan atau bajakan, hal ini sangat berbahaya bagi komputer Anda. Bisa jadi aplikasi bajakan tersebut mengandung malware. Pastikan Anda mendownload aplikasi di tempat yang tepat dan hindari aplikasi bajakan.

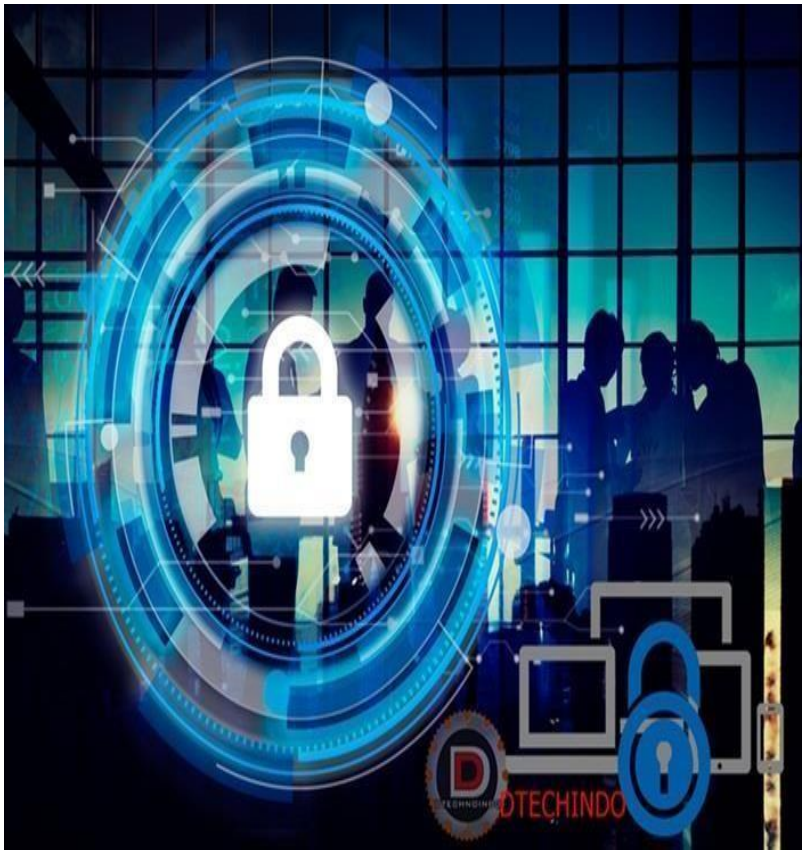
Selektif saat browsing

Untuk mencegah malware masuk ke komputer Anda, hindari menelusuri web atau situs yang kurang jelas atau tidak terpercaya. Jangan sekali-kali mendownload file atau aplikasi pada situs yang tidak jelas dan menggunakan file hosting mediafire dan lainnya.

Hati-hati dalam membuat pasword

Anda harus lebih berhati-hati saat membuat pasword baik pasword email ataupun pasword lainnya. Pastikan menggunakan kombinasi huruf, angka dan kode yang sangat sulit.

Tips menjaga keamanan data dan informasi



Di era modern seperti saat ini, teknologi sangat erat kaitannya dengan komputer. Komputer sudah menjadi bagian penting dalam kehidupan manusia millenium, penggunaan komputer sendiri sudah menjadi kebutuhan primer dalam tupoksi yang kecil hinga yang besar. Tak dipungkiri lagi, semua orang yang melakukan komunikasi atau pertukaran data serta informasi dengan pihak lainnya melalui internet ataupun mengcopy data menggunakan media penyimpanan secara manual. Data dan informasi itu akan disimpan pada komputer atau laptop pribadi ataupun juga yang berada di kantor.

Data penting yang berada dalam komputer perlu dijaga kerahasiaannya, karena data tersebut bisa saja menjadi target pihak yang tak berwenang, terutama data dan informasi milik pejabat dalam pemerintahan, pemegang tampu kebijakan dalam perdagang, militer, dan pihak penting lainnya. Ada beberapa cara yang dapat dilakukan oleh pihak yang tidak bertanggung jawab untuk mendapatkan data dan informasi, antara lain seperti probe, scan, account compromise, packet sniffer, hacking, denial of service, malicious code, dan social engineering. Cara – cara ini dapat merusak sistem pada komputer.

Tindakan preventif dapat dilakukan untuk pengamanan data, berikut tips dan trik untuk selalu aman dari serangan pihak yang tidak berwenang.

1. Tetap Update

Habisnya masa berlaku dapat menjadi masalah besar, ini dikarenakan banyak terdapat bug pada aplikasi ataupun sistem operasi. Oleh karena itu, keberadaan versi terbaru dari software sangatlah penting, karena dapat menjadi solusi bagi bug yang terdapat pada versi sebelumnya. Hal ini menjadi sangat penting pada sistem operasi yang bertanggung jawab terhadap manajemen file dan terutama ketika terkoneksi ke internet.

2. Mengamankan email

Email menjadi salah satu celah favorit pihak yang tidak berwenang untuk mengakses data pribadi. Password dan username bukanlah salah satu cara pengamanan email. Pengamanan email lainnya dapat dilakukan dengan cara menambahkan security question, dengan syarat jawaban yang akan menjadi kunci hanya diketahui pemilik email, selanjutnya adalah verifikasi email, tahapan ini berguna untuk melakukan verifikasi terhadap orang yang mencoba login pada akun milik kita, sehingga kita dapat mengetahui kapan akun media social kita diakses, dan yang terakhir adalah verifikasi email cadangan ataupun verifikasi nomor telepon.

Verifikasi email cadangan dapat dilakukan ketika akun email utama kita tidak bisa dibuka dikarenakan lupa password atau terkena aktivitas hacking, dan penggunaan verifikasi nomor telepon dapat sangat berguna ketika ingin mengakses, sistem otentikasi berbasis one time password akan mengirimkan nomor ataupun angka acak ke nomor handphone yang telah terdaftar, sehingga orang lain tidak bisa mengakses email kita.

3. Lakukan beberapa hal penting pada komputer

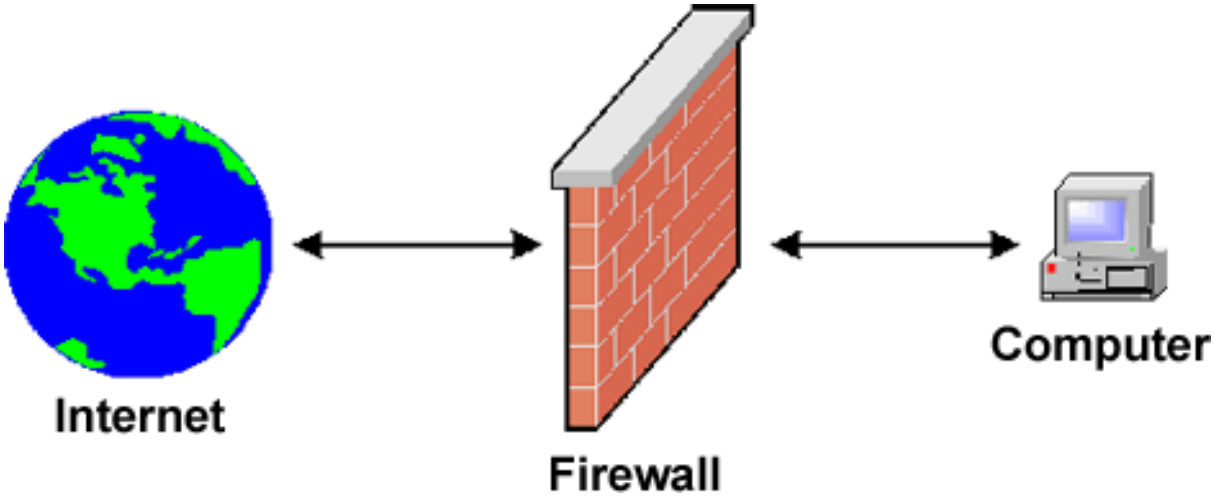
a) Setting personal firewall
b) Berikan password pada komputer
c) Gunakan enkripsi pada penamaan file ataupun folder pada media penyimpanan kita.
d) Lakukan backup data secara berkala.
e) Install anti virus.

Apa itu Firewall ?

Apa itu Firewall dan Apa Fungsi Firewall Pada Jaringan Komputer Dan Voip. - Kali ini saya akan membahas apa itu firewall dan fungsi firewall pada jaringan komputer dan voip itu apa? Firewall adalah tembok api, lantas apa fungsinya untuk jaringan komputer dan voip?
internal.

Firewall adalah sebuah sistem keamanan pada jaringan komputer yang digunakan untuk melindungi suatu komputer dari beberapa jenis serangan dari komputer luar, MenurutWikipedia Firewall itu adalah tembok api, tembok pelindung, atau dinding api yang merupakan suatu sistem yang dirancang untuk mencegah akses yang tidak di inginkan dari atau kedalam suatu jaringan.

Secara umum firewall digunakan untuk mengontrol akses terhadap siapapun yang memiliki akses jaringan private dari pihak luar. Tembok api atau firewall berkerja dengan cara melacak dan mengendalikan jalannya data serta memutuskan aksi untuk melewatkan, menjatuhkan, menolak, mengenkripsi atau melakukan pencatatan aktifitas data.



Fungsi Firewall Pada Jaringan Komputer

Fungsi firewall pada jaringan komputer antara lain :

- Mengontrol dan mengawasi paket data yang mengalir di jaringan.
- Melakukan melakukan autentifikasi terhadap akses
- Mencatat setiap transaksi kejadian yang terjadi di firewall
- Aplikasi proxy firewall mampu memeriksa lebih dari sekedar header dari paket data.

Fungsi Firewall Pada VOIP

selain pada jaringan komputer firewall juga memiliki fungsi pada VOIP antara lain :

- Voip memiliki ribuan port yang dapat di akses untuk berbagai keperluan
- Firewall di voip bertindak sebagai garis pertahanan pertama dalam mencegah semua jenis Hacking
- Firewall komputer bertugas menutup port port tersebut kecuali beberapa port yang perlu tetap terbuka
- Menjaga informasi rahasia dan berharga agar tidak keluar tanpa diketahui oleh pengguna

Memasang software anti malware

Saat ini banyak pabrikan teknologi yang menjual software anti malware yang berkualitas. Anda bisa memilih sofware tersebut untuk mencegah malware masuk kedalam komputer. Beberapa software anti malware tersebut terbukti bisa mencegah, menghindari dan juga mengatasi malware pada komputer dan perangkat lainnya.

Antivirus Android Terbaik Gratis

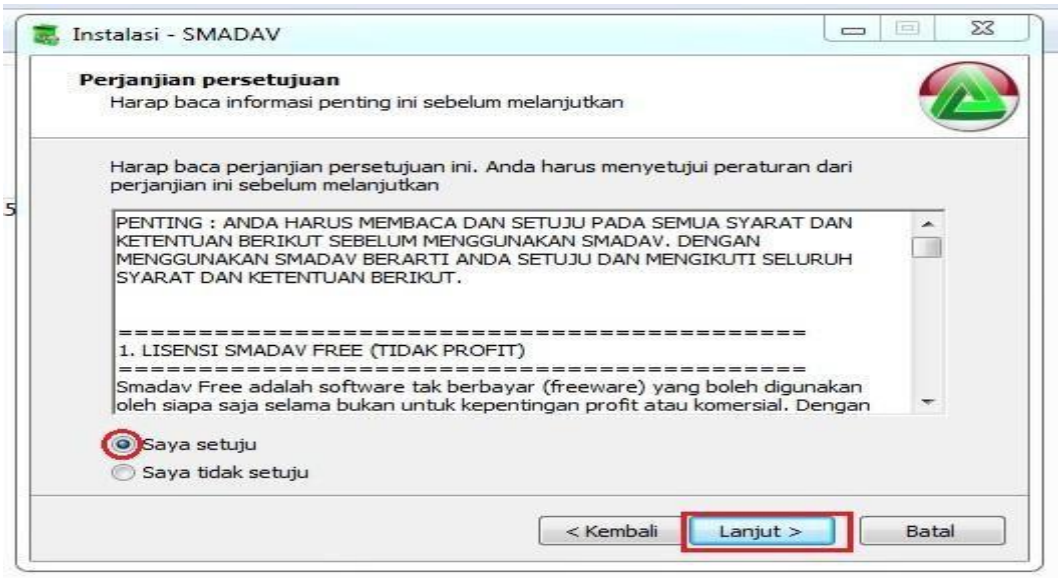
1. Antivirus FREE (AVG)
2. Avast! Mobile Security & Antivirus
3. McAfee Antivirus & Security
4. Norton Security Antivirus
5. Kaspersky Mobile Security Lite
6. Bitdefender Antivirus Free
7. Avira Antivirus Security
8. 360 Security- Antivirus, Clean
9. Sophos Security & Antivirus
10. G Data Antivirus Free
11. Dr. Web Anti-virus Light
12. Mobile Security & Antivirus (Trend Micro)

Cara Menginstal Antivirus Smadav

- Jalankan file smadav installernya.
- Pilih bahasa yang akan digunakan. Saya sarankan pilih bahasa Indonesia supaya mudah dipahami. Tetapi jika anda sudah mahir berbahasa Inggris, monggo pilih English.
- Klik OK.

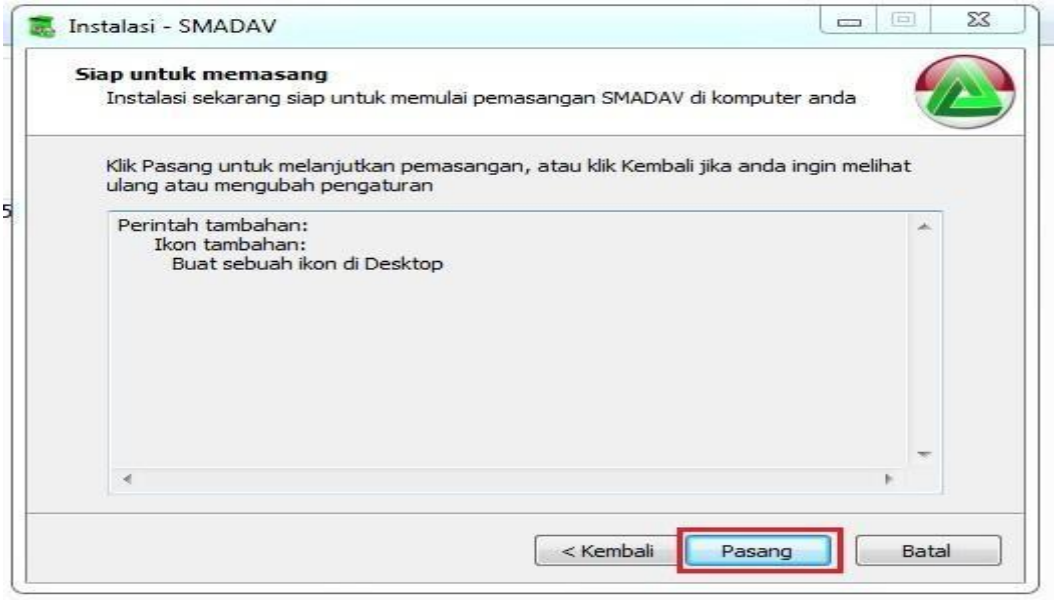
- Muncul tampilan Selamat Datang, Klik Lanjut.

- Centang pada kolom "Saya Setuju", dan Klik Lanjut.



- Jika anda ingin ikon smadav ada di desktop PC anda, maka centang (v) pada kolom "Buat sebuah ikon di desktop". Tetapi jika anda tidak ingin, hilangkan centangnya.
- Klik Lanjut.

- Klik Pasang.



- Klik Selesai. Smadav akan berjalan secara otomatis, karena kolom perintah "Jalankan Smadav" di Centang (v)"

- Pilih kembali bahasa yang digunakan, kali ini bahasanya di gunakan untuk bahasa aplikasi Smadav. Sesuaikan dengan kemampuan berbahasa anda.

- Selesai.

Manajemen password

1. Hindari Password Tunggal

Menggunakan password tunggal memang unggul dari segi kemudahan mengingat, namun kelemahannya jika sampai diketahui orang lain, bayangkan akses yang dimiliki oleh orang tersebut kepada semua account kita
.

Bagi account-account kita menjadi tiga level, yaitu klasifikasi „amat rahasia", „rahasia" dan „formalitas".

Tentukan masing-masing passwordnya lalu kategorikan account-account yang kita punya, misalnya account internet banking sebagai „amat rahasia", email termasuk „rahasia", tetapi account info airlines hanya „formalitas" (untuk password formalitas pakai saja password yang gampang misalnya delapan angka ulang tahun pasangan kita).Bayangkan, untuk semua account, kita hanya perlu menghapal tiga password saja, misalnya kita lupa paling tidak hanya butuh dua kali coba-coba.

2. Gunakan password yang tidak mungkin ditebak

Salah satu metoda paling amatir, dan dapat dilakukan oleh siapa saja untuk mendapatkan password kita, yaitu metoda brute force atau menebak-nebak segala kemungkinan password. Untuk klasifikasi account yang amat rahasia, pastikan password tidak mungkin dapat ditebak.

Anda bisa membuat password dengan kalimat biasa namun aman, misal nama anda Budi, maka anda bisa membuat password „Budi33tahun_Kerenloh", walau terlihat sederhana namun password seperti ini sudah memenuhi kaidah

password yang aman; selain karakternya panjang, juga menggunakan gabungan huruf besar kecil, karakter khusus serta angka. Ini dapat menghalau bukan saja metoda brute force tetapi juga metoda lain yang lebih canggih.

3. Simpan password di tempat paling aman, kepala anda

Banyak orang yang karena takut lupa, lantas menuliskan password dan disimpan di tempat yang (dipikir) aman, baik secara tertulis maupun elektronik. Namun tidak ada tempat yang paling aman selain di kepala kita sendiri, jika tiga password terlalu banyak, maka kita bisa membuat klasifikasi nya menjadi dua saja, yaitu password untuk account „amat rahasia" dan password „formalitas".

4. Bentengi komputer anda, gunakan sistem operasi dan software asli lalu update rutin

Komputer yang tidak dilengkapi dengan software asli atau tidak pernah di update, adalah ibarat rumah yang pintu pagarnya terbuka dan satpam nya sudah pantas masuk panti jompo.
Permasalahannya karena software-software tersebut tidak dapat melakukan update secara berkala, karena banyak update adalah guna menutup celah keamanan nya. Anti virus bahkan rutin memiliki update baru dalam hitungan jam saja.

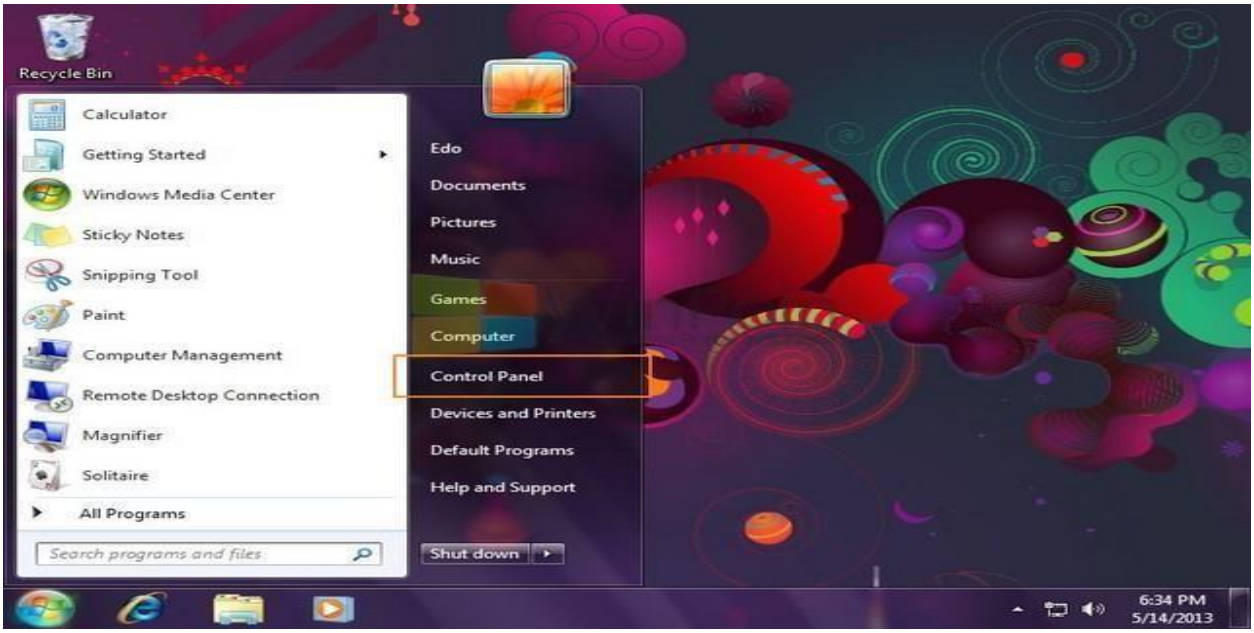
Se kompleks apapun password yang kita miliki, tidak ada artinya jika software-software di komputer kita tidak ter update, celah kemanan pada software dapat memberikan akses ilegal menyusup dan mencuri informasi termasuk password anda.

5. Ganti password secara periodik

Pakai momen-momen seperti ulang tahun atau tahun baru sebagai pengingat bahwa sudah saatnya kita mengganti password, idealnya password diganti sesering mungkin, namun akan cukup merepotkan.

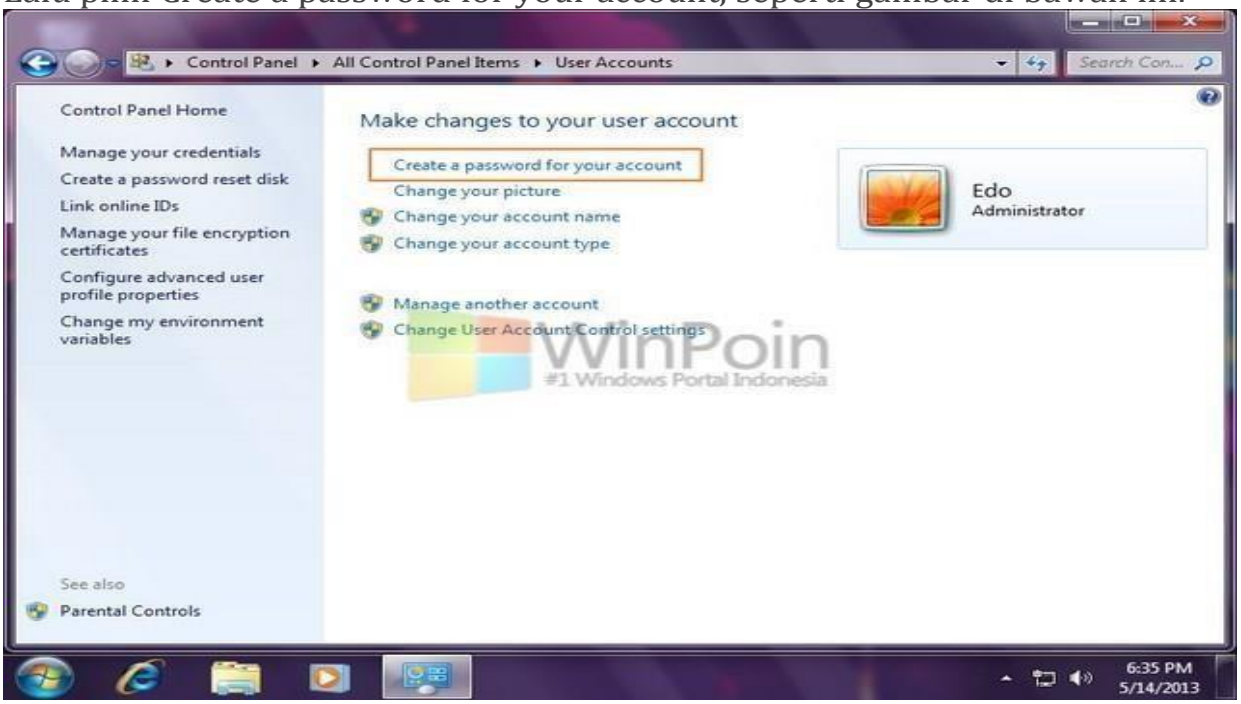
Cara Membuat Password Pada Komputer Windows 7

Pertama-tama buka Start Menu di Control Panel.

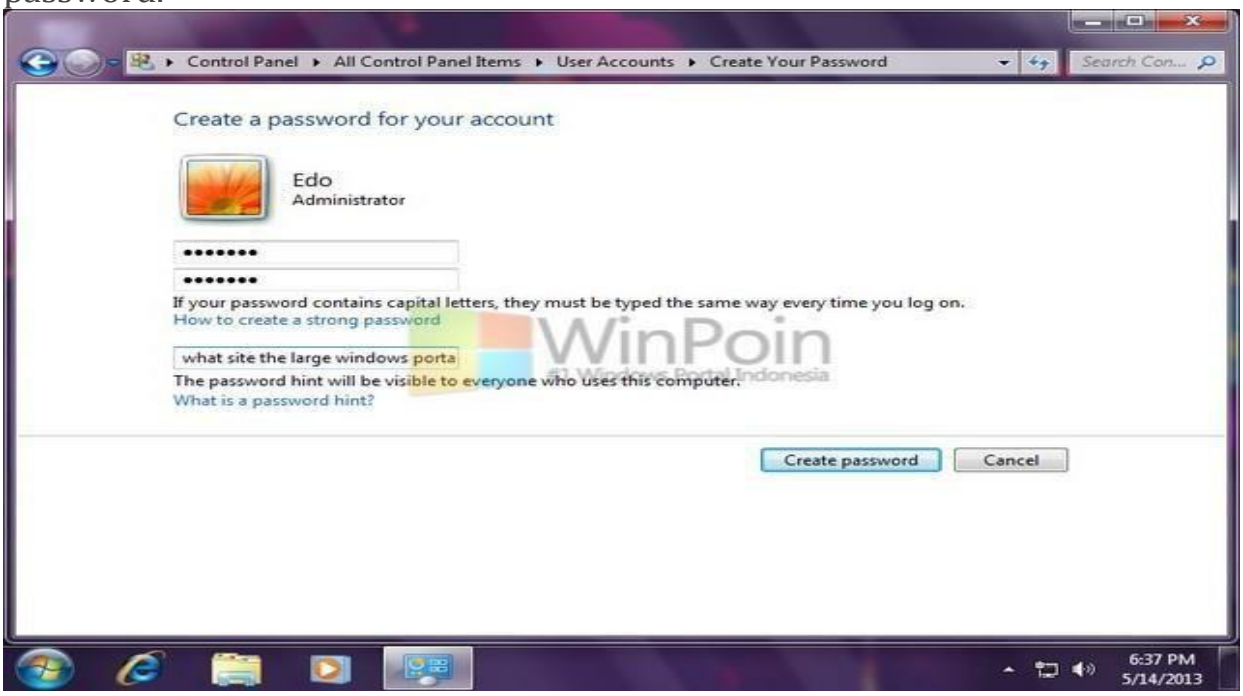


Kemudian setelah Window Control Panel terbuka, pilih view by small icon dan klik icon User Accounts.

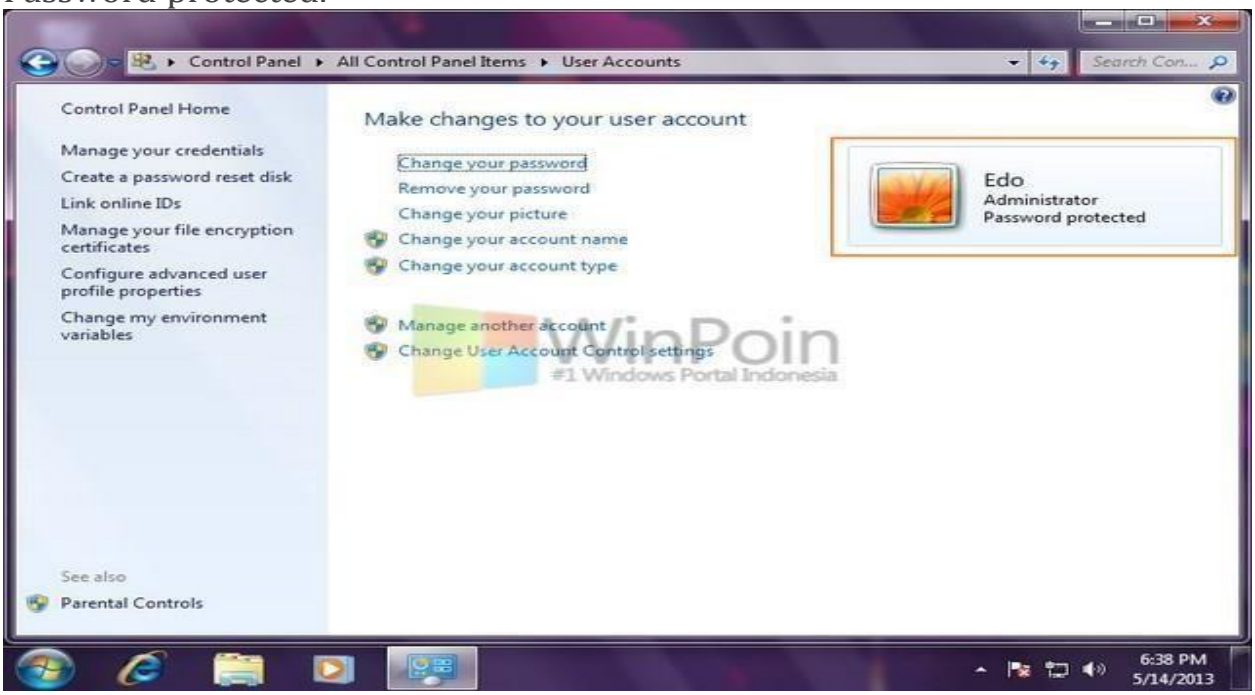
Lalu pilih Create a password for your account, seperti gambar di bawah ini.



Isikan password yang kamu inginkan dan ulangi lagi, setelah itu berikan petunjuk atau pertanyaan dari password yang kamu buat tadi dan klik Create password.



Ketika password selesai di buat maka profile kamu akan berubah bertuliskan Password protected.



Untuk mengganti password tidaklah sulit, tetapi hal pertama yang harus kita pelajari adalah membuat password yang kuat. Jika Anda yang awalnya menggunakan password sederhana namun di ganti dengan yang lebih sederhana, maka sama saja akan tetap mudah di hack.

Ini adalah daftar password / kata sandi yang paling buruk karena terlalu sederhana dan mudah ditebak orang. Hindari mengguanakan kata sandi seperti dibawah ini. Kata sandi yang buruk :12345678, Password, Admin, Login, Master, Katasandi, Aa12345, Admin12345, Abcd123, 30081993(format tanggal ulang tahun)

Cara membuat kata sandi yang kuat menggunakan gabungan kata special, huruf besar, huruf kecil dan angka. Anda juga bias membentuk sebuah nama tetapi dengan rumus gabungan special.Contoh kata sandi kuat dan mudah diingat: ##NamaSayaRudi**. Contoh kata sandi yang kuat tetapi sulit diingat:N4masa74Rudi$sXsa@

Jika anda ingin membuat kata sandi lebih kuat lagi tetapi masih mudah di ingat anda bias memanfaatkan metode sistem kode prefix dan suffix. Jadi konsepnya anda menggunakan katasandi yang lemah tetapi anda selalu ingat koe prefix yang ditambahkan didepan suffix di belakang kata sandi lemah tersebut. Contoh kata sandi sistem prefix suffix :1789@X&x[namasayarudi]x&X@1789

Pada cintoh diatas 1789@X&x adalah kode sandi prefix dan x&X@1789 adalah kode sandi suffix. Sandi [namasayarudi] adalah kata sandi yang lemah dan mudah diingat.

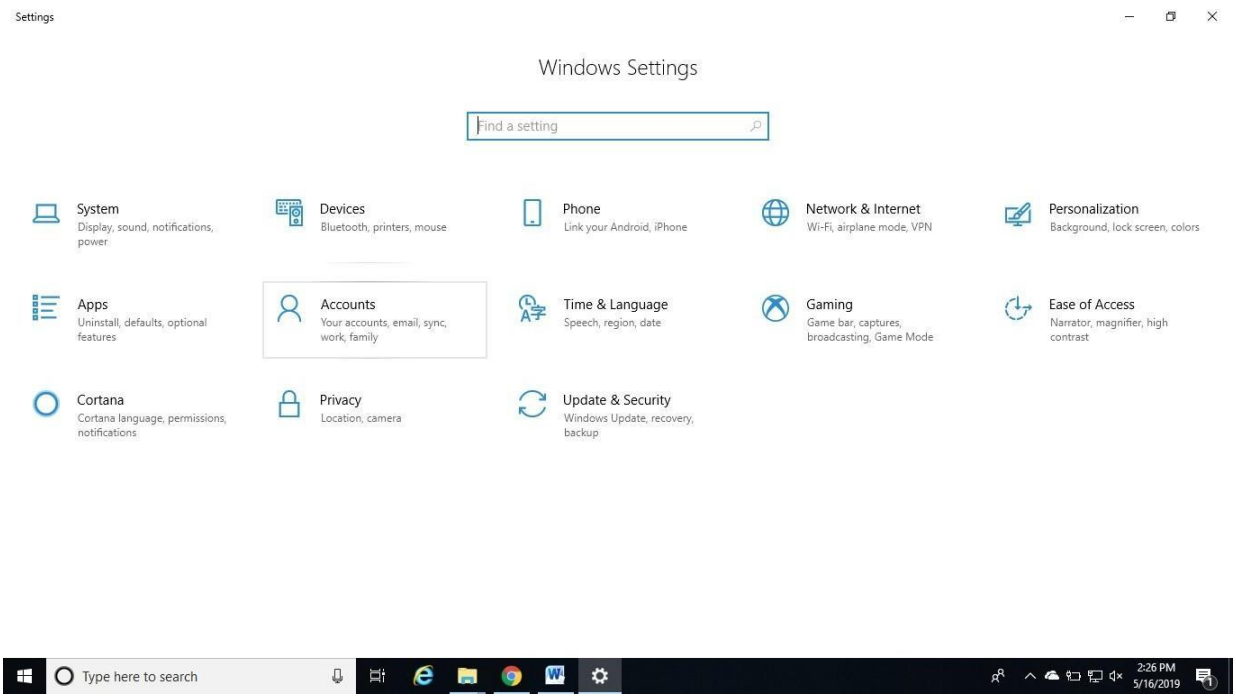
Anda bias buat variasi lain yang memperkuat kata sandi anda karena anda bias membuat kata sandi lemah berbeda-beda diberbagai situs. Karena adanya kode prefix dan suffix maka sangat mudah diciptakan kata sandi terkait layanan yang bervariasi.

Jika anda hanya perlu mengingat prefix dan suffix saja kemudian sesuai nama layanan anda jadikan kata sandi tengah

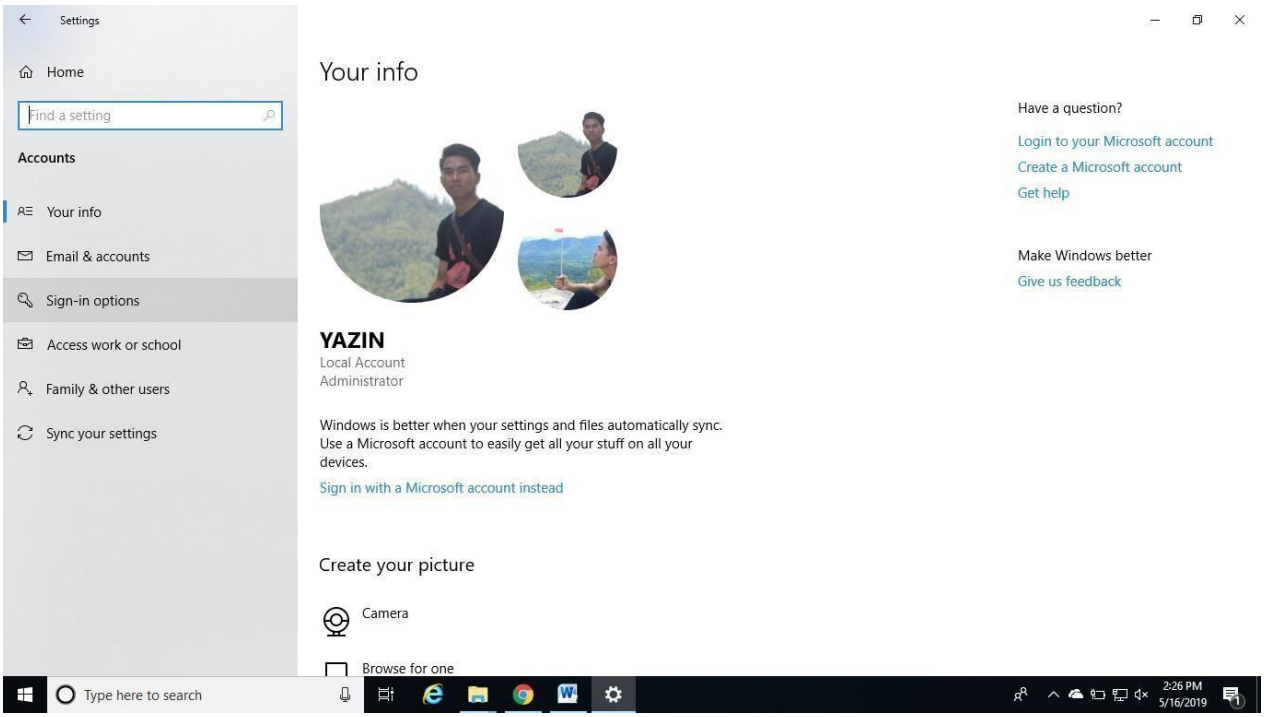
Cara Membuat Password di Komputer Windows 10

Adapun langkah-langkah memberi password pada komputer/laptop yang menggunakan windows 10 adalah sebagai berikut:

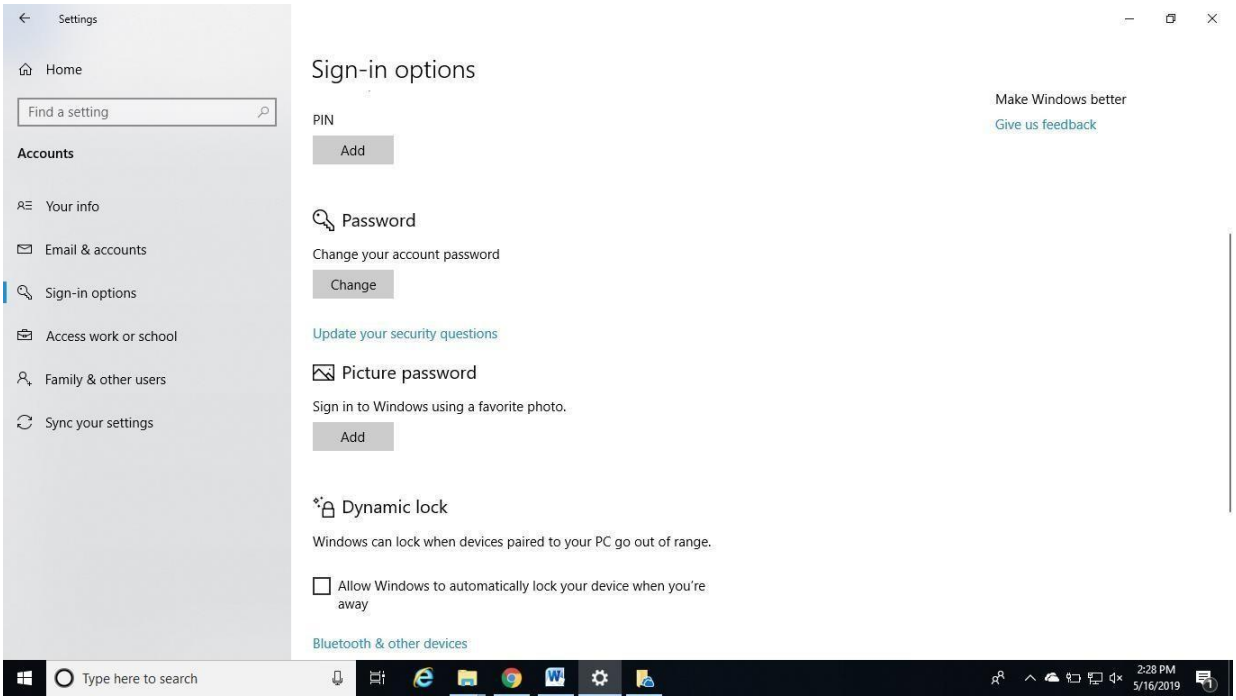
- Klik Tombol Star
- Pilih Setting yang berbentuk icon GIR
- Pilih Account (Your accounts, email, sync, work, family)



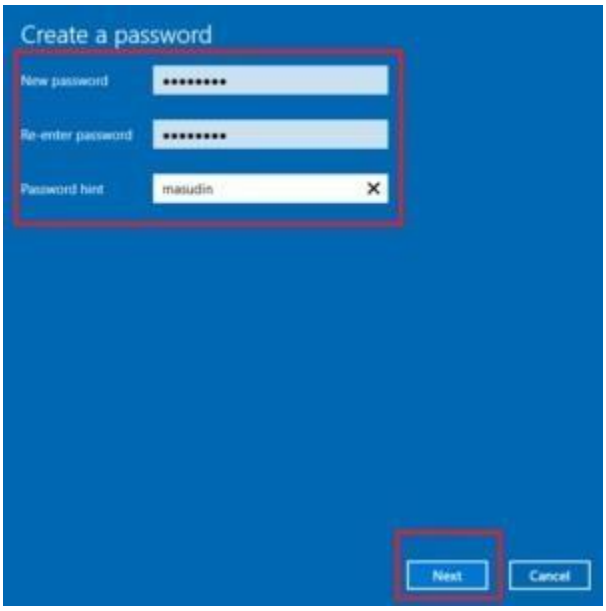
- Pilih Sig-in options



- Pada Menu Password, Klik tombol Add yang berada di bawahnya



- Maka akan muncul jendela Create a Password



- Isi data-data tersebut sebagai berikut:

1. New Password: masukkan kata sandi yang anda inginkan, usahakan kombinasi huruf dan angka supaya tidak mudah ditebak orang lain

2. Re-enter password: ulangi password yang anda buat tadi

3. Password hint: masukkan petunjuk kata sandi, isi dengan kata apa saja asalkan jagan anda isi sama dengan password

- Klik Tombol Next

- Maka akan muncul Jendela Create a password, Next time you sign in, use your new password

- Klik tombol Finish yang ada di bawahnya

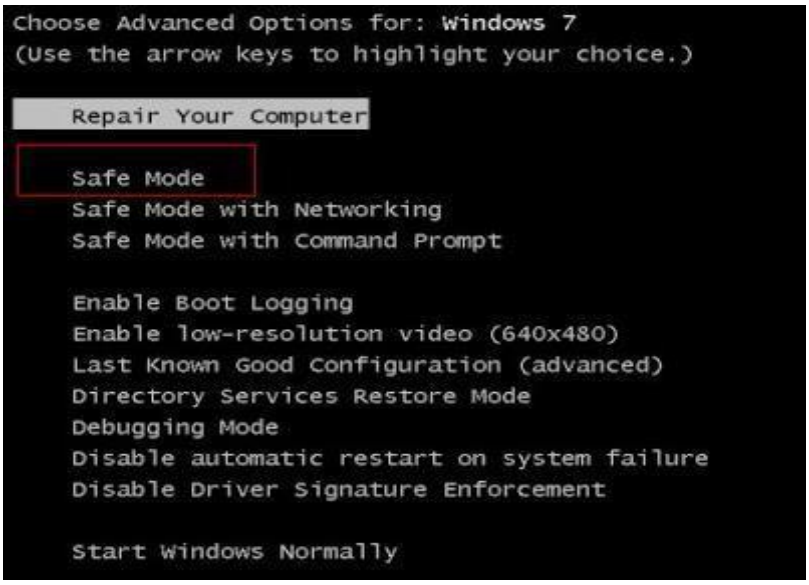
- Untuk menguji apakah komputer/laptop anda sudah ada passwordnya maka silahkan restart PC anda

Pernah Lupa password ?

Berikut ini langkah-langkah untuk log in ke dalam akun Anda melalui safe mode di windows 7.

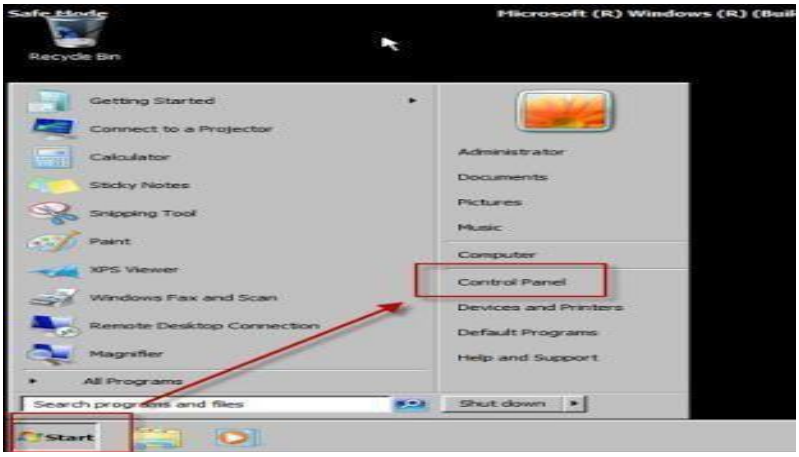
1.Nyalakan komputer Anda lalu tekan F8 saat komputer masih dalam proses booting. Kemudian layar Advanced Boot Options akan muncul.

2. Pilih "Safe Mode" dan tekan "Enter." Komputer Anda akan menyala dalam keadaan safe mode..



3.Dalam tampilan layar Anda, Anda akan melihat beberapa akun. Pilih akun Administrator (*built-in*). Secara *default*, akun ini tidak memerlukan *password*.

4.Setelah komputer Anda masuk dalam keadaan *safe mode*, klik tombol "Start" lalu "Control Panel."



5. Anda akan masuk ke "All Control Panel Items", lalu klik "User Accounts".

6. Setelah itu, klik "Manage Another Account". Pilih akun yang akan Anda ubah *password*-nya.

7. Klik "Change the password" di sisi kiri dan ketikkan *password* baru Anda dua kali. Kemudian klik "Change password."

8. *Restart* komputer dan jalankan seperti biasa lalu masukkan *password* baru di akun yang terkunci.

Log in menggunakan password reset disk

Untuk bisa menggunakan *password reset disk*, Anda harus membuatnya terlebih dahulu sebelum Anda lupa akan *password* windows 7 Anda. Jika Anda sudah membuatnya, inilah langkah-langkah untuk mengakses komputer Anda.

1. Saat Anda salah mengetikkan *password* Anda, Windows 7 akan menampilkan "Reset Password" yang dapat Anda klik.

2. Klik tautan tersebut dan Anda akan melihat „Password Reset Wizard" muncul pada layar komputer Anda. Lalu, klik „Next".

3. Pasang *flashdisk* tempat Anda menyimpan *password reset disk* dan klik „Next".

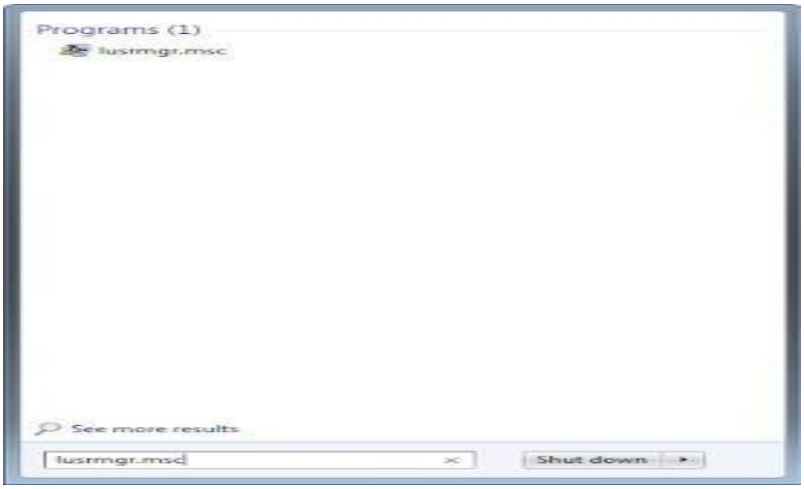
4. Lalu Anda harus mengetikkan *password* baru Anda. Setelahnya klik "Next".

5. Klik "Finish" dan Anda pun dapat membuka komputer Anda dengan *password* baru.

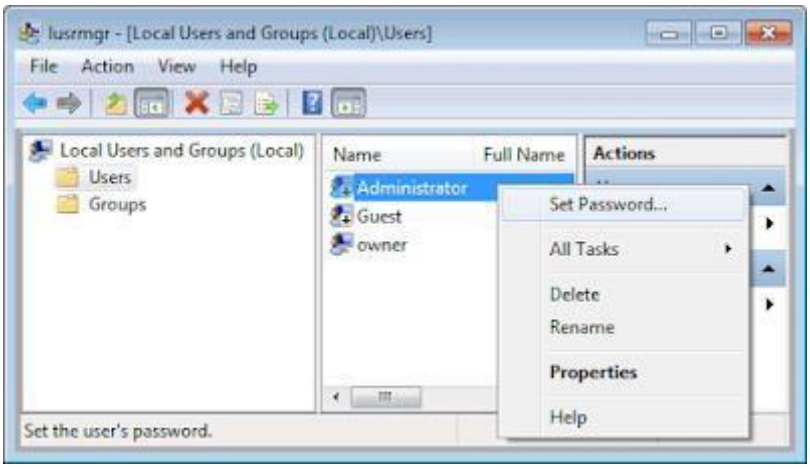
Log in menggunakan akun administrator

Jika Anda bisa membuka akun Administrator, Anda dapat dengan mudah mengubah *password*akun lain yang terkunci *password*. Ketika salah satu akun Anda terkunci, masuklah lebih dulu dengan akun Administrator Anda.

1. Pada menu Start, ketikkan "lusrmgr.msc"



2. Anda akan masuk menu Local Users and Groups
3. Klik menu "Users"
4. Klik kanan pada akun yang muncul di sisi kanan yang Anda lupa *password*-nya dan pilih "Set Password..."



5. Klik "Proceed" lalu ketikkan *password* baru Anda.
6. Klik "OK"

Untuk para pemakai Windows 10 tentu kamu sudah tidak asing lagi ketika kamu mau login ke PC kamu, kamu akan di suguhi dengan halaman untuk login ke komputer kamu tersebut. Kamu akan diminta terlebih dahulu untuk memasukkan passwords sebelum kamu bisa menggunakan laptop kamu.

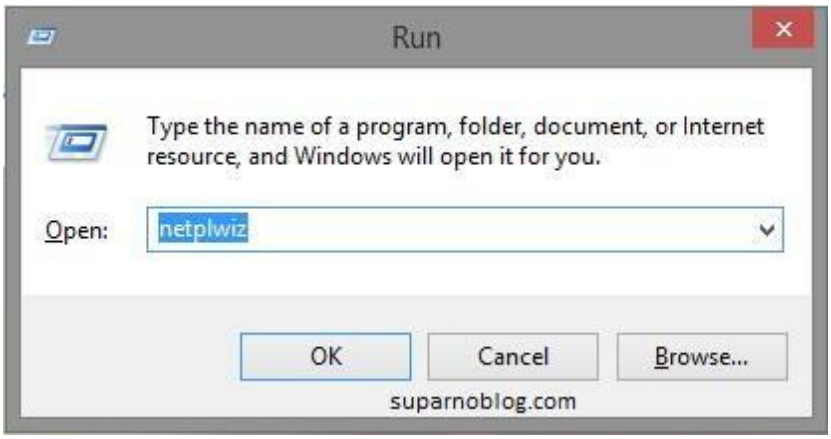
Sebenarnya hal ini bagus sekali sih untuk segi keamanan semua data yang ada di PC kamu. Karena tidak semua orang bisa mengakses komputer kamu tersebut tanpa tahu passwordnya. Ini juga bagus ketika Pc kamu mungkin hilang di curi orang, maka si pencuri akan kesulitan untuk mengakses laptop kamu. Tapi sebagian orang ada juga yang tidak suka dengan hal-hal yang rumit, contohnya saya sendiri tidak suka dengan hal yang membuat lambat pekerjaan saya. Makanya setiap saya mau buka laptop dan menghidupkanya saya paling malas kalau suruh masukkan password seperti itu.

Untuk itulah saya mencari cara bagaimana *cara menghilangkan Password Login di Windows 10*yang ada di komputer saya tersebut. Setelah saya browsing saya mendapat satu cara yang cukup mudah untuk menghilangkan password login di pc saya tersebut.

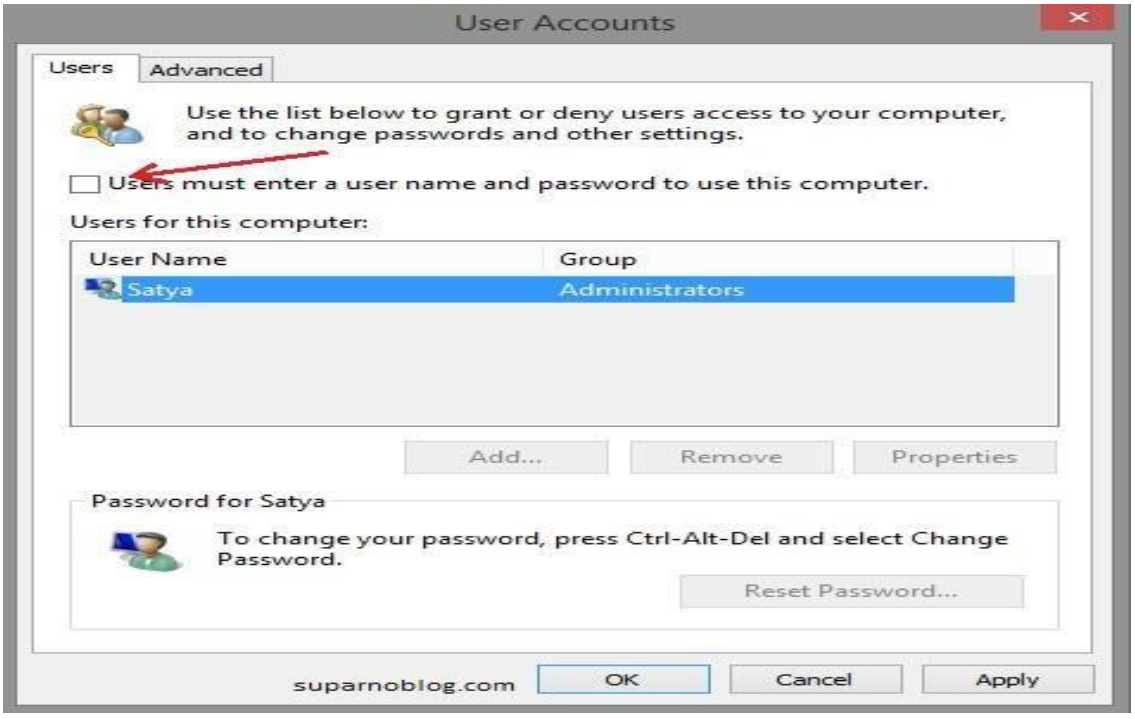
Step by Step cara menghilangkan password login di Windows 10

Berikut ini adalah cara menghilangkan password login di Windows 10 tersebut agar kamu bisa langsung masuk ke Windows tanpa harus repot-repot memasukkan password dan pin account kamu.

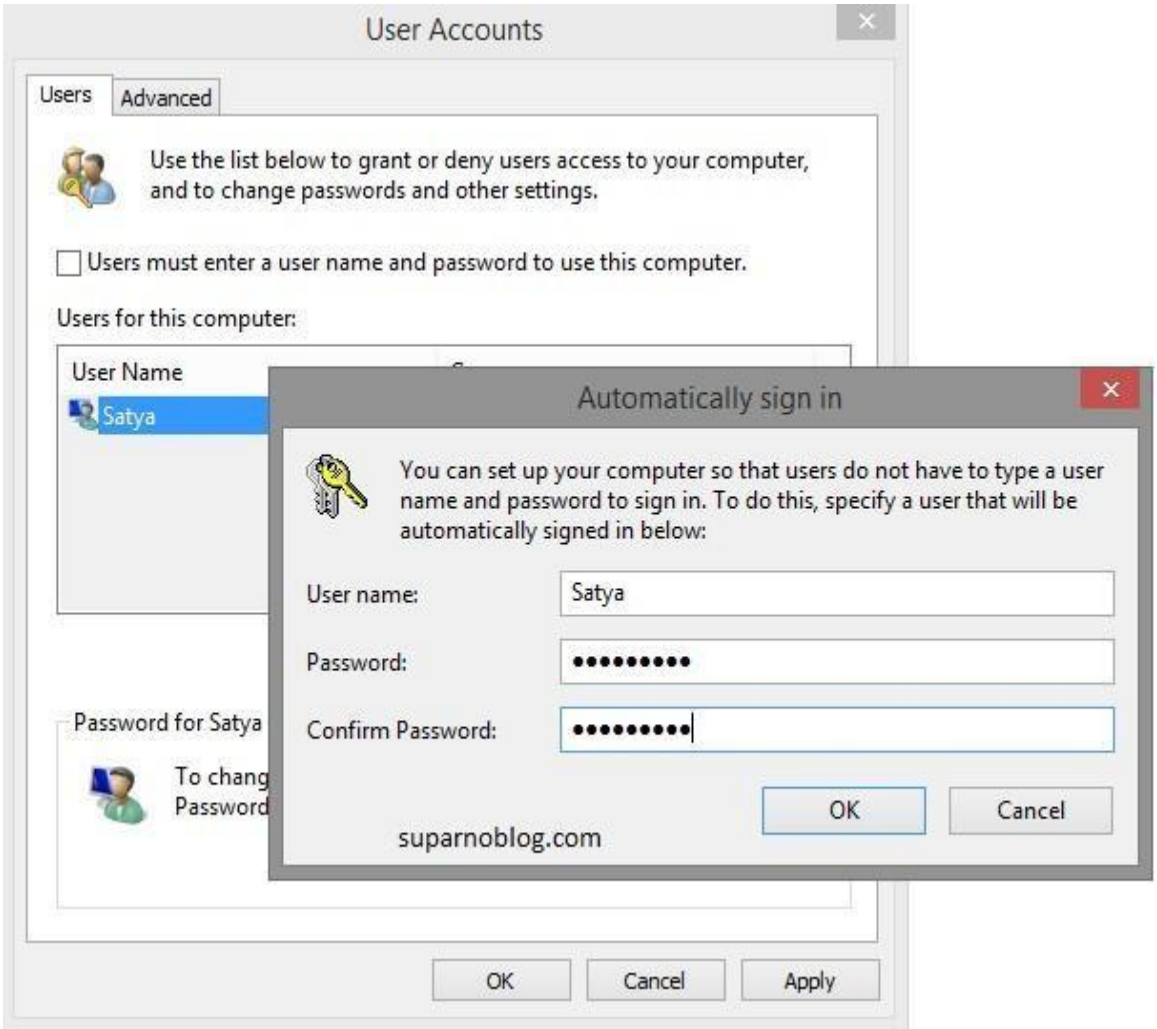
1. Pertama buka Run (Win + R), setelah itu ketikkan netplwiz, enter



2. Hilangkan centang "Users must enter a user name and password to use this computer" di account yang kamu gunakan. Setelah itu langsung saja klik Apply.



3. Setelah itu untuk konfirmasi kamu akan diminta memasukkan username dan password Windows 10 kamu. Pastikan kamu memasukkan detail yang benar, karena kalau tidak maka trik ini akan gagal. Jika sudah, klik Ok.



Selesai, gampang sekali khan? :))

Sekarang Coba kamu restart Windows 10 di PC kamu kalau kamu tidak salah langkah tentunya sekarang kamu tidak akan lagi diminta untuk memasukkan password lagi. Login screen tidak akan ditampilkan lagi, dan kamu bisa langsung menggunakan Windows sesaat setelah PC dinyalakan.

Untuk mengembalikan seperti semula, kembalikan lagi centang di opsi yang kamu ubah sebelumnya dan login screen akan kembali ditampilkan lagi.

Mengapa Backup Data Itu Penting ?

Backup data adalah kegiatan menyalin data yang telah tersimpan di sebuah perangkat ke media penyimpanan lain seperti USB flashdisk, Hardisk eksternal, maupun penyimpanan cloud. Membackup data ini bisa dibilang adalah suatu aktivitas yang sangat penting yang kerap kali dilupakan banyak orang.

Dan rasanya semua data perlu dibackup, mulai dari data hosting, data komputer, data kontak ponsel, dan lain-lain. Semua perlu dibackup dan anda simpan salinanannya agar apabila ada hal yang tidak diinginkan terjadi, maka anda masih punya salinannya. Dengan begitu, anda juga tidak akan repot-repot lagi mencari atau membuat data baru. Selain merepotkan, hal itu pastinya juga akan memakan banyak waktu.

ada beberapa alasan mengapa backup data itu penting.

1. Data Bisa Hilang Kapan Saja

Data komputer, data hosting, maupun data kontak ponsel bisa saja hilang kapan pun tanpa pernah anda perkirakan sebelumnya. Data komputer bisa hilang karena hardisk komputer rusak, data hosting bisa saja hilang jika hosting tersebut terjadi gangguan maupun terserang virus. Dan data ponsel mungkin saja hilang karena ponsel anda rusak atau pun hilang.

Intinya, semua data bisa hilang tanpa pernah kita perkiran sebelumnya.

Maka demikian, membackup data adalah satu-satunya cara guna menghindari kehilangan data. Komputer dan ponsel boleh saja rusak, namun data jangan sampai hilang. Oleh sebab itu, segeralah backup data-data anda, terlepas dari data komputer maupun data apapun itu.

2. Data Penting Adalah Waktu yang Berharga

Sekecil apapun data penting, maka hal itu pasti sangat penting. Membuat atau mengolah data tentu membutuhkan waktu yang tidak sebentar. Bahkan, meskipun data itu kecil, bisa saja nilainya setara dengan puluhan atau ratusan jam kerja anda.

Misalkan saja seorang konten kreator yang menyimpan data-datanya di komputer maupun di kontrol panel hosting, membuat data tersebut sudah menghabiskan puluhan jam duduk di depan komputer. Namun tiba-tiba, hardisk komputer itu rusak ataupun kontrol panel tidak bisa lagi diakses, maka tidak terbayang berapa lama waktu yang konten kreator itu habiskan untuk membuat konten-konten penting kembali.

Tidak hanya itu, salah satu contoh lagi adalah ketika anda sudah bersusah payah mengerjakan laporan skripsi. Dan anda sudah menghabiskan banyak waktu untuk menyelesaikan laporan tersebut. Akan tetapi, tiba-tiba hardisk komputer maupun laptop anda rusak dan tidak bisa lagi diperbaiki. Kejadian itu pastinya sangat mengerikan. Tidak hanya kehilangan laporan skripsi saja, anda juga telah menghilangkan puluhan bahkan ratusan jam waktu yang sangat berharga.

Oleh karena itu, melakukan backup data secara berkala tidak hanya dapat menyelamatkan data penting saja, tapi anda juga telah menyelamatkan waktu yang sangat berharga.

3. Virus yang Ada di Mana-Mana

Virus juga merupakan salah satu ancaman bagi data-data penting anda. Tidak sedikit ditemukan bahwa ada beberapa virus yang bekerja dengan menghapus atau merusak berbagai data dengan format tertentu. Misalnya, salah satu virus komputer yang bernama Blackmall, virus yang mampu menghapus sekitar 11 format file. Tentu hal tersebut merupakan ancaman bagi data-data penting nan berharga anda

Dengan begitu, untuk meminimalisir kejadian seperti itu, membackup data merupakan langkah yang penting guna mengamankan data-data anda dari serangan virus berbahaya semacam itu.

4. Membackup Data Itu Mudah

Bagi pengguna komputer, khususnya pengguna Windows yang ingin membackup data, maka anda dapat membackup data secara online, memanfaatkan layanan One Drive yang sudah terintegrasi baik di OS tersebut, maka secara otomatis anda dapat membackup data yang anda inginkan.

Bagi pengguna komputer yang ingin membackup data secara offline, anda bisa menggunakan USB flashdisk, hardisk eksternal, hingga CD/DVD yang sudah anda miliki.

Bagi konten kreator ataupun blogger yang ingin membackup data dari hosting, maka rasanya anda bisa menggunakan cara online. Contohnya, membackup data ke Dropbox, GoogleDrive, SugarSync, dan lain-lainnya. (Untuk pengguna Indoworx yang ingin membackup data hostingnya, maka salah satunya bisa menggunakan cara ini; Bagaimana Cara Melakukan Backup)

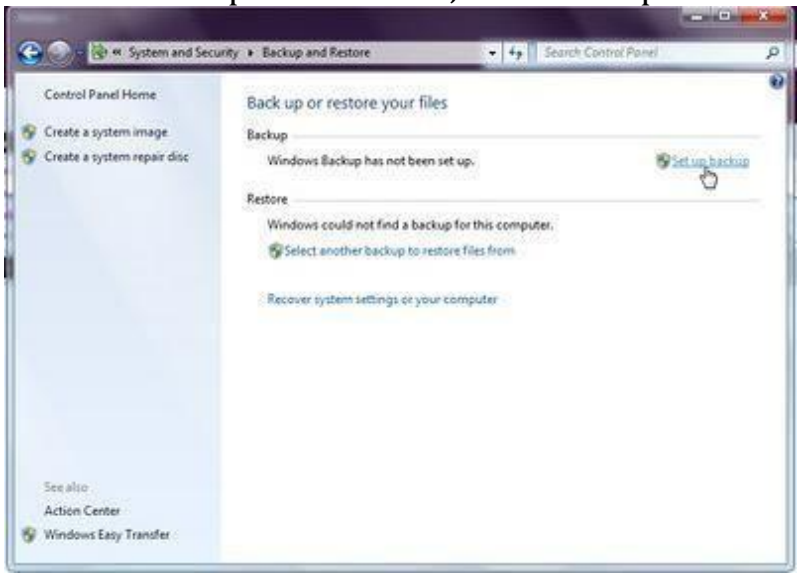
Untuk pengguna ponsel yang ingin membackup data kontak ponsel atau yang lainnya, maka anda bisa membackup data ke USB Flashdisk, Hardisk eksternal, maupun menyalinnya ke komputer atau laptop anda. Selain itu, anda juga bisa membackup data-data ponsel secara online ke penyimpanan cloud, seperti Dropbox dan lainnya.

Tips Cara Backup Data Windows 7

Apa itu backup data? Backup data pada laptop anda sangat penting untuk keperluan menyimpan data-data yang tersimpan di laptop atau backup data secara online juga bisa dilakukan. Terkadang dalam penyimpanan data yang penting perlu dilakukan secara berkala jika suatu saat sobat ingin mengembalikan data nya kembali maka dengan mudah di restore.
Backup data sebenarnya banyak caranya mulai dari membackup data dengan menggunakan media online, flashdisk, cd/dvd, hardisk external, maupun bisa juga menggunakan software. Pada tutorial kali ini IT Newbie ingin memberikan Tips Cara Backup data di Windows 7 yang ternyata masih banyak yang belum tahu caranya. langsung saja ikuti langkah nya sebagai berikut :

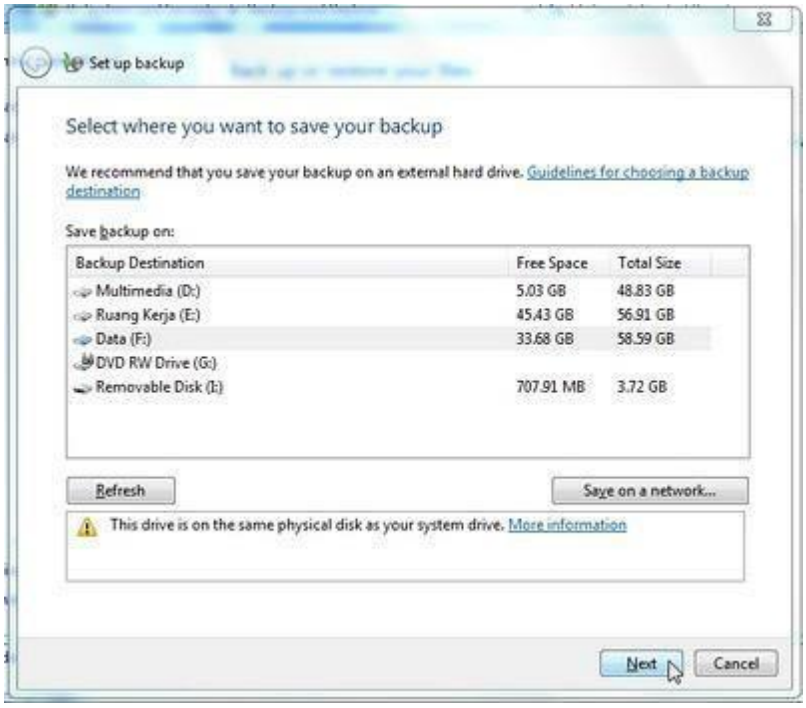
1. Sobat bisa klik tombol start kemudian klik control panel
2. Pada jendela control panel sobat bisa melihat opsi System and security, kemudian pilih Backup your computer

3. Lalu pada halaman Backup and Restore, sobat bisa pilih Set up Backup

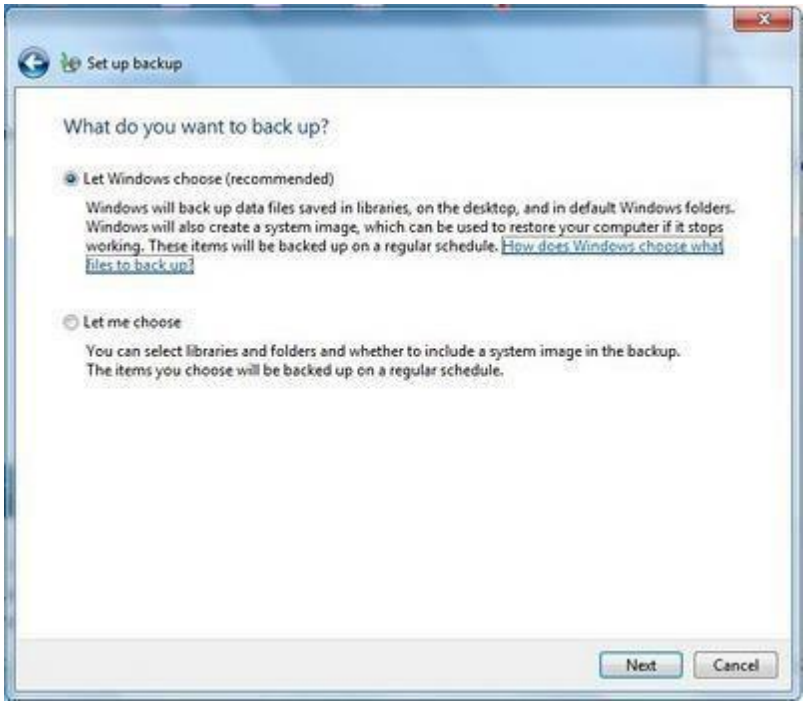


4. Sobat bisa tunggu beberapa menit sampai muncul kotak dialog set up backup

5. Pada kotak dialog set up backup, kemudian sobat bisa menentukan tujuan penyimpanan hasil backup data sobat, kemudian klik next.



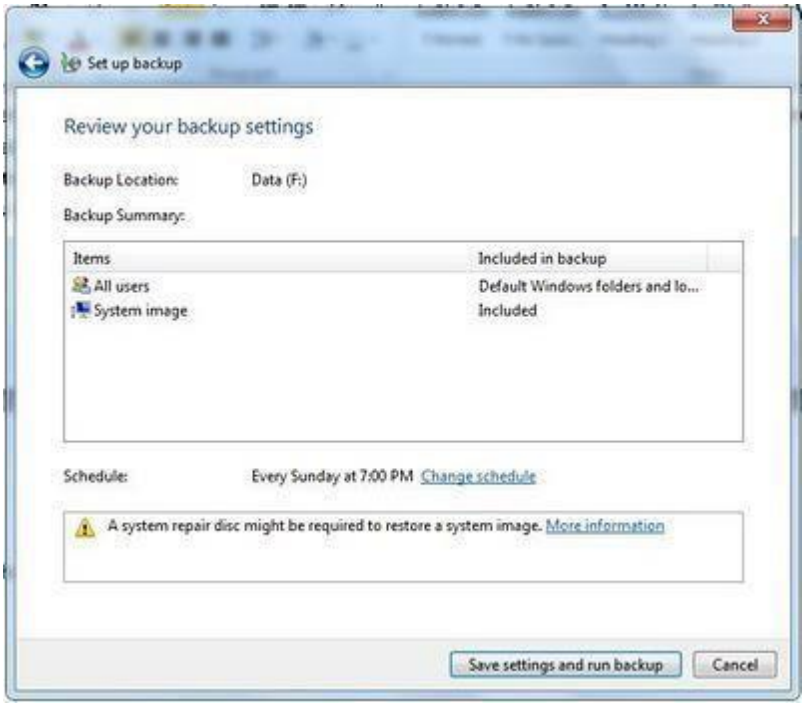
6. Kemudian halaman berikutnya akan ada 2 kotak dialog yang bisa sobat pilih



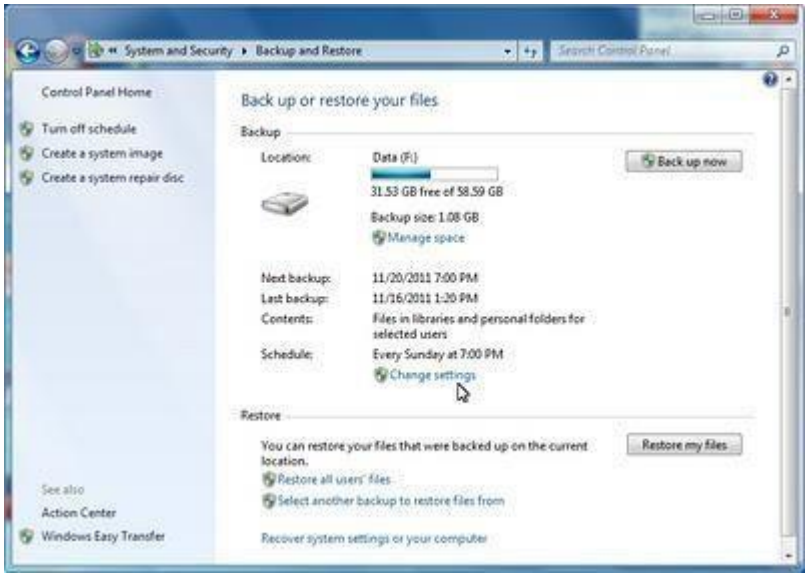
Keterangan :

Let Windows Choose (Recommended) : Windows otomatis akan melakukan backup data pada windows 7 yang terimpan pada Libraries, desktop, favorite, my document dan folder-folder standar windows. Dan windows juga akan membuat sebuah system image, jika dimana suatu saat windows sobat rusak, corrupt atau error maka sobat bisa merestore dengan cepat dan mudah.
Let me choose : Sobat bisa memilih sesuai dengan keinginan sobat folder-folder mana saja yang sobat anggap penting serta menyimpan system image dalam backup.

7. Kemudian setelah sobat memilih salah satu opso diatas lalu klik next
8. Langkah terakhir sobat bisa klik save settings and run backup untuk menyimpan dan menjalankan proses backup data.

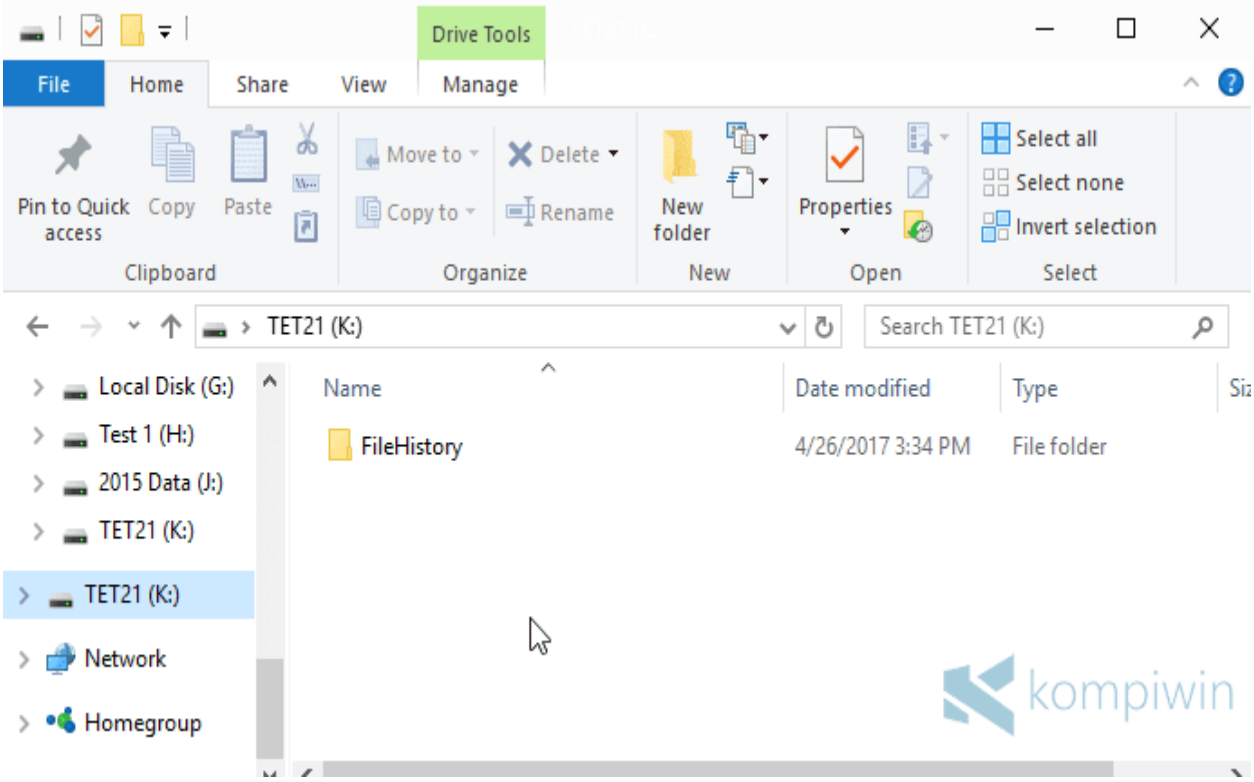


9. Sobat bisa tunggu sampai proses backup data system windows 7 selesai. Lama nya proses backup data tergantung dari besarnya data sobat.
10. Selesai sudah sobat membackup data system windows 7 maka hasil backup data sudah tersimpan dengan aman. Selanjutnya sobat dapat mengatur melakukan penjadwalan backup data secara otomatis, jika diperlukan.



Bagaimana cukup mudah bukan??
Sekarang sobat sudah mempunyai backup data yang tersimpan di hardisk sobat. Jika suatu saat system sobat rusak, hang, atau currupt/error sobat dapat dengan mudah mengembalikannya seperti hasil terakhir backup data nya.

Cara Back Up data



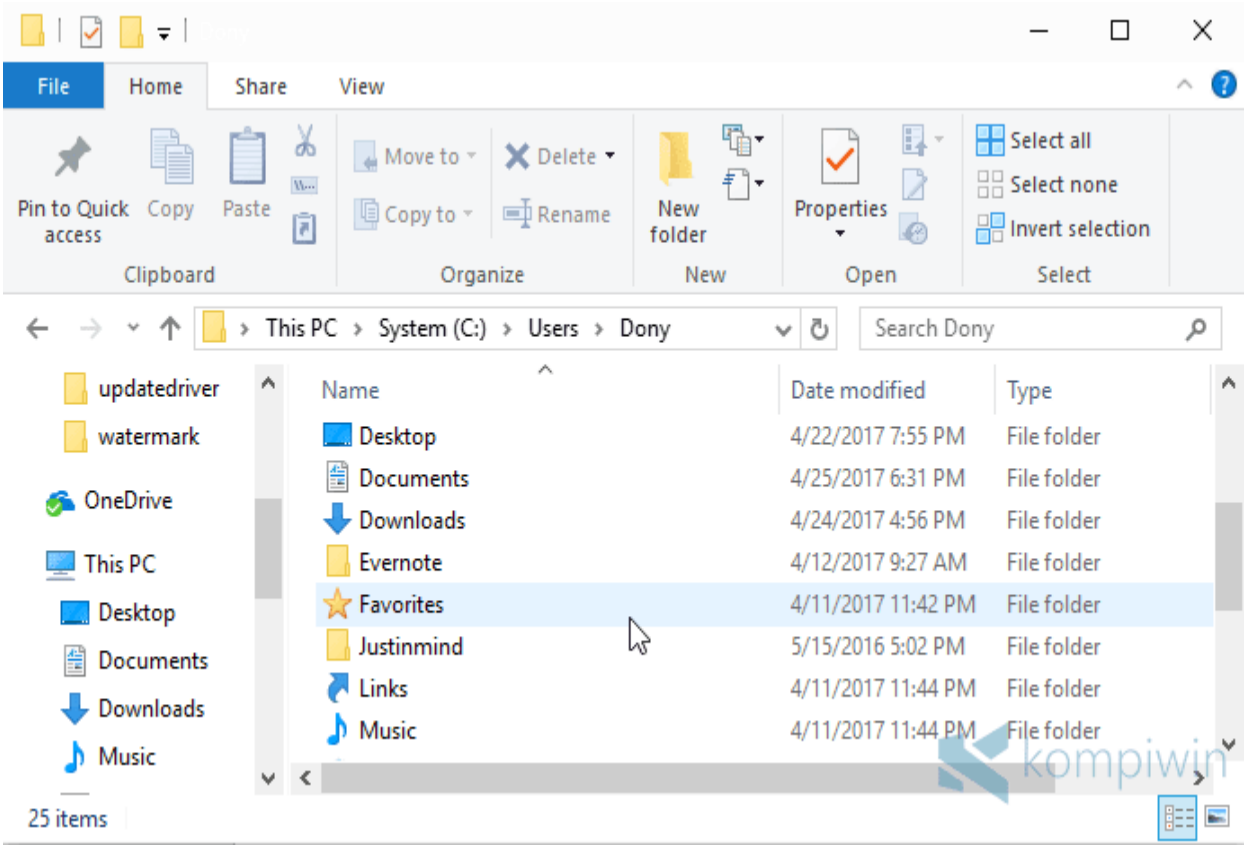
Backup data atau file pribadi di komputer itu sangat penting. Dengan mem-backup data, sobat dapat mengembalikan data ketika laptop/PC mengalami kerusakan. Ketika saat-saat darurat, laptop dapat bekerja dengan file-file pribadi yang baru saja dikembalikan.

Ada banyak cara yang dapat dilakukan untuk mem-backup data. Khususnya di PC/laptop, sobat bisa menggunakan berbagai cara dari yang mudah hingga sulit dilakukan, juga bergantung pada jenis backup yang sobat inginkan. Windows punya berbagai tools bawaan yang dapat sobat manfaatkan untuk mem-backup data, tanpa software tambahan. Mulai dari File History (Windows 8, Windows 8.1, Windows 10), Backup & Restore (Windows 7), System Image Backup, dan OneDrive.

Mem-Backup Data dengan File History

File History bukan hanya mem-backup data pribadi. Sobat juga dapat mengembalikan versi dari suatu file ke versi lamanya dengan File History. Misalkan, sobat membuat dokumen Word yang telah di-save berkali-kali. Maka sobat dapat mengembalikan kondisi dokumen Word menjadi semula sebelum kembali di-save. Jadi, apa itu File History? Bagaimana mem-backup data pribadi di Windows dengan File History?

#1 File History Hanya Mem-backup Data Pribadi



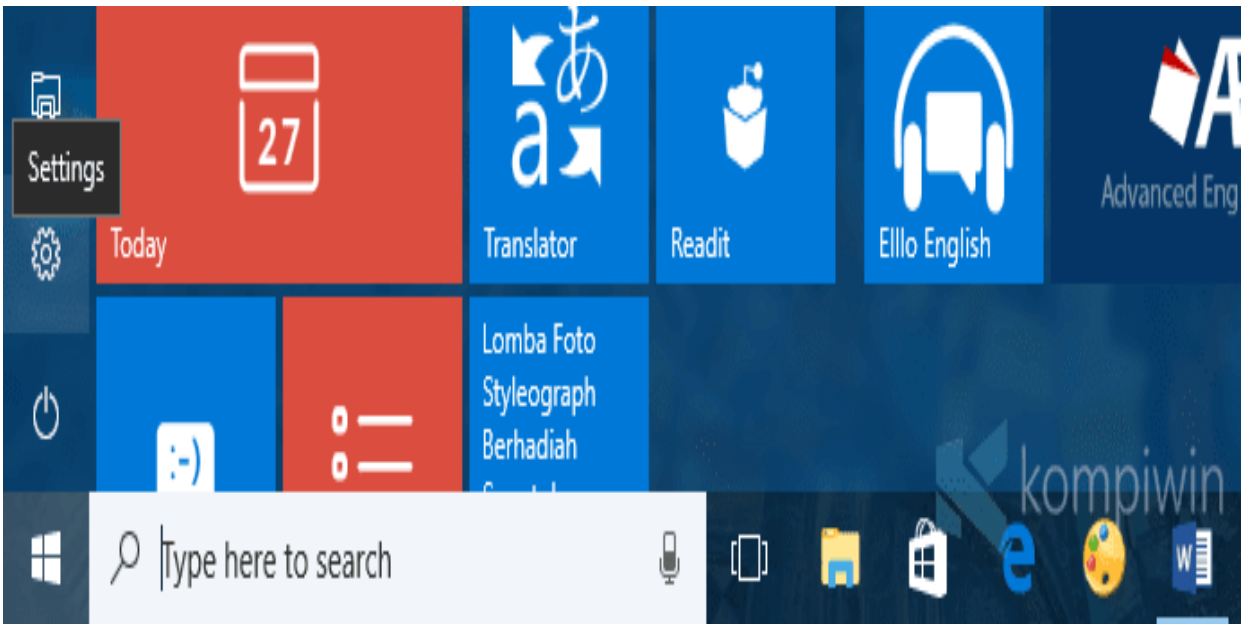
File History hanya mampu mem-backup data pribadi. Data pribadi ini mencakup folder "Pictures", "Videos", "Music", "Documents", "Downloads", dan folder pribadi lainnya di user account sobat. File History tentu saja bukanlah satu-satunya fitur bawaan Windows untuk mem-backup. Ada beberapa fitur lain yang juga berfungsi untuk mem-backup. Jika sobat hendak mem-backup keseluruhan harddisk, gunakan System Image Backup ketimbang File History.

Jika sobat ingin mem-backup folder/file yang tak terletak di folder pribadi di user account, maka sobat nantinya bisa menambahkan folder tersebut untuk ikut ter-backup. Lalu, bagaimana cara mem-backup menggunakan File History?

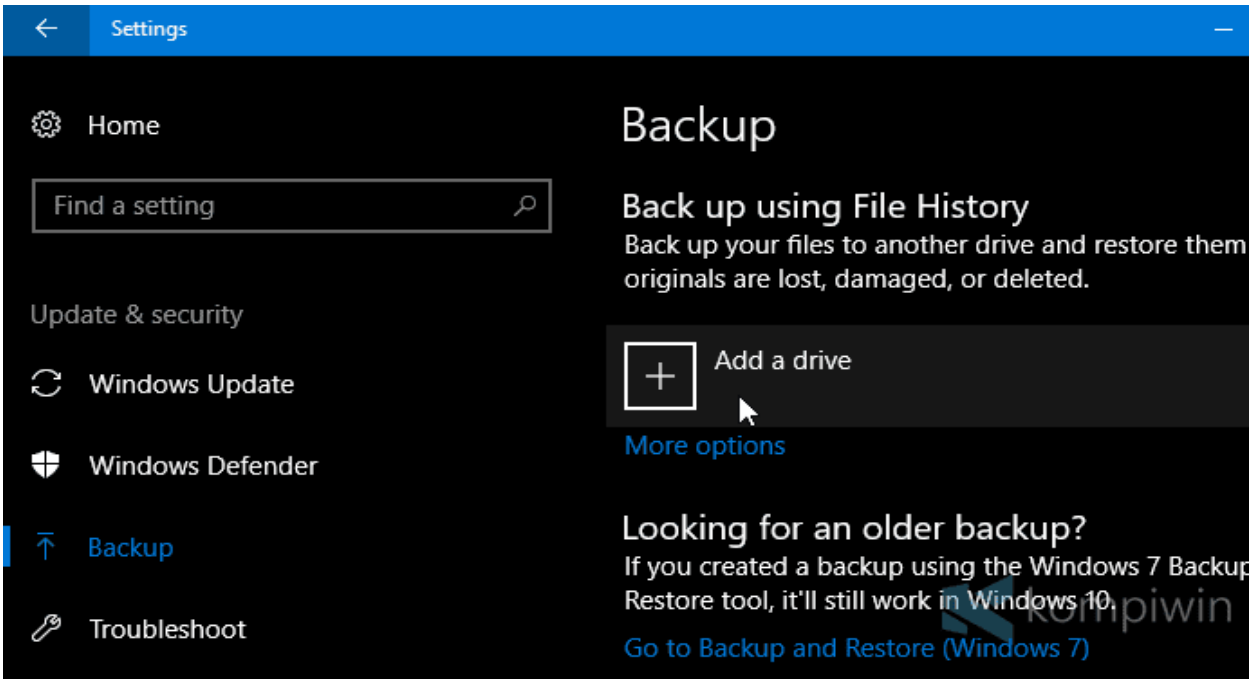
#2 Cara Mem-backup File Menggunakan File History

File History bekerja layaknya aplikasi/software/fitur backup lainnya. Bedanya, File History adalah fitur bawaan Windows yang hanya mampu mem-backup data-data pribadi, serta kemampuannya mengembalikan versi dari suatu file. Untuk mengaktifkan File History, colok dan hubungkan flashdisk, DVD, harddisk eksternal, SD card, atau media penyimpanan eksternal lainnya sebagai tempat untuk menyimpan backup nanti. Perhatikan kapasitasnya juga.

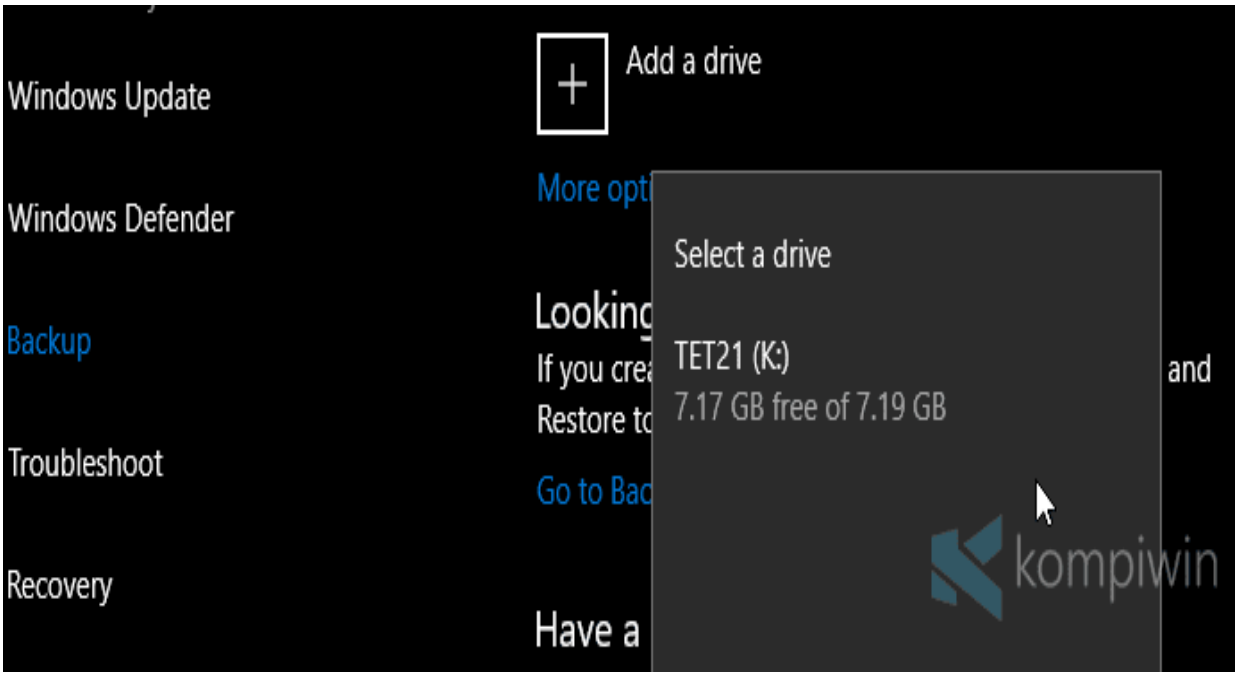
Buka Settings > Update & Security > Backup.



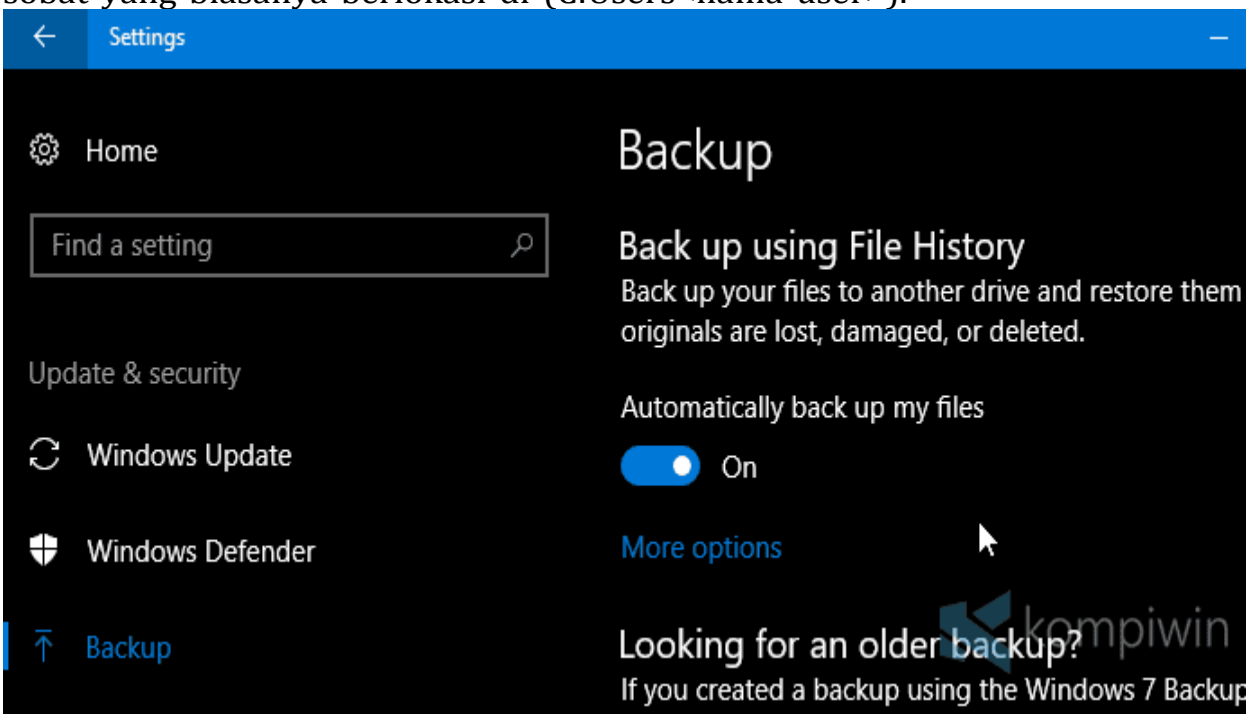
Klik “Add a drive” untuk menambahkan flashdisk, DVD, harddisk eksternal, SD card, atau media penyimpanan eksternal lainnya.



Muncullah list dari semua drive eksternal. Pilih salah satu untuk dijadikan tempat backup.

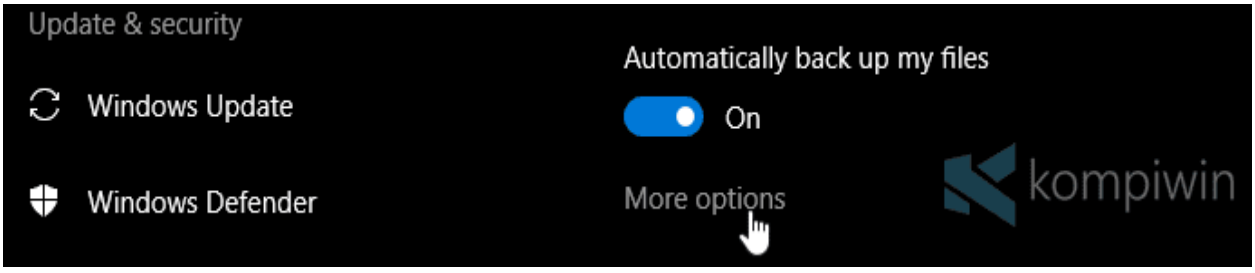


File History kemudian akan mem-backup secara otomatis semua data pribadi sobat yang biasanya berlokasi di (C:Users<nama user>).



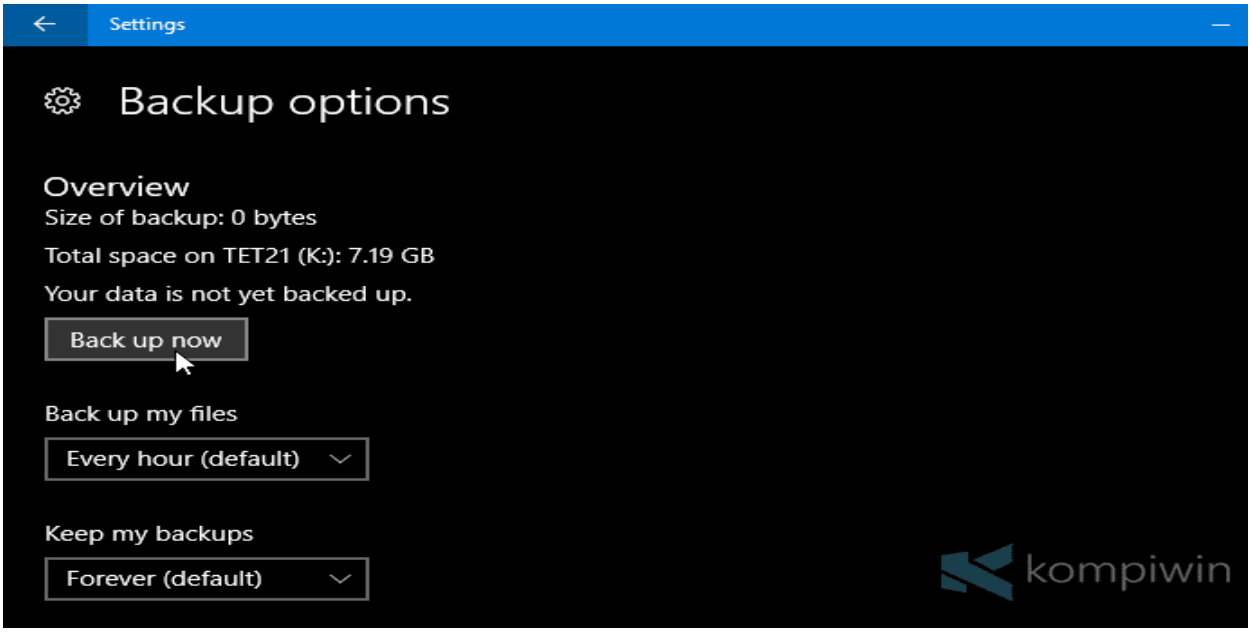
#3 Cara Memilih Setiap Kapan File Di-backup

Masih di Settings > Update & Security > Backup. Klik "More options" untuk melihat settings dan mengatur bagaimana File History mem-backup file pribadi sobat.



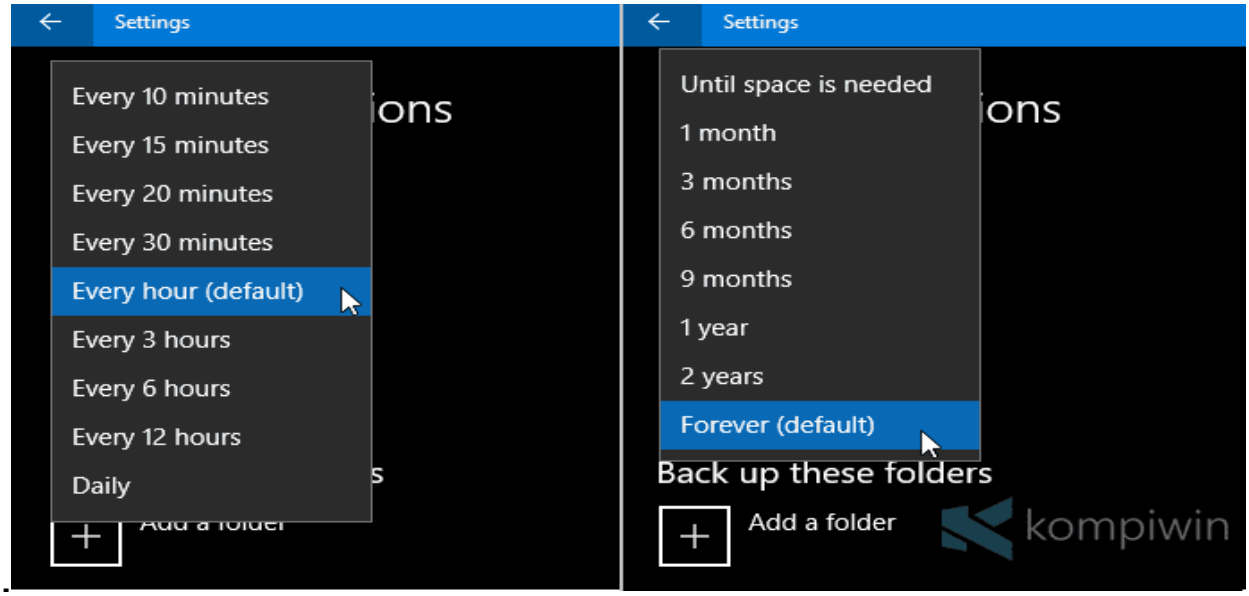
Di sini, sobat bisa mengatur seberapa sering File History mem-backup, berapa lama file akan di-backup, dan memilih folder mana saja yang ingin sobat backup. Sobat juga akan melihat berapa size dari total file yang di-backup.

Untuk mem-backup secara manual, klik "Backup now". Proses backup memakan waktu yang tak bisa diprediksi, dan bergantung dengan jumlah file serta kecepatan flashdisk, DVD, atau tempat menyimpan backup lainnya.



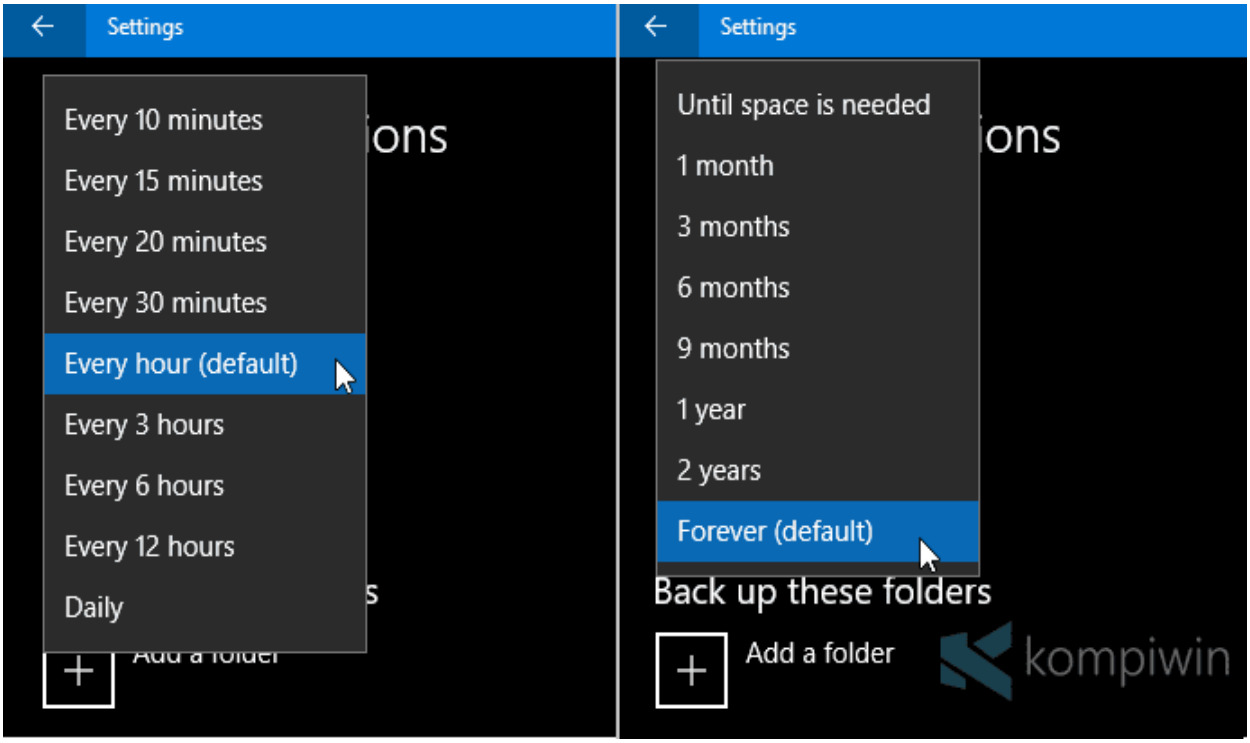
Di sini, sobat bisa mengatur seberapa sering File History mem-backup, berapa lama file akan di-backup, dan memilih folder mana saja yang ingin sobat backup. Sobat juga akan melihat berapa size dari total file yang di-backup.

Untuk mem-backup secara manual, klik "Backup now". Proses backup memakan waktu yang tak bisa diprediksi, dan bergantung dengan jumlah file. Serta kecepatan flashdisk, DVD, atau tempat menyimpan backup lainnya



#4 Cara Memilih Berapa Lama File Di-backup

Pada "Keep my backup", pilih berapa lama File History akan mempertahankan semua file yang di-backup. Mulai dari ketika kapasitas kepenuhan, satu bulan, tiga bulan, enam bulan, sembilan bulan, satu tahun, dua tahun, dan selamanya.

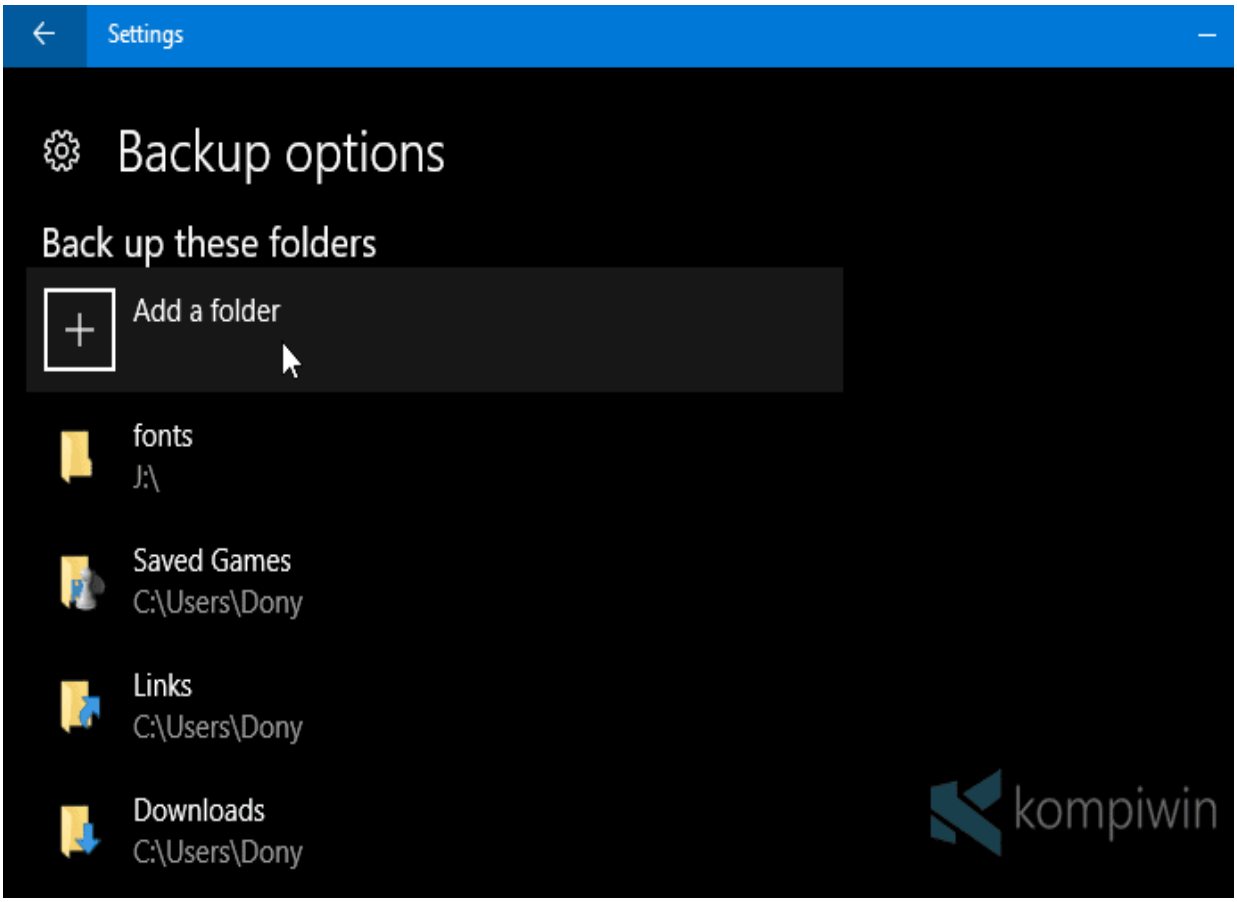


Jika sobat memilih "Until space is needed", File History akan memperingatkan sobat untuk menghapus backup ketika kapasitas sudah terlalu penuh.#5 Cara Memilih Folder yang akan Di-backup

#5 Cara Memilih Folder yang akan di Backup

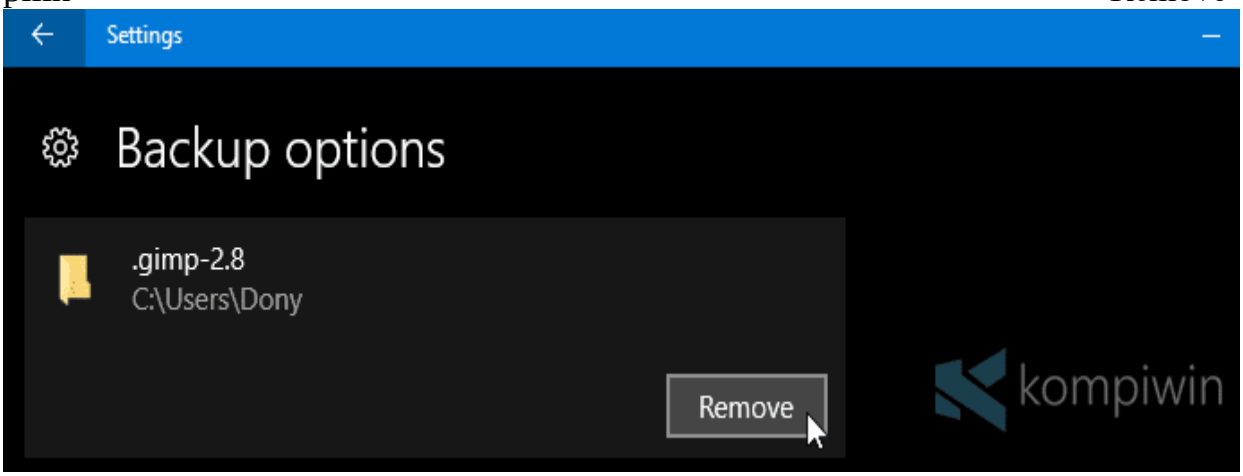
Secara default, File History akan mem-backup secara otomatis semua folder yang terletak di user account sobat (C:Users<nama user>).

Untuk menambah folder yang tak terletak di user account, yang terletak di partisi lain misalnya, klik "Add a folder". Lalu cari dan pilih folder yang hendak ikut di-backup.

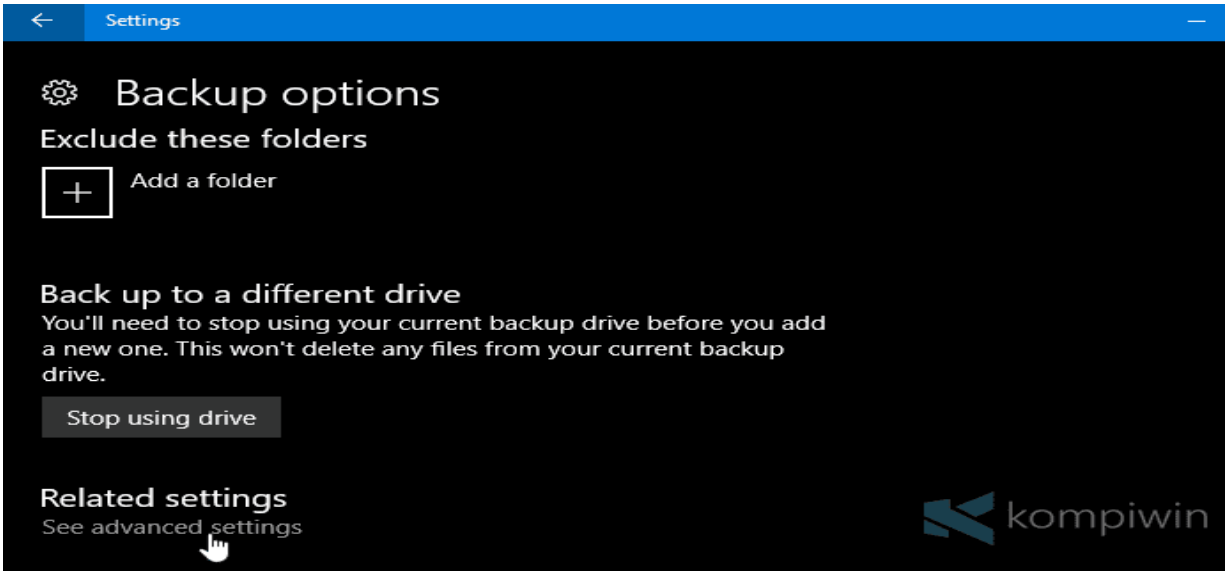


#6 Cara Menghapus Folder agar Tak Ikut Ter-backup

Di bawah tombol "Add a folder", terdapat list dari folder-folder yang hendak di-backup. Untuk menghapus folder dari list backup, klik folder tersebut dan pilih "Remove".



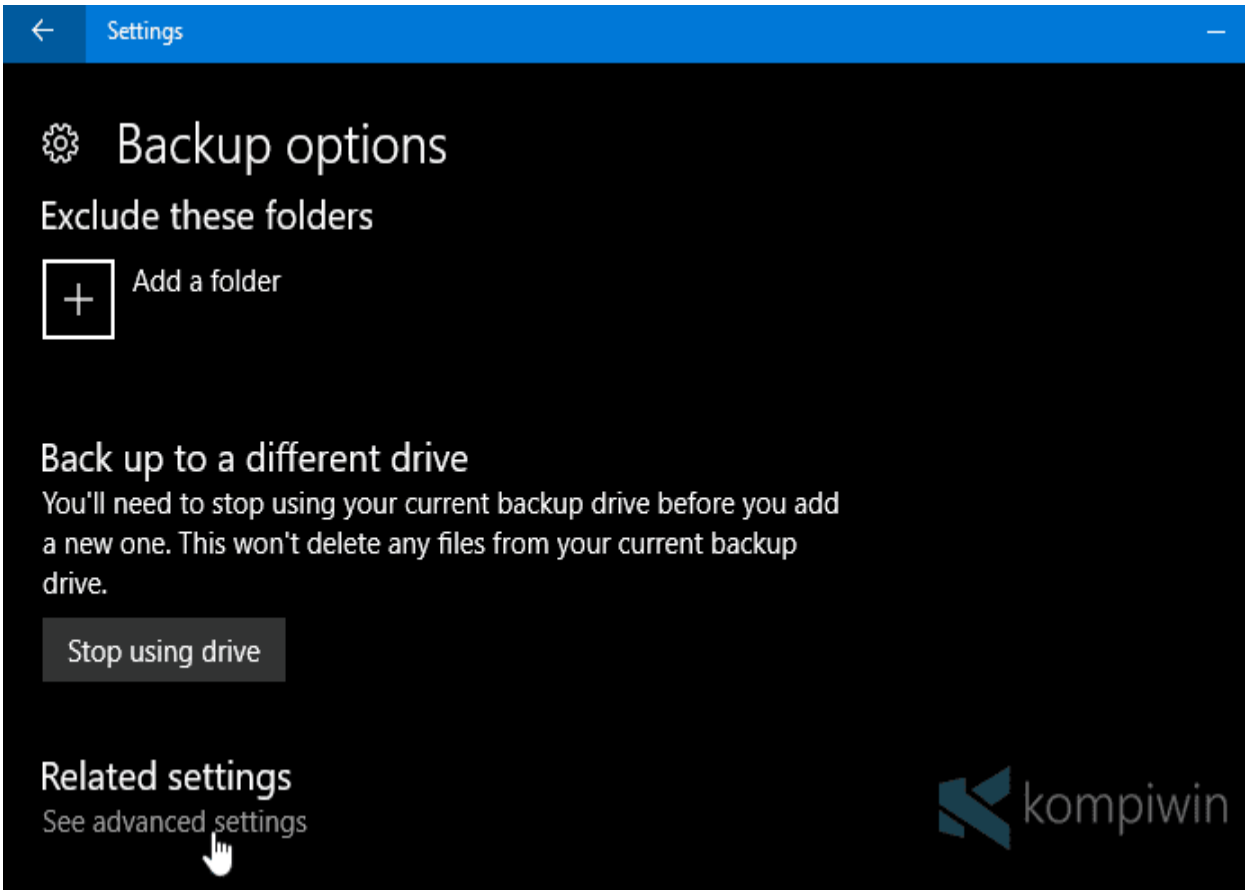
Coba gulir lagi layarnya. Sobat akan melihat "Exclude folder". Fitur itu berfungsi untuk mengecualikan suatu folder agar tidak ikut ter-backup. Misalnya, sobat memilih folder Downloads untuk di-backup, maka sobat dapat memilih sejumlah folder di dalam folder Downloads untuk tidak ter-backup



. #7 Menggunakan Drive yang Lain

Jika sobat merasa kapasitas flashdisk, DVD, atau apa pun sudah terlalu penuh dan tak dapat menampung lagi file-file untuk di-backup, sobat juga dapat menggunakan flashdisk, DVD, atau tempat penyimpanan yang lain untuk menyimpan backup.

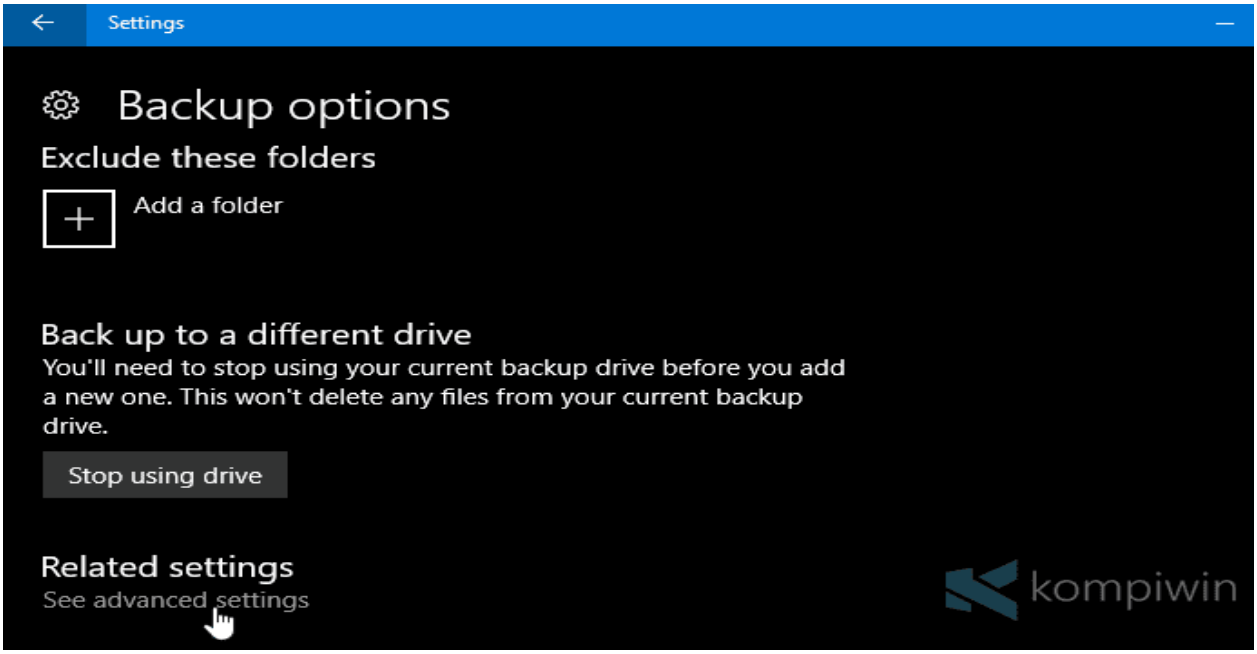
Tinggal klik "Stop using drive". Maka File History akan men-stop proses backup menuju drive tersebut. Lepas drive tersebut dari PC/laptop, lalu colok dan hubungkan drive yang baru ke PC/laptop. Terakhir, klik "Add a drive" untuk menambahkan drive baru tersebut.



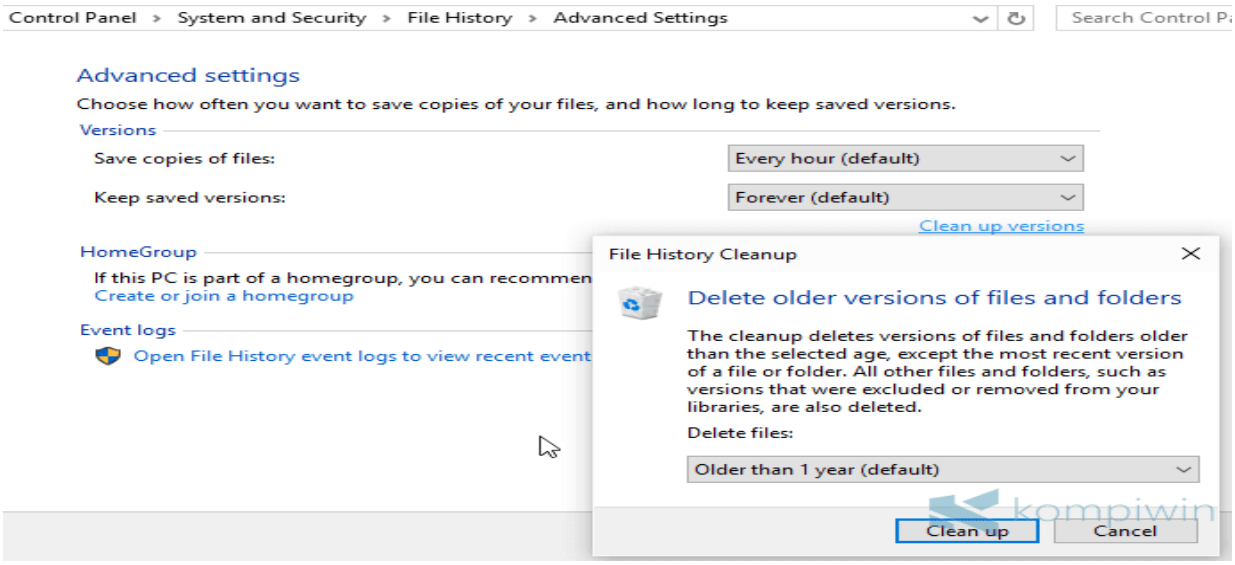
File History tak akan menghapus backup yang telah disimpan di drive lama. Drive yang baru akan berfungsi dengan cara yang sama. Jadi, drive yang baru akan mengulang proses backup dari awal lagi.

#8 Homegroup, Event Logs, Menghapus File Backup

Di bawah, sobat akan melihat "See advanced settings". Klik tombol itu..



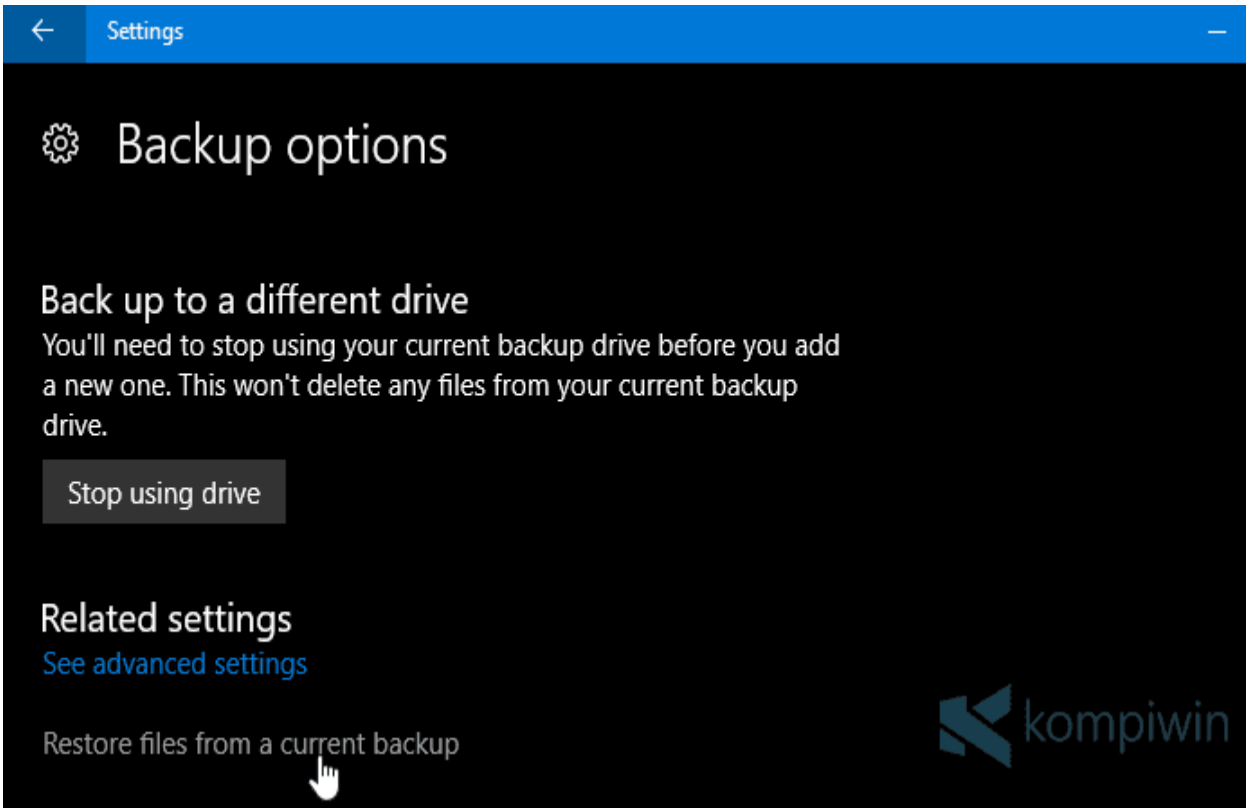
Sobat akan dibawa menuju Control Panel. Di situ, sobat dapat menghapus backup yang telah disimpan dalam jangka waktu yang tersedia, menambah folder dari komputer lain (dalam Homegroup) untuk di-backup, serta melihat event logs.



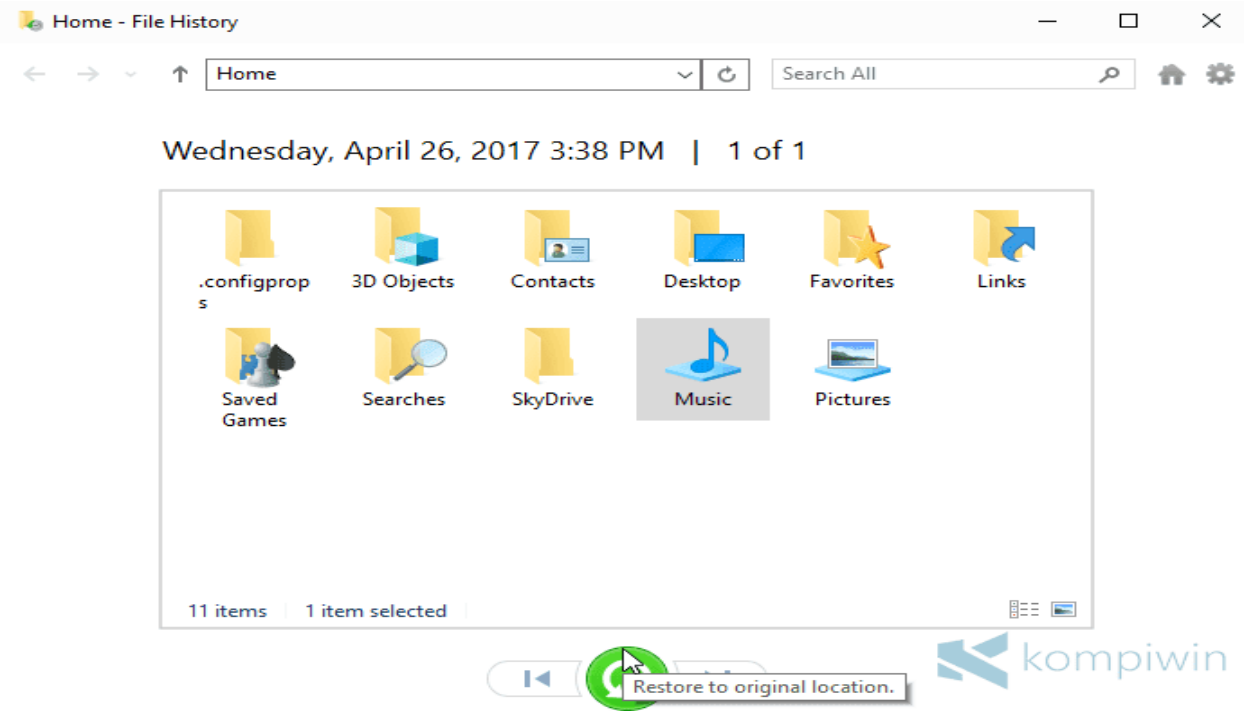
#9 Cara Mengembalikan File yang Telah Di-backup

Kembali ke Settings > Update & Security > Backup > More options.

Gulir layar ke paling bawah, dan pilih "Restore files from a current backup" untuk mengembalikan file-file yang telah di-backup.

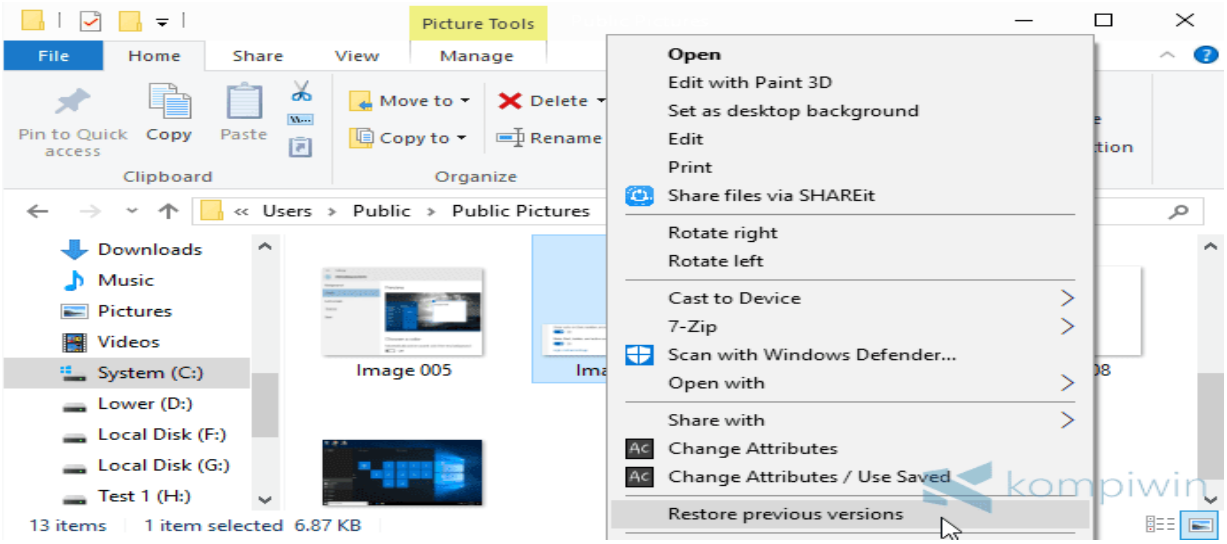


Sobat akan dibawa menuju window yang baru. Di sana terdapat daftar folder-folder yang telah di-backup. Pilih folder-folder yang hendak dikembalikan, dan klik tombol hijau di bawahnya untuk mengembalikan.

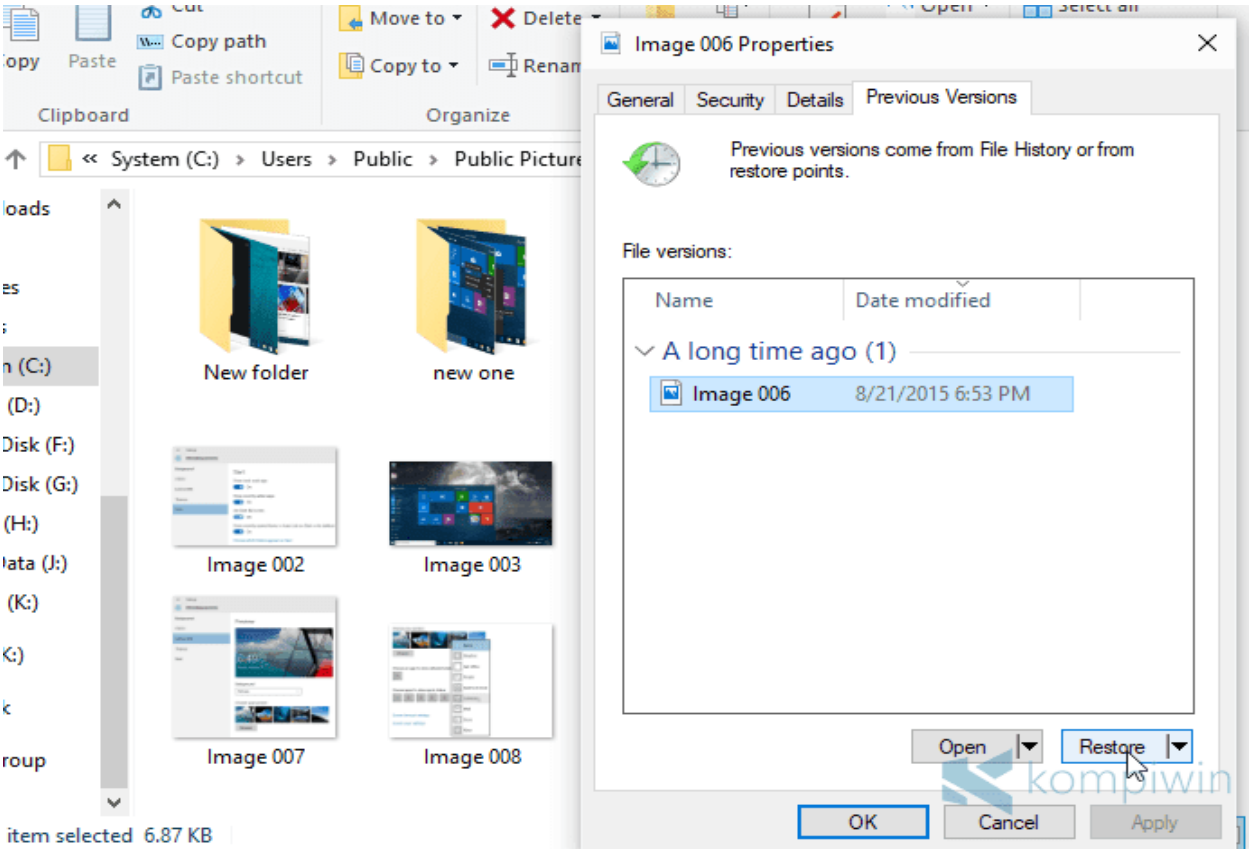


#10 Cara Mengembalikan Versi File dengan File History

Seperti yang saya tulis awal-awal, bahwa File History dapat mem-backup versi-versi file yang dapat sobat kembalikan lagi. Untuk mengembalikan versi suatu file, pergi ke file tersebut dan klik-kanan, lalu pilih "Restore previous version".



Kemudian terbuka kotak dialog baru, yang menunjukkan versi-versi dari file tersebut, yang dapat sobat kembalikan.



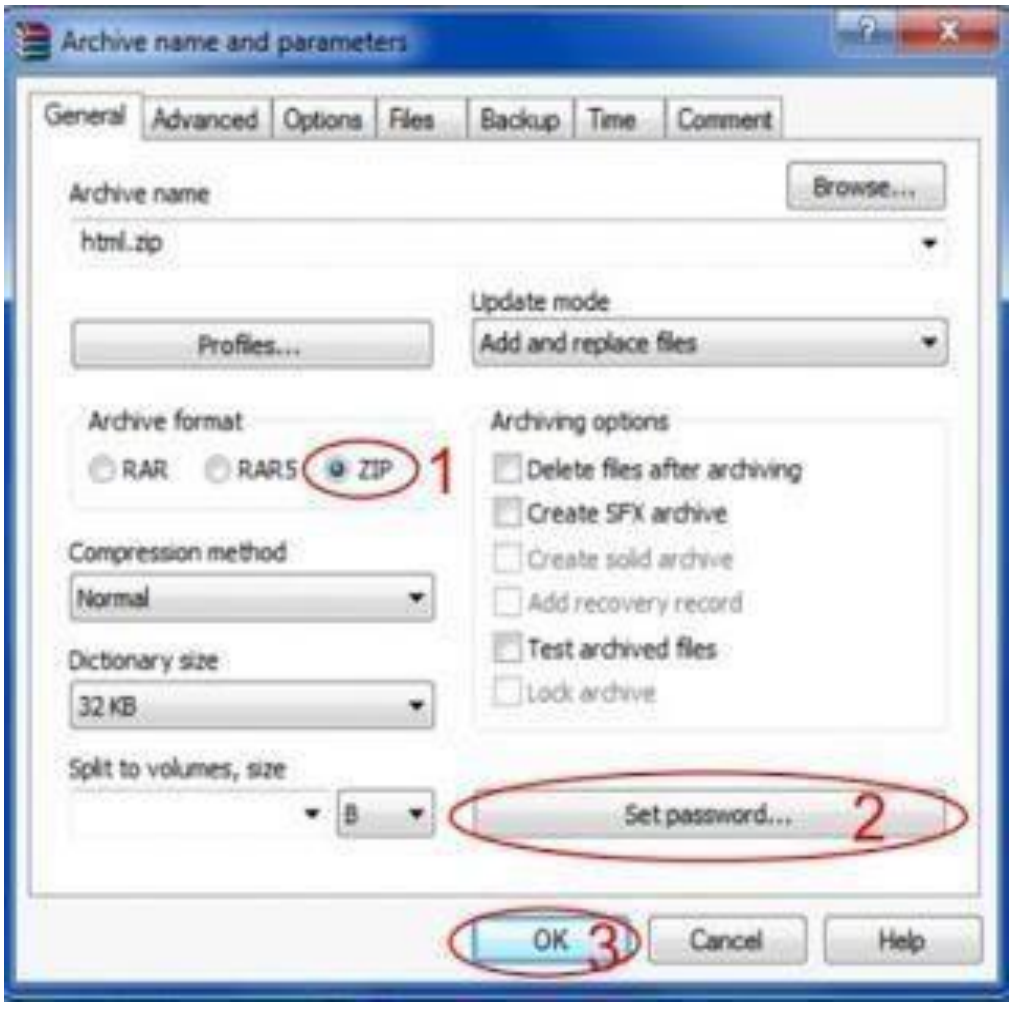
Klik "Restore" untuk langsung mengembalikan versi.

File History tampaknya adalah alat backup yang paling mudah digunakan. Ia gratis, dan merupakan fitur bawaan Windows. Satu-satunya alat dan bahan hanyalah flashdisk, DVD, atau tempat penyimpanan lain untuk menyimpan backup.

File History diluncurkan sejak Windows 8, hingga Windows 10. Jika sobat menggunakan Windows 7, sobat dapat menggunakan System Image Backup untuk mem-backup harddisk secara keseluruhan.

Cara mengamankan data yang berbentuk file atau folder:

- Tempatkan file/folder dilokasi yang sulit dijangkau, tetapi Anda ingat dimana anda meletakkannya.
- Dengan aplikasi WinRar atau WinZip
- Klik kanan folder yang akan diamankan, pilih Add To Archive(Sebelumnya komputer Anda sudah harus diinstal aplikasi WinRar ataupun WinZip)
- Maka muncul kotak dialog Archive name and parameters
- Klik tab Archive Format pilih Zip
- Pilih Set Password. Buatlah password yang unik, susah diketahui tetapi Anda harus mengingatnya.

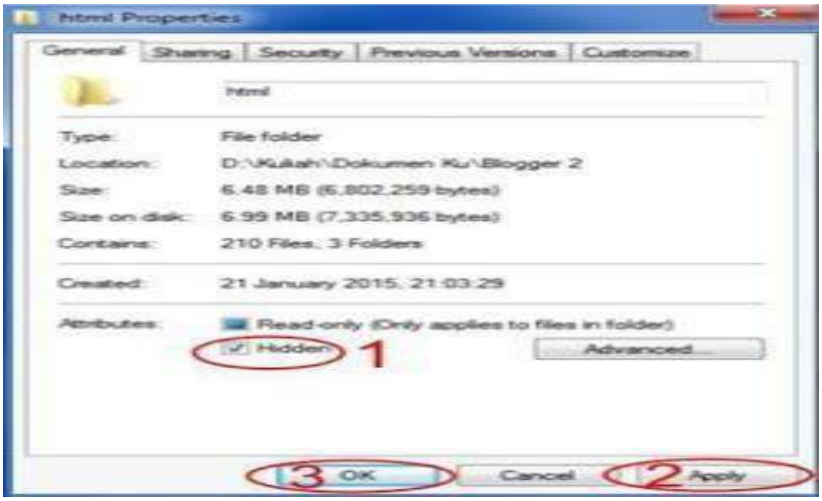


- Klik OK

Cara menghidden ini berarti file atau folder tetap ditempat biasa tetapi tidak terlihat hanya kita yang membuatnya.

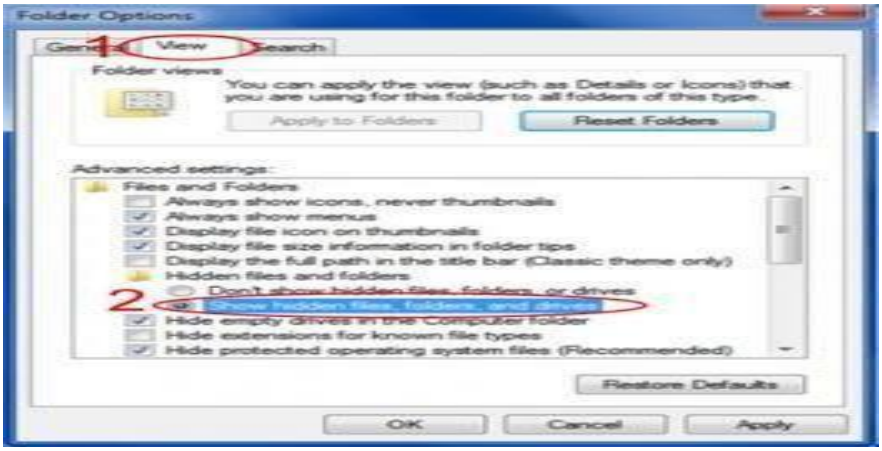
- Klik kanan pada sebuah file atau folder tersebut, pilih properties
- Pada option attributes, cek list hidden
- Klik aplly, kemudian klik OK

Perhatikan gambar berikut ini :



Maka file tersebut akan disembunyikan. Saat ini data anda sudah sangat amankarena diberi perlindungan berlapis. Untuk mengakses data yang disembunyikan taersebut lakukan cara berikut :

- Klik star
- Pilih control panel
- Pilih large icons pada tab view by
- Pilih folder options



- Pada tab view, pilih file hiden files, folder or drivers pada pilihan hidden files and folders seperti pada gambar diatas.

Cybercrime dan Jenis-jenis serangannya?

Cybercrime dalam arti luas (computer related crime atau kejahatan yang berkaitan dengan computer) : setiap perilaku illegal yang dilakukan dengan maksud atau berhubungan dengan system computer atau jaringan , atau singkatnya tindak pidana apa saja yang dilakukan dengan memakai computer (hardware dan software) sebagai sarana atau alat, computer sebagai objek baik untuk memperoleh keuntungan atau tidak, dengan merugikan pihak lain.

Jenis –jenis Serangan Cyber

1. Malware

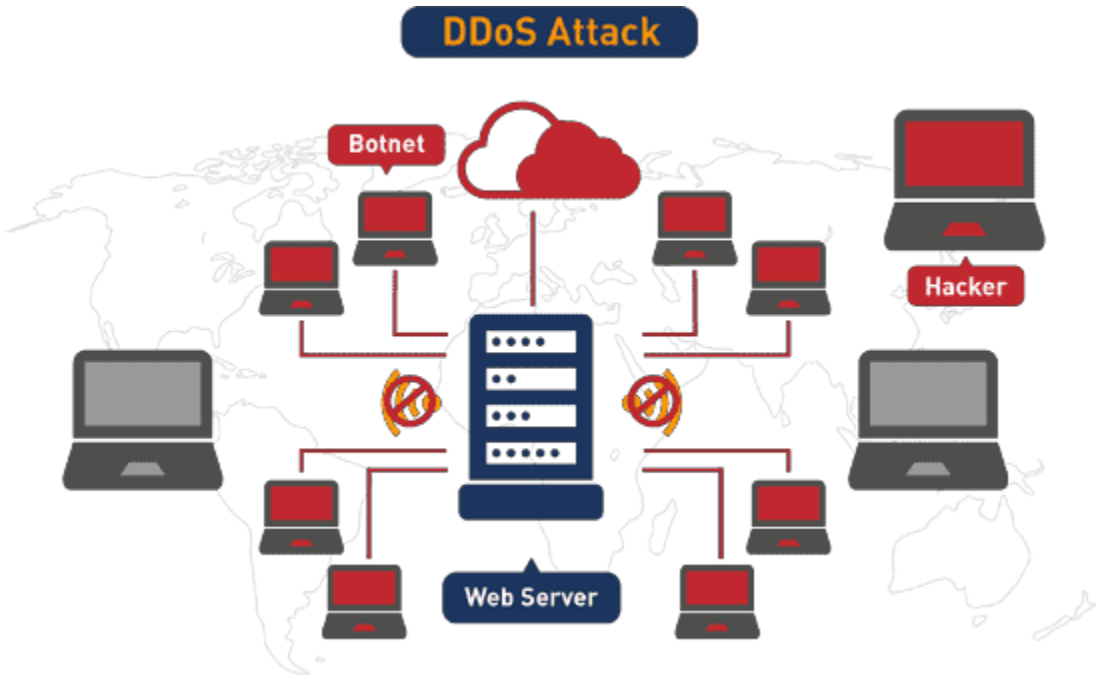
Jenis serangan hacker pertama adalah Malware. Malware merupakan sebutan untuk berbagai perangkat lunak berbahaya termasuk di dalamnya virus dan ransomware. Ketika masuk ke perangkat kalian, malware ini dapat melakukan berbagai hal seperti mengambil alih sistem perangkat kalian, membaca aktivitas kalian selama menggunakan perangkat tersebut dan bahkan mencuri data.

2. Phishing

Phishing merupakan jenis serangan cyber yang bertujuan untuk memperoleh berbagai informasi penting dan sensitif seperti username, password, PIN dan sebagainya. Umumnya phishing ini dilakukan melalui layanan surat elektronik atau email yang di dalamnya terdapat *attachment*.

Nah, ketika membuka *attachment* inilah, para penyerang bisa mencuri informasi penting tersebut dengan memanfaatkan *malware* yang disisipkan dalam *attachment* tadi.

3. DoS (Denial of Service)



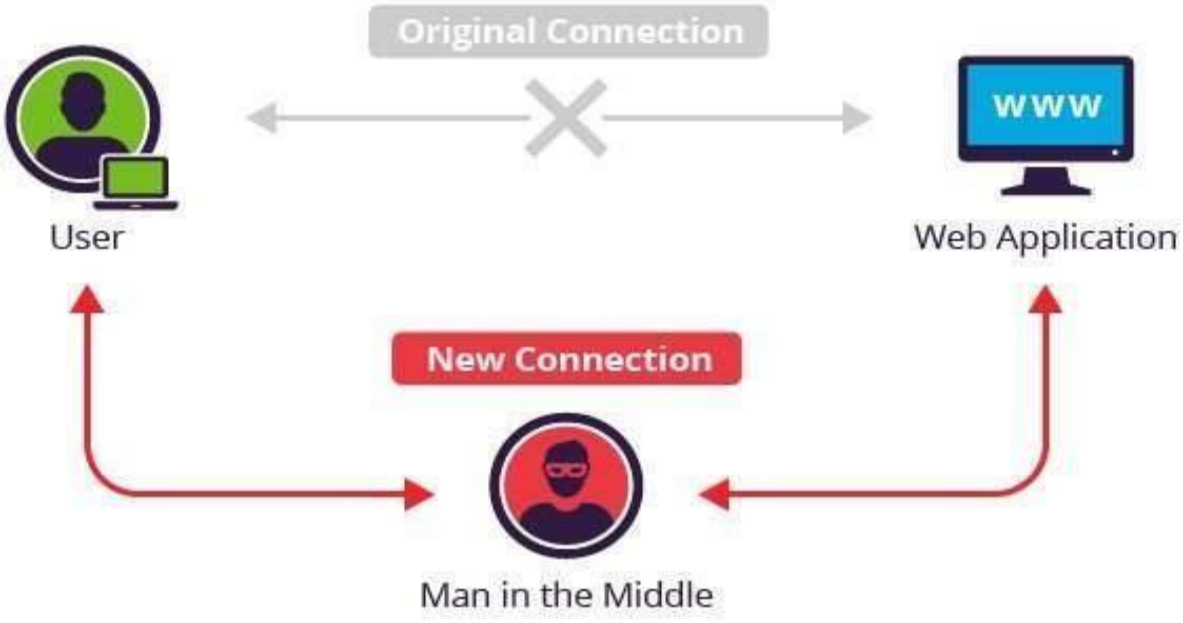
DoS atau Denial of Service merupakan serangan *cyber* yang dilakukan dengan cara mencegah pengguna mendapatkan akses ke suatu situs yang ingin dikunjungi dengan cara menganggu server situs tersebut. Untuk menganggu suatu server, para penyerang akan membanjiri situs tersebut dengan *request* dari banyak sekali komputer sehingga *server* tidak mampu menampung *request*baru lagi.

4. SQL Injection

SQL Injection merupakan jenis serangan cyber di mana para penyerang berusaha mendapatkan akses ke database sistem tersebut. Serangan ini dilakukan dengan memanfaatkan celah keamanan yang ada pada sistem tersebut seperti tidak adanya penyaring untuk berbagai karakter input yang biasa digunakan dalam kode SQL.

Contonhya, para pengguna bisa menggunakan simbol seperti tanda petik, titik koma, =, tanda seru dan lain sebagainya untuk melakukan *dumping* (pengosongan) seluruh data username dan password yang dimiliki suatu situs.

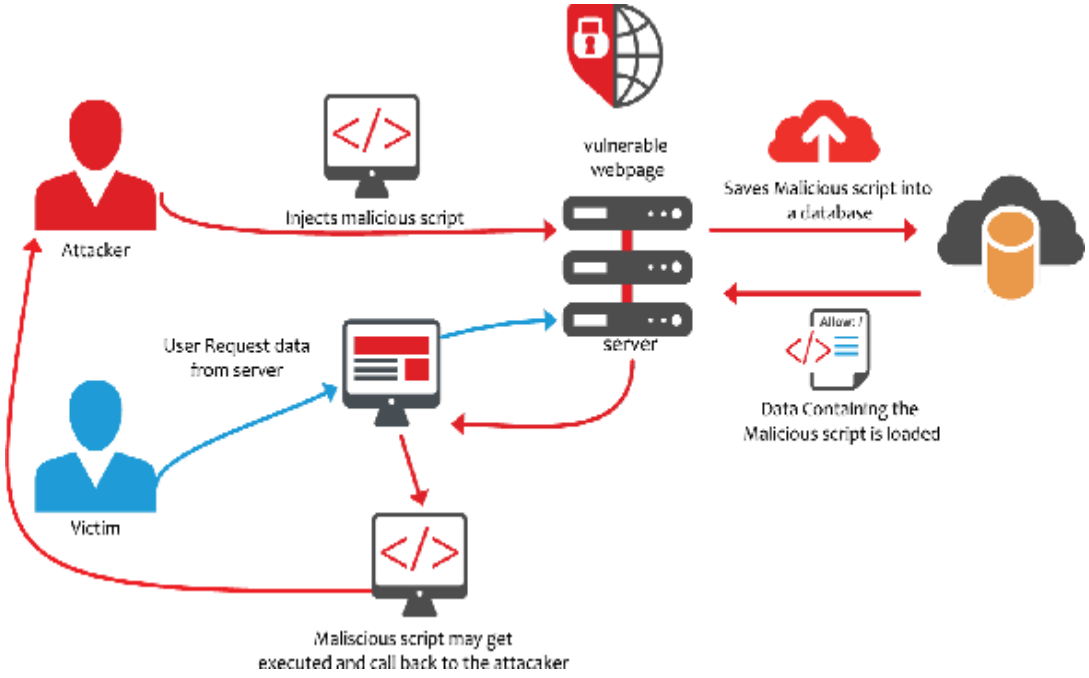
5. Man in the Middle



Man in the Middle merupakan jenis serangan *cyber* di mana para penyerang berada di antara komunikasi antara dua pengguna sehingga para penyerang tersebut dapat mengetahui seluruh informasi yang mengalir antara dua pengguna tadi.

Tentu saja serangan ini berbahaya karena para penyerang dapat mencegat dan memodifikasi informasi yang mengalir serta bahkan bisa menyisipkan *malware* atau semacamnya ke dalam informasi yang mengalir tersebut.

6. Cross-Site Scripting (XSS)



Cross-Site Scripting (XSS) merupakan jenis serangan *cyber* di mana para penyerang menyuntikkan suatu kode tertentu ke suatu *website* terpercaya.

Nantinya, seluruh informasi dari pengguna yang masuk ke *website* tersebut dapat mengalir kepada para penyerang entah itu informasi seperti username, password, PIN dan lain sebagainya.

Selain merugikan korban yang informasinya dicuri, serangan ini juga dapat merusak reputasi suatu *website*.

7. Credential Reuse

Credential Reuse merupakan jenis serangan *cyber* di mana para *hacker* menggunakan ulang berbagai informasi pengguna yang telah mereka dapatkan sebelumnya dengan melakukan berbagai jenis serangan.

Menggunakan ulang di sini maksudnya adalah mereka menggunakan informasi akun A milik pengguna untuk mengakses akun B milik pengguna yang sama.

Hal ini dimungkinkan karena banyak pengguna yang menggunakan username, password dan PIN yang mirip untuk beberapa akun milik mereka.

Email adalah media cepat dan aman untuk mengirim dan

Meskipun Email adalah media cepat dan aman untuk mengirim dan menerima banyak informasi, penting diingat bahwa informasi pribadi anda harus tetap aman dan anda tidak terbuka terhadap virus, phisher maupun hacker. Berikut adalah sejumlah tips keamanan untuk membantu anda tetap aman saat menggunakan email.

1. Jangan menggunakan WARNET / Komputer Publik

Sebaiknya jangan menggunakan WARNET atau komputer yang ada di publi untuk membuka email. Karena di takutkan mereka memasang keylogger yang akan melihat password yang kita ketik.

2. Pilih password yang aman

Ini adalah saran untuk memastikan bahwa saat membuat password untuk akun email anda, pastikan password anda panjangnya minimal delapan karakter. Anda juga melakukan ini dengan menggunakan kombinasi huruf besar dan huruf kecil dan minimal satu angka dan / atau simbol. Hindari penggunaan password yang dapat diprediksi seperti 'password' atau bahkan nama anda, karena ini sering merupakan tebakan pertama bagi peretas / phisher. Selain itu, anda tidak boleh mencoba menggunakan password yang sama di beberapa akun, yaitu menggunakan password yang sama untuk login email dan login bank anda.

3. Ubah password anda secara teratur

Sebagai sebuah rekomendasi, anda harus mengganti password anda setiap 60 hari untuk memastikan akun email anda aman dan ini terutama jika anda secara teratur masuk ke akun email anda di komputer yang tersedia untuk umum.

4. Pastikan logoff & jangan simpan password

Pastikan keluar dari akun anda setelah membaca email anda. Hal ini sangat penting bila anda menggunakan sistem publik seperti di kafe. Anda tidak boleh mengklik tab 'save your password' saat anda menggunakan komputer umum untuk mengakses email anda. Dengan mengklik save, ini menyimpan

password anda dan membuat anda tetap masuk bahkan setelah anda logoff dari sistem, sehingga memungkinkan pengguna lain mengakses akun anda.

5. Hindari email spam

Jangan membuka email yang dikirim oleh seseorang yang tidak anda kenal atau percaya. Ikuti naluri anda! Laporkan pesan sebagai spam atau drag ke junk dan lanjutkan. Anda seharusnya tidak pernah membalas email semacam itu atau mengklik tautan di dalamnya karena dengan melakukan salah satu dari itu atau bahkan delisting dari email semacam itu, anda akan memberi tahu pengirim (phisher) bahwa email anda aktif untuk menerima lebih banyak email spam.

6. Safe sender

Dengan membuat daftar pengirim yang aman, anda dapat yakin bahwa hanya email yang aman yang akan masuk ke dalam kotak inbox anda. Ini hanya akan memungkinkan alamat email orang yang anda kenal dan percaya untuk memasukkan kotak inbox Anda. Setiap pengirim lain yang tidak ada dalam daftar anda akan secara otomatis masuk di folder junk anda.

7. Jangan berbagi data pribadi

Jika anda menerima korespondensi yang mengklaim berasal dari bank anda, sebaiknya anda menelepon cabang bank anda untuk mengkonfirmasi dan membicarakan masalah ini melalui telepon. Jangan pernah membagi informasi rahasia seperti password, rincian data bank, dan nomor e-KTP melalui email. Selalu ingat bahwa setiap kali anda mengirim pesan email, anda telah kehilangan kendali atas apa yang dilakukan dengan hal itu atau terhadap siapa pesan itu didapat.

8. Perangkat Lunak Antivirus

Pastikan anda telah menginstal perangkat lunak antivirus dan selalu selalu memperbaruinya. Norton, McAfee, Kaspersky adalah alternatif yang baik untuk mengamankan PC, Mac, Androids, dan perangkat iOS anda dari virus, spyware, malware & phishing.

9. Gunakan email yang berbeda

Jangan gunakan alamat email yang sama untuk penggunaan pribadi dan umum. Siapkan akun email kedua untuk mendaftar ke situs web publik seperti situs belanja online, dan mendaftar ke layanan baru seperti buletin. Ini akan membatasi jumlah spam (seperti yang tidak dapat dihindari) yang akan diterima oleh akun email pribadi anda.

10. Update web browser tepat waktu

Sebaiknya perbarui browser web anda dari waktu ke waktu karena pembaruan keamanan sering kali diperkenalkan ke browser web terbaru, sehingga mencegah serangan berbahaya pada akun email. Google Chrome sering dianggap sebagai salah satu browser web yang paling aman yang tersedia.

Tips berkomputer sehat

Walaupun tingkat kecelakaan saat bekerja di depan komputer sangat kecil atau bahkan bisa dibilang tidak ada, tetapi jika aspek kesehatan dan keselamatan kerja K3 dalam penggunaan komputer tidak diperhatikan, tidak mustahil jika kita akan mengalami kecelakaan saat bekerja di depan komputer.

1. Gunakan kursi yang secara dinamis dapat diatur tinggi-rendah dan senderan punggungnya .
2. Posisi monitor bagian paling atas setidaknya setinggi 5-8 cm di atas arah pandang mata .
3. Untuk menghindari efek silau dari layar monitor, bisa gunakan filter atau pelindung anti-silau .
4. Duduklah dengan jarak sekitar satu rentangan tangan dari monitor.
5. Kaki harus dapat menjejak pada lantai atau pada pijakan kaki yang stabil.
6. Jika menggunakanalat pemegang/penjepit dokumen, tingginya samakan dengan layar monitor .
7. Antara siku dan pergelangan tangan sejajar dan lurus saat menggunakan keyboard / mouse .
8. Lengan dan siku berada dalam posisi santai dekat dengan tubuh Anda .
9. Monitor dan keyboard posisikan di tengah hadapan Anda .
10. Gunakan keyboard yang memiliki bagian pengungkit di bawahnyauntuk mengatur posisi .
11. Gunakan alas kerja atau meja yang stabil dan tidak goyah .
12. Sesekali lakukan istirahat pendek dengan berdiri .

Komputer kantor biasanya digunakan oleh banyak orang dan tidak hanya untuk pekerjaan kantor, komputer kantor juga biasanya digunakan untuk kepentingan pribadi. Apalagi jika komputer kantor tersebut dilengkapi dengan fasilitas internet. Pasti sering digunakan untuk berselancar di internet. Bagaimana cara kita agar tetap aman dan nyaman dalam menggunakan komputer kantor? Supaya terhindar dari hal-hal yang tidak diinginkan, berikuti tips yang harus diperhatikan oleh penggunaan komputer kantor.

1. Bersihkan atau Hapus Jejak: Hal yang paling sering terjadi adalah Lupa log out atau keluar dari akun pribadi seperti email, media sosial, maupun akun pribadi lainnya yang bisa berakibat buruk. Selain data pribadi Anda akan terekspos bebas, keadaan seperti ini sering mengundang tangan-tangan jahil. Teman yang jahil bisa memainkan status jejaring sosial Anda, membaca pesan-pesan Anda, atau melakukan hal-hal lain yang tidak menyenangkan. Selama menggunakan fasilitas kantor, jangan pernah mencentang atau menyetujui pilihan untuk mengingat kata sandi atau password demi keamanan data Anda. Untuk membersihkannya kamu bisa menggunakan CCleaner atau sejenisnya.
2. Atur Berkas: Bersifatlah profesional. Jangan menggabungkan berkas kantor dengan berkas pribadi. Usahakan file-file pribadi tersimpan dengan baik dalam folder yang tidak mudah ditemukan dan tidak

bercampur dengan file kantor. Jika menyimpan berkas yang sifatnya rahasia dan pribadi, gunakan kata sandi. Lebih baik lagi, gunakan alat penyimpan data seperti harddisk eksternal atau flashdisk.

3. Etika dan peraturan: Pahami peraturan penggunaan elektronik dan aktivitas digital pada perusahaan Anda. Beberapa perusahaan punya peraturan yang keras tentang apa yang boleh dan tidak boleh dilakukan ketika menggunakan email resmi kantor.
4. Ilegal: Hindari membuka website terlarang seperti tempat download ilegal atau pornografi. Gunakan fasilitas kantor untuk kepentingan pekerjaan. Selain sangat mencoreng reputasi, jika diketahui oleh atasan, kegiatan ini bisa membuat Anda berisiko dipecat. Kepercayaan yang sudah diberikan kepada Anda dalam bentuk pekerjaan dan fasilitas sebaiknya dijaga baik-baik untuk kebaikan Anda sendiri.
5. Keamanan: Jangan membuka internet banking atau fasilitas sejenis komputer bersama. Walaupun sudah banyak protokol keamanan untuk menjaga data, tapi tetap saja Anda harus berhati-hati. Begitu juga dengan penggunaan kartu kredit untuk belanja online. Sebisa mungkin hindari memasukkan data-data sensitif kartu kredit Anda pada komputer bersama. Lebih baik bermain aman daripada menyesal belakangan.
6. Untuk komputer yang digunakan bersama, usahakan untuk tahu diri dan tidak berlama-lama menggunakan komputer saat ada teman yang menunggu. Selalu tinggalkan fasilitas komputer dalam keadaan bersih dan pastikan keyboard komputer yang ditinggalkan tidak lengket karena bekas makanan atau keringat.

Pengaruh Perilaku Karyawan dan Keamanan Informasi

Dalam berbagai penelitian dibidang keamanan informasi, terungkap bahwa celah terbesar selama ini adalah manusia itu sendiri. Adanya kecerobohan, tidak mengikuti SOP dengan benar, dan lingkungan sangat berpengaruh besar terhadap kinerja SDM tersebut terhadap kelangsungan aktivitas operasional perusahaan. Berikut ini adalah kecerobohan karyawan dalam hal keamanan informasi :

1. Menggunakan post-it-note, untuk menyimpan password atau username.
2. Meninggalkan komputer dalam keadaan menyala.
3. Membuka email attachments.
4. Pemilihan password yang buruk.
5. Anda lebih tahu dari mereka.
6. Laptop punya kaki.
7. Sakit hati seorang karyawan.
8. Keceplosan berbicara.
9. Penegakan security policy yang lemah atau tidak tegas.

Berikut adalah tips dalam menggunakan wifi gratis (wifi yang tidak memerlukan kata sandi)

-Tidak melakukan hal-hal yang sifatnya pribadi, seperti transaksi online aktivitas perbankan.

Jangan Percaya pada jaringan WiFi yang tidak memerlukan kata sandi untuk terhubung kejaringan, karena para penjahat syber umumnya membuat jaringan seperti itu guna melacak data pribadi pengguna.

-Matikan WiFi pada saat anda tidak menggunakannya. Selain untuk mencegah terkoneksi secara langsung ke Jaringan Wifi yang sebelumnya tersimpan juga dapat menghemat daya baterai perangkat anda.

-Ketika anda menggunakan WiFi gratis, hindari untuk membuka akun perbankan atau layanan layanan penting lainnya yang terdapat informasi akun sensitif anda. Lebih baik gunakan koneksi Data Mobile pribadi.

-Penggunaan VPN (Virtual Private Network) dapat menjadi pertimbangan karena sistem VPN tersebut akan menenkripsi data – data yang di kirim sehingga dalam perjalanan data – data tersebut tidak akan terlihat.

-Gunakan Antivirus. Menggunakan antivirus dapat membantu mendeteksi beberapa kemungkinan keanehan yang akan muncul ketika terhubung dengan jaringan internet.

-Selalu log in log out

CARA MENGGUNAKAN MEDIA SOSIAL DENGAN BIJAK

1. Filter Pertemanan

Hampir semua media sosial memiliki fitur untuk menfilter siapa saja yang bisa berteman dan mengikuti kita. Misalnya di Instagram, Anda bisa mengaktifkan mode akun private. Hal ini akan membatasi Informasi yang dapat di akses publik tentang diri Anda.

2. Pasang Foto Profil Sewajarnya

Foto adalah hal pertama yang akan di lihat orang lain, selain untuk mengidentifikasi itu memang akun Anda, foto juga dapat menyebabkan orang lain bisa dengan mudah menilai diri Anda. Misalnya ketika Anda memasang foto yang tidak enak di lihat, lalu bayangkan apa yang ada dipikiran orang lain tentang foto tersebut.

Tidak hanya foto profil, foto-foto yang Anda bagikan di media sosial juga akan demikian. Bisa saja orang yang tak bertanggung jawab menyimpan foto Anda tersebut, dan digunakan untuk hal-hal yang tidak baik.

3. Pikir Duhulu sebelum Membuat Status

Hal ini mungkin terlihat simple namun cukup berdampak bagi diri kita sendiri. Kebanyakan dari kita seolah tak memikirkan lebih dulu apa yang hendak kita tulis di status media sosial, atau bahasa kerena ‘‘asal ceplas-ceplos’’. Bisa saja kan status kamu dapat menyinggung bahkan menyakiti perasaan orang lain, tentu hal ini tidak baik untuk kita lakukan. Maka sebelum membuat status, pikirkan terlebih dahulu ‘‘Apa yang hendak kamu tulis, apa tujuannya, dan apa dampaknya’’. Jangan sampe status kamu menjadi bumerang kamu sendiri di kemudian hari.

4. Publish Informasi Seadaanya, jangan Bersifat Pribadi

Memberikan informasi tentang identitas diri dirasa tidak ada masalahnya. Namun akan menjadi masalah jika kamu memberikan informasi yang bersifat sangat pribadi. Seperti nomor telepon, alamat rumah, dan informasi penting lainnya. Bukan mengajarkan berpikiran negatif, namun bisa saja informasi penting tersebut menjadi celah yang bisa di manfaatkan orang-orang yang tak bertanggung jawab untuk berbuat kejahatan.

5. Bijak Membagikan Konten

Kita bisa menganggap bahwa semua yang ada di media sosial itu 100 persen adalah konten, baik video, status, dan gambar, itu semua termasuk konten juga. Nah dari hal itu, apakah kamu pernah membagikan konten orang lain di media sosial milikmu ? jawabannnya mungkin pernah. Jika pernah. Mungkin Anda harus lebih bijak untuk membagikan konten-konten di media sosial kedepannya. Karena jika Anda justru membagikan konten yang negatif, misalnya, profaganda, SARA, rasis, makar, dan sebagainya. mungkin Anda akan terlihat setuju, mendukung, atau mengakui tentang konten tersebut.

Daripada membagikan konten-konten yang gak jelas, lebih baik kamu membagikan konten-konten yang positif, misalnya konten yang bisa mendidik, atau konten yang bisa menambah pengetahuan.

6. Bijak Memilih Informasi Yang di Dapatkan

Banyak sekali informasi yang akan kita dapat di media sosial. Dan tak menutup kemungkinan. setengah dari informasi yang kita dapat adalah informasi yang hoax. Maka dari itu, selektif lah untuk memilah-milah informasi di media sosial. Jangan mudah percaya informasi yang belum jelas sumbernya.

7. Jangan Suka Pamer

Salah satu yang paling menyebalkan di media sosial adalah ketika kita melihat seseorang membuat status yang terkesan mau pamer. Ya, sesekali pamer juga tidak ada masalah, terkadang berbagi semua pencapaian dan prestasi dengan maksud bisa memotivasi orang lain adalah salah satu hal yang positif juga.

Namun hal positif itu mungkin bisa berubah menjadi negatif jika kata "pamer" itu menimbulkan kesan merendahkan orang lain, terlihat sombong, dan terlihat paling istimewa sendiri. Ya mungkin orang-orang itu dalam hidupnya sedikit sekali mendapatkan sebuah "Pujian", atau mungkin hidup mereka tak bahagia sehingga mencari kebahagiaan di dunia "Virtual".

Tak perlu memaksakan diri mendapatkan pengakuan dari orang lain kok, karena orang yang benar-benar tulus menyayangi Anda tak butuh semua pengakuan tersebut. Oleh karena itu, hindarilah membuat status-status yang terkesan mau pamer.

8. Jangan Oversharing/Spamming

Buatlah kesan kepada teman-teman media sosial bahwa kamu bukanlah orang yang suka "nyampah". Walaupun kita semua berhak memposting apapun di media sosial, namun kalo terlalu oversharing "setiap yang dilakukan harus dikatakan semua", mungkin hal itu tidaklah baik. Sebab akan membuat Anda jadi tidak menarik lagi di mata orang lain. Jangan sampai Anda dicap sebagai orang "lebay".

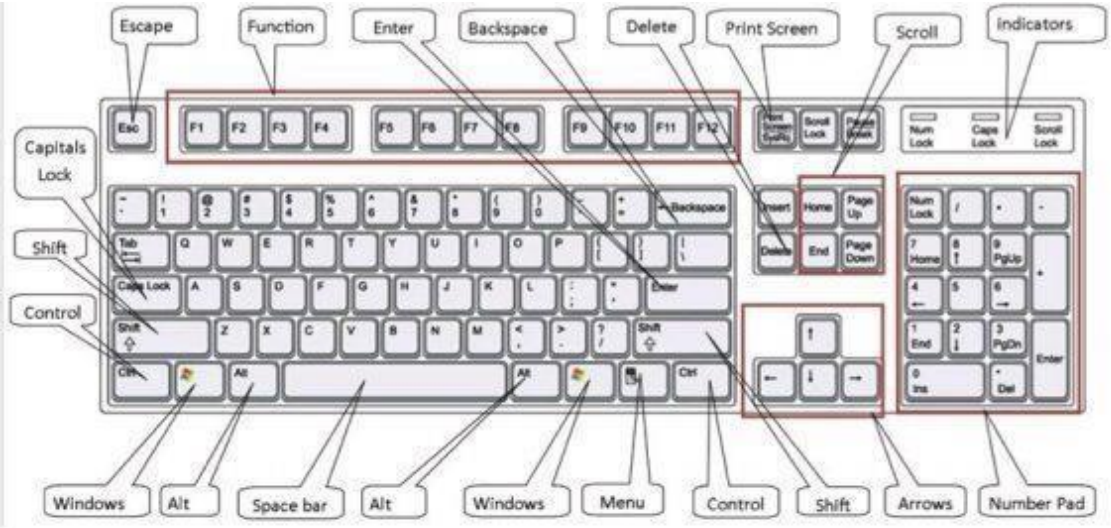
Dan lagi, jangan berpikiran ketika melihat beranda sosmed seseorang yang terlihat sepi seperti "kuburan" itu sama sekali tidak ada yang istimewa yang dapat mereka bagikan. Karena bisa jadi kehidupan di dunia "nyata-nya" lebih bahagia daripada dunia "virtual-nya". So, hindari Oversharing dan Spamming.

9. Selalu Punya Etika Saat Berinteraksi di Sosmed

Selanjutnya adalah menjaga etika saat berinteraksi di media sosial. Diantara kita mungkin sering memberikan komentar pada sebuah postingan di media sosial. Nah kalo iya, usahakan komentar tersebut masih dalam koridor yang wajar. Hindari menyindir dan hormati perasaan orang lain, kemudian, tidak usah mengeluarkan kata-kata yang kasar, meskipun tak saling mengenal. Itu karena komentar kamu akan di lihat oleh publik.

10. Interaksi Seperlunya Saja

Batasi interaksi di media sosial seperlunya saja, baik itu berkomentar, percakapan, atau memberikan sebuah like. Hormati privacy orang lain, lebih baik kita "cukup tahu saja" daripada membuat orang lain merasa tidak nyaman.



Fungsi Tombol Keyboard Pada Ms.Word

- Ctrl + A : Tombol Select All (Memilih Semua Kolom Ms Word)
- Ctrl + B : Menebalkan Huruf dan Karakter Angka pada Ms Word
- Ctrl + C : Menyalin atau MengCopy
- Ctrl + D : Pilihan Font Pada Ms Word
- Ctrl + E : Membuat Center Alignment (Rata Tengah Tulisan pada Ms Word)
- Ctrl + F : Mencari Karakter (Find Karakter)
- Ctrl + G : Go To
- Ctrl + H : Menggantikan (Repleace)
- Ctrl + I : Membuat Tulisan Menjadi Miring (Italic)
- Ctrl + J : Membuat Tulisan Menjadi Rata Kiri Kanan(Justify Aligment)
- Ctrl + K : Membuat Hyperlink (Insert Hyperlink)
- Ctrl + L : Membuat Tulisan Menjadi Rata Kiri (Left Aligment)
- Ctrl + M : Increase Ident
- Ctrl + N : Membuat Sebuah File Baru (New File)
- Ctrl + O : Membuka File (Open File)
- Ctrl + P : Printah Cepat untuk Melakukan Print
- Ctrl + Q : Mengubah Pengaturan Style Menjadi Normal
- Ctrl + R : Membuat Tulisan Menjadi Rata Kanan (Right Alignment
- Ctrl + S : Printah Untuk Menyimpan File (Save / Save As)
- Ctrl + T : Hanging Ident
- Ctrl + U : Membuat Tulisan Menjadi Garis Bawah (Underline)
- Ctrl + V : Mempaste Tulisan Yang Sudah Di Copy Dengan (Ctrl + C)
- Ctrl + W : Menutup Menu Word (Close Ms.Word)
- Ctrl + X : Memotong Tulisan Yang sudah Di Block
- Ctrl + Y : Mengembalikan Sesudahnya (Redo)
- Ctrl + Z : mengembalikan Sebelumnya (Undo)
- Ctrl + 1 : Membuat Sebuah Spasi Single (Single Spacing)
- Ctrl + 2 : Membuat Sebuah Spasi Double (Double Spacing)
- Ctrl + 5 : Membuat Spasi 1.5 Lines

fungsi tombol pada keyboard komputer yang khususnya seperti berikut.

- F1 : Membuka Sebuah Fungsi Bantuan pada Komputer anda.
- F2 : Mengubah Nambah File atau Berkas (Rename)
- F3 : Perintah Auto Text (Find Text)
- F4 : Pengulangan Printah Sebelumnya/
- F5 : Perintah Temukan (Find) Ganti (Replace) atau Go To
- F6 : Membuka Pengaturan Other Pane
- F7 : Membuat Perintah Spelling (Pengecekan Penulisan)
- F8 : Membuka Perintah Awal Untuk memilih (Coret Text atau Objek)
- F9 : Memperbaruhi Field (Mail Marge)
- F10 : Membuat Sebuah Menu menjadi Aktif
- F11 : Membuat Sebuah Masukan Field berikutnya (mail Marge)
- F12 : Membuka Dialog Save As (Simpan Sebagai)
- Esc : Tombol Perintah Membatalkan Dialog
- Enter : Tombol Untuk Mengahiri satu paragraf atau Melaksanakan Perintah / Pilihan
- Tab : Memposisikan Teks sesuai dengan tanda Ruler Horizontal
- Windows : Tombol untuk Membuka Start Menu
- Shorcut : Tombol untuk mengaktifkan Shorcut di posisi kursor
- Delete : Tombol untuk Menghapus Sebuah Karakter dari Kanan Pada Penulisan anda
- Backspace : Tombol untuk Menghapus Sebuah Karakter dari Kiri Pada Penulisan anda
- Insert : Tombol Untuk menyisipkan karakter pada Posisi Kursor Anda.
- End : Tombol Untuk memindahkan Posisi Kursor ke akhir baris.
- Home : Tombol Untuk memindahkan Kursor ke awal baris
- Page Up : Tombol Untuk Menggulung Layar ke atas
- Page Down : Tombol Untuk Menggulung Layar ke bawah
- Up : Tombol Untuk memindahkan Kursor 1 ke baris atas
- Down : Tombol Untuk memindahkan Kursor 1 ke baris bawah
- Left : Tombol Untuk memindahkan Kursor 1 ke Kiri
- Right : Tombol Untuk memindahkan Kursor 1 ke Kanan
- Num Lock On : Tombol Untuk Mengaktifkan Fungsi Angka dan Operasi matematik
- Shift + F10 : Tombol Untuk membuka Menu Pintas.
- Alt : Tombol ini jika tidak di Kombinasikan maka hanya akan berfungsi sebagai memulai / mengaktifkan menu bar.
- Shift + Delete : Tombol ini untuk menghapus file Secara permanent serta tidak akan masuk ke *Recyle bin* terlebih dahulu
- Ctrl + Right Arrow : Tombol ini Berfungsi Untuk Memindahkan titik sisipan ke awal kata berikutnya