BAWASLU
BADAN PENGAWAS PEMILIHAN UMUM

# BUKU PANDUAN

# KEBERSIHAN SIBER

• • •

## PEMILIHAN KEPALA DAERAH (PILKADA) 2020

# KATA PENGANTAR BUKU PANDUAN KEBERSIHAN SIBER

*Assalamulaikum,*

Salam sejahtera untuk kita semua.

Seluruh pelaksanaan tugas dan fungsi Bawaslu membutuhkan data dan informasi untuk melakukan kajian dan penyusunan kebijakan. Data dan informasi yang dikelola Bawaslu sebahagian besar merupakan informasi publik. Ketersediaan data dan informasi yang terintegrasi akan membuat pendokumentasian data menjadi lebih baik dan simpang siur data dapat dicegah sehingga pelayanan kepada masyarakat semakin Baik.

Pendokumentasian dan pelayanan data dan informasi ke publik membutuhkan sarana dan prasarana penunjang yang memadai termasuk siber atau sistem komputer dan informasi yang harus dipastikan kehandalan dan keamanannya. Kehandalan dan keamanan siber Bawaslu tidak terlepas dari perilaku dan kebiasaan sehari-hari setiap Pegawai Bawaslu atau pihak lain yang mendapat akses ke internet Bawaslu.

Perilaku dan perlakuan kita dalam menggunakan komputer dan internet tanpa kita sadari berpotensi membuka celah masuknya pihak-pihak yang tidak bertanggungjawab dan dapat merusak atau bahkan merusak data dan informasi yang ditampilkan Bawaslu di media sosial dan website.

Buku Panduan Kebersihan ini diharapkan tidak sekedar memberikan pengetahuan terkait kebersihan siber dalam memberikan keamanan di Bawaslu, akan tetapi juga mengubah perilaku kita untuk lebih berhati-hati dalam bertindak di dunia siber.

**Fritz Edward Siregar**
**Koordinator Divisi Hukum, Humas dan Datin**

# BAWASLU

## Buku Panduan Kebersihan Siber

### Pemilihan Kepala Daerah (PILKADA) 2020

Materi Pendamping Pelatihan Kebersihan dan Kesadaran Siber Bawaslu

# PENGANTAR

Selama beberapa tahun terakhir, gangguan dari luar dan serangan siber untuk mendelegitimasi proses pemilu telah berlipat ganda dan menjadi ancaman global bagi negara-negara demokratis. Seiring dengan meningkatnya ancaman siber A yang mengancam integritas pemilu, sangat penting bagi lembaga penyelenggara pemilu untuk mengembangkan strategi keamanan siber untuk melindungi diri lembaganya, penggunanya, dan proses pemilu secara keseluruhan.

Indonesia pernah mengalami beberapa insiden siber kepemiluan di masa lalu, meskipun tidak satupun yang menjadi ancaman serius bagi Pemilu, adalah sebuah kepastian bahwa penyerang, baik itu dari dalam maupun luar negeri, akan mencoba kembali menggunakan serangan siber terhadap KPU dan Bawaslu pada tahun 2020 dan di masa yang akan datang.

Banyak lembaga yang telah berinvestasi pada perangkat teknologi keamanan siber. Hal tersebut adalah sesuatu yang penting dan perlu, akan tetapi meminimalkan kesalahan yang dilakukan oleh manusia adalah sebuah faktor yang tanpanya terciptanya keamanan siber tinggalah sebuah ilusi.

Sebagian besar insiden keamanan siber disebabkan oleh faktor manusia: pengguna yang mengabaikan aturan keamanan yang sederhana merupakan faktor utama yang membuka jalan bagi sebagian besar serangan siber.

**Buku pedoman ini diperuntukkan bagi semua staf Bawaslu, berisi pedoman dan rekomendasi tentang sikap dan praktik yang aman untuk melindungi akun-akun pribadi maupun profesional mereka, serta organisasi tempat mereka bekerja secara keseluruhan.**

Ancaman keamanan siber menyerang semua bidang usaha terlepas dari ukurannya dan melibatkan lebih dari sekadar perlindungan terhadap virus di komputer. Secara global, salah satu sektor yang paling rentan adalah perawatan kesehatan, diikuti oleh manufaktur dan perbankan/keuangan. Sedangkan kegiatan kepemiluan memilik sifat terbuka dan politis, pemilu biasanya diwarnai dengan serangan disinformasi dan oleh karenanya membutuhkan perhatian dan perlakuan khusus.

Ancaman terus berkembang, penting untuk selalu mengikuti tren serangan terbaru.

**Berpartisipasilah dalam pelatihan kebersihan siber, baca dengan seksama petunjuk dan peringatan yang dikeluarkan oleh Bagian Datin, dan ajarkan diri Anda dan rekan kerja Anda tentang praktik baru keamanan siber.**

BAWASLU
BADAN PENGAWAS PEMILIHAN UMUM

# Waspada Email Phising!


Di dalam laut, targetnya **ikan**
Di dalam Phising, targetnya **anda!**

# 1. PHISING

## 1.1 PENGANTAR PHISHING

Phishing adalah salah satu ancaman siber terbesar saat ini. Dari semua jenis serangan siber yang memanfaatkan manipulasi psikologis, phishing adalah yang paling terkenal dan paling berhasil. Kegiatan kerja dari rumah dan pandemi COVID-19 telah meningkatkan tingkat ancaman phishing. Serangan phishing yang paling sering terjadi adalah serangan phishing melalui emails, namun sebetulnya semua jenis media dapat digunakan untuk melakukan serangan ini seperti melalui pesan instan (Whatsapp, Viber), Facebook, aplikasi video conference, maupun SMS.

**Definisi: Serangan phishing mencoba mengelabui orang agar memberikan informasi seperti sandi, atau nomor rekening bank dan kartu kredit melalui email yang dibuat sedemikian rupa sepaya seolah terlihat berasal dari sumber yang "terpercaya".**

Phishing adalah ancaman besar bagi semua jenis organisasi, baik besar maupun kecil. Informasi yang berhasil didapatkan dari serangan phishing dapat digunakan untuk mengakses akun penting dan dapat mengakibatkan pencurian identitas, kerugian finansial, atau kerusakan reputasi Anda maupun Bawaslu.

## 1.2 SPEAR-PHISHING

Spear-Phishing adalah serangan siber yang terarah. Serangan ini secara spesifik menargetkan calon korban, penyerang telah terlebih dahulu menentukan siapa individu atau organisasi yang mereka incar (mereka melakukan penelitian pada target untuk merancang serangan yang lebih personal dan bisa meningkatkan kemungkinan target calon korban jatuh ke dalam perangkap mereka).

Email spear-phishing seringkali dibuat seolah-olah berasal dari teman, kolega atau atasan korban, atau terkadang bahkan layanan online yang digunakan oleh korban (Gmail atau Bank).

Email yang dikirimkan biasanya akan "memberitahukan" Anda bahwa ada beberapa hal atau masalah yang perlu Anda selesaikan. Email tersebut juga berisi tautan atau lampiran yang jika dibukan akan memungkinkan peretas mengakses akun dan informasi Anda.

## 1.3 CARA MELINDUNGI DARI PHISHING DAN SPEAR-PHISHING

Tidak ada cara yang 100 persen berhasil untuk menghindari serangan phishing, namun Anda bisa selamat dari serangan ini dengan melakukan beberapa tindakan pencegahan mendasar seperti berikut ini:

**1. Selalu Curiga dan Pikir Baik-Baik Sebelum Anda Mengklik!**

Kita sehari-hari terbiasa dengan mengklik tautan, entah itu ketika membalas email, melakukan pencarian online, maupun berselancar di dunia maya, Mengklik pada tautan sudah jadi semacam kebiasaan. Penjahat siber memanfaatkan kebiasaan tersebut – yang telah membuat menurunnya tingkat kewaspadaan – untuk membuat kita membuka tautan di email hanya karena isinya terlihat menarik. Anda harus selalu bertanya pada diri sendiri: siapa yang mengirimnya? kapan? apakah ada sesuatu yang mencurigakan?

Meluangkan beberapa detik untuk mengarahkan kursor ke atas link yang diberikan dan melihat kemana arah tautan tersebut. Hal sederhana ini dapat menyelamatkan Anda dari serangan phishing.

Waspadalah, phishing tidak hanya dilakukan melalui email. Akun media sosial, pesan instan mobile, layanan e-commerce, dan semua jenis alat komunikasi online dapat digunakan sebagai vektor serangan phishing.

**2. Verifikasi Pengirim atau Legitimasi dari Situs Web**

Penyerang biasanya akan menirukan tampilan situs web yang asli. Ada beberapa kegiatan verifikasi yang dapat Anda lakukan agar tidak terperangkap ke dalam serangan phishing yang umum dilakukan:

Cek apakah pada sebuah email ada tautan yang tidak mengandung nama organisasi atau perusahaan yang digunakan untuk mengirim email.

Salah satu rekomendasi yang sangat berguna adalah dengan mengetik tautan seluruhnya pada browser dari pade mengklik langsung dari email yang Anda terima.

**3. Gunakan Otentikasi 2 Langkah (2FA)**

Praktik ini adalah cara terbaik untuk melindungi Anda dari phishing dan spear-phishing yang canggih. Jika seorang hacker berhasil mendapatkan password Anda, mereka tidak akan bisa login ke akun Anda jika mereka tidak memiliki "faktor login ke-dua" Anda.

**4. Selalu Perbarui Antivirus Anda**

Sebagian besar anti-virus sudah dilengkapi dengan fitur anti-phishing (terkadang disebut Web-Shield) yang secara otomatis terinstall di browser Anda dan memblokir situs-situs phishing dari komputer Anda. Jangan install toolbar anti-phishing yang Anda temukan secara acak di internet! Seringkali, toolbar tersebut justru mengandung spyware yang akan merekam dan mengirimkan semua situs yang Anda kunjungi ke pihak ketiga. Dalam hal ini, obatnya malah bisa lebih buruk dari penyakitnya. Jika lembaga Anda tidak menyediakan anti-virus untuk perangkat Anda, maka Anda disarankan untuk menggunakan anti-virus yang berbayar atau anti-virus gratisan yang telah dikenal luas olah masyarakat, misalnya Avast anti-virus. Hanya install anti-virus yang diunduh dari website resmi pembuatnya.

**5. Jangan Memberi Informasi Pribadi**

Sebagai aturan umum, Anda harus selalu berhati-hati saat berbagi data pribadi maupun informasi keuangan di Internet.

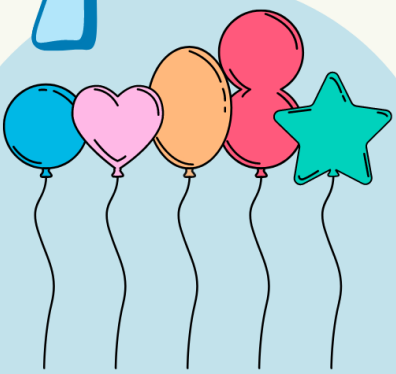
Rata-rata lembaga keuangan memiliki aturan ketat terkait dengan permintaan informasi data sensitif. Mereka tidak akan meminta data personal tanpa mengonfirmasi identitas Anda, dan Anda tidak boleh memberikannya tanpa mengonfirmasi identitas mereka.

Kunjungi situs web perusahaan, dapatkan nomor mereka dan hubungi mereka.

Juga, berhati- hatilah dengan pertanyaan reset password: nama Ibu Anda, kota kelahiran Anda, dan sekolah pertama Anda bukanlah sebuah rahasia. Jadi data tersebut sebaiknya tidak dijadikan sebagai pertanyaan untuk pemulihan kata sandi.

# Bagaimana cara membuat password yang baik?

1



unik

2

tidak mengandung data pribadi

3

tidak digunakan pada platform lainnya

BAWASLU
BADAN PENGAWAS PEMILIHAN UMUM

# 2. MELINDUNGI AKUN ANDA

## 2.1 DIMULAI DENGAN PEMILIHAN PASSWORD YANG KUAT

**Password yang Kuat**

- Dibuat dan disimpan secara otomatis oleh password manager.
- Unik, digunakan hanya untuk satu akun.
- Harus berupa frasa daripada kata, minimal 20 karakter.
- Dapat menyertakan angka, huruf kapital dan simbol.
- Ditambah dengan otentikasi 2 faktor.

**Password yang Lemah**

- Terdiri dari beberapa karakter (pendek).
- Berisi data pribadi (misal tanggal lahir).
- Digunakan untuk lebih dari satu akun.
- Dicatat dan disimpan secara sembarangan (ditulis di post note, notepad, dll.).
- Dibagikan di antara teman dan keluarga Anda.

## 2.2 MENGGUNAKAN PASSWORD YANG SAMA ITU BERBAHAYA

Faktor yang membuat password yang kuat juga membuatnya sulit untuk diingat; menggunakan password yang sama pada beberapa akun adalah hal yang berbahaya: jika satu akun diretas, maka penyerang memiliki akses ke semua akun digital Anda: email, internet banking, media sosial, penyimpanan cloud, dll. Meskipun tidak terlalu rumit untuk membuat password yang sesuai dengan kaidah dasar pemilihan password, membuat satu password untuk satu akun akan sangat menyulitkan bagi Anda untuk mengingatnya. Di sinilah Password Manager berperan.

**Password Manager memungkinkan Anda untuk untuk memastikan setiap password Anda adalah unik dan kuat (dihasilkan secara otomatis oleh software) dan menyimpannya dalam database yang aman sehingga Anda tidak perlu mengingatnya atau bahkan mengetiknya. Anda hanya akan perlu mengingat satu password: password untuk mengakses Password Manager itu sendiri.**

Salah satu solusi Password Manager yang bisa digunakan adalah Last Pass (https://www.lastpass.com). Tata cara aktivasi dan penggunaan password manager LastPass dapat dilihat di lampiran A pada buku panduan ini.

Password tidak boleh dibagikan ke orang lain, jika ingin berbagi akses terhadap sebuah akun software password manager bisa menfasilitasi hal tersebut tanpa perlu memberitahukan apa passwordnya.

BAWASLU
BADAN PENGAWAS PEMILIHAN UMUM

# Seberapa penting melakukan **Multi Factor Authentication**?

Melakukan **MFA** seperti mengunci pagar dan pintu rumah, agar **aman dan tidak kemalingan.**

## 2.3. MENGAKTIFKAN OTENTIKASI MULTI FAKTOR

Otentikasi dua langkah (2FA) adalah lapisan keamanan kedua untuk melindungi sebuah akun atau system saat login. Metode keamanan ini terdiri dari dua tahap otentikasi yang berisikan:

- **Tahap pertama adalah sesuatu yang Anda ketahui (misalnya password), dan**
- **Tahap kedua adalah sesuatu yang Anda miliki (berupa kode yang dihasilkan lewat ponsel, SMS, maupun kode dari stik USB khusus).**

  ***Tahap kedua dari otentikasi bisa juga diri Anda sendiri, misalnya jari, wajah, maupun fitur biometrik lainnya.***

Faktor otentikasi kedua bisa juga berupa lokasi di mana Anda berada (misalnya, ponsel Anda yang mendeteksi bahwa Anda sudah di rumah dan secara otomatis menon-aktifkan kunci layer ponsel.

Tidak semua metode otentikasi dua langkah (2FA) menawarkan tingkat perlindungan yang sama:

**1. Berbasis SMS**

Anda diminta menyediakan nomor ponsel saat aktivitasi. Ketika Anda akan login, Anda akan diminta memasukkan kode otentikasi yang secara otomatis akan dikirim ke ponsel Anda. Meskipun ini memberikan peningkatan yang signifikan dalam keamanan akun yang relatif hanya dengan nama pengguna dan password, ini tidak akan menghentikan penjahat siber yang termotivasi dan ahli.

**2. Berbasis Aplikasi Authenticator**

Opsi ini menggunakan aplikasi yang secara berkala menghasilkan kode khusus di ponsel Anda. Google Authenticator adalah aplikasi yang sangat populer untuk ini; Alternatif lainnya adalah Microsoft Authenticator, Authy, dan FreeOTP. Setiap 30 detik, aplikasi akan menghasilkan 6-digit kode baru yang berlaku sekali pakai. Ini jauh lebih aman daripada otentikasi SMS. Tata cara aktivasi dan penggunaan aplikasi otentikator dapat dilihat pada lampiran B di panduan ini.

**3. Otentikasi Dua Langkah Berbasis PUSH**

Beberapa layanan (Gmail contohnya) akan mengirimkan konfirmasi login ke ponsel Anda dimana Anda dapat menyetujui atau tidak sebuah aktivitas login ke akun Anda. Pemberitahuan ini akan menunjukkan bahwa seseorang (mudah-mudahan Anda) telah mencoba untuk login. Metode ini memberikan perkiraan waktu dan lokasi untuk selanjutkan dapat Anda periksa apakah benar Anda yang berusaha login.

**4. Berbasis Kunci Keamanan (FIDO (Fast ID Online) U2F)**

Bukan merupakan mekanisme pengamanan yang sangat popular. Untuk penggunaannya pada suatu situs, Anda perlu mendaftarkan perangkat Anda terlebih dahulu. Setelah terdaftar, saat login situs akan meminta konfirmasi login lewat komputer atau telepon Anda. Perangkat U2F memang membutuhkan biaya, dari 20USD hingga 60USD per unit. Metode ini disarankan untuk akun yang membutuhkan pengamanan leih lebih tinggi, seperti administrator TI.

## 2.4 MENGENALI JIKA AKUN ANDA TELAH DISUSUPI

Rekomendasi berikut ini berlaku untuk akun personal Anda, untuk kebijakan resmi lembaga bisa menghubungi bagian Datin Bawaslu. **Jika akun kantor Anda diretas, Anda harus secepatnya memberitahu bagian Datin, sebaiknya melalui telepon.**

**1. Password berubah tiba-tiba**

Hal pertama yang harus dilakukan adalah memastikan password yang dimasukkan adalah password yang benar, bahkan meskipun telah menggunakan password manager dan praktik pengelolaan password pun, masih memungkinkan terjadinya kesalahaan pengguna. Jika tetap tidak bisa masuk, Anda bisa memulai proses pemulihan password.

**2. Ada e-mail yang tidak wajar di dalam folder terkirim (*sent item*)**

Sering kali, penyerang hanya menggunakan akun Anda untuk mengumpulkan informasi tentang Anda, dan menyembunyikan aktivitas mereka. Mereka bisa saja secara diam-diam mengirimkan email orang-orang di dalam address book Anda dan meminta uang atas nama Anda dan tidak sepenuhnya menutup akses Anda terhadap email Anda.

**3. Adanya email perubahan password secara tiba-tiba**

Email setel ulang kata sandi yang tidak Anda minta harus diambil dengan kecurigaan. Jika permintaan tersebut sah dan berasal dari layanan yang sebenarnya Anda gunakan, penyerang mungkin mencoba mengambil alihnya.

**3. Adanya laporan dari kontak Anda**

Jika Anda mulai menerima pesan dari kontak Anda (kolega, keluarga, teman) yang memberitahukan bahwa mereka menerima email aneh dari Anda, ini bisa jadi pertanda seseorang telah menggunakan email Anda untuk mengirimkan email phishing.

**4. Adanya alamat IP, perangkat, dan/atau browser yang tidak dikenal**

Penyedia layanan email biasanya menyediakan fitur yang memungkinkan Anda untuk memeriksa aktivitas login dan lokasi dari mana perangkat Anda terhubung. Sebaiknya periksa fitur ini secara berkala dan lihat jika ada perangkat atau lokasi yang tidak dikenali.

## 2.5 JIKA ANDA MERASA AKUN ANDA TELAH DISUSUPI

**1. Ganti password**

Ini adalah praktik yang baik meskipun Anda hanya sebatas curiga terhadap kemungkinan akun Anda sudah diretas. Password yang dipilih haruslah panjang dan unik dan gunakan password manager jika memungkinkan. Jika Anda sudah kehilangan akses ke akun Anda, lakukan proses pemulihan password. Jika tidak berhasil, satu-satunya pilihan Anda adalah menghubungi layanan pelanggan dari penyedia email tersebut. Proses ini mungkin akan memakan waktu beberapa hari dan tidak ada jaminan Anda akan mendapatkan akun Anda kembali.

Sekarang saatnya untuk memeriksa pengaturan pemulihan akun pada akun-akun yang Anda miliki. Anda diminta untuk mencantumkan alamat email dan nomor telepon pemulihan ketika Anda membuat akun tersebut, periksa apakah alamat email dan nomor telepon pemulihan sudah benar, jika tidak, segera ubah.

**2. Aktifkan otentikasi dua langkah (2FA)**

Jika sebelumnya Anda tidak menggunakan autentikasi dua langkah, maka sekarang Anda harus mengaktifkannya. Sebagian besar penyedia layanan email mendukung opsi untuk login dengan otentikasi dua langkah. Unduh dan install Google Authenticator atau Authy, keduanya mudah disiapkan.

**3. Beri tahu teman dan keluarga Anda**

Beberapa dari mereka mungkin sudah memberitahu Anda tentang adanya aktivitas yang mencurigakan dari akun Anda. Anda pun harus sesegera mungkin memberi tahu yang lain agar mereka tidak menjadi mangsa serangan phishing yang menggunakan nama dan alamat email Anda.

**4. Periksa penerusan akun, balasan otomatis, dsb.**

Penerusan otomatis dan balasan otomatis bukanlah fungsi umum digunakan sehari-hari. Untuk mengakses pengaturannya juga terkadang rumit dan berbelit tapi Anda harus memeriksa apakah fitur ini aktif atau tidak. Anda bisa saja telah mengubah password Anda, tetapi jika fitur penerusan akun dan balasan otomatis dalam keadaaan aktif, maka semua informasi yang dikirim ke email Anda akan dikirimkan juga ke email penyerang.

**5. Periksa opsi keamanan tambahan**

Cari opsi keamanan lain yang disediakan oleh penyedia layanan email Anda, atau opsi keamanan lain yang secara spesifik disediakan oleh perangkat Anda. Opsi ini bisa berupa peringatan jika ada aktivitas login dari perangkat atau lokasi baru, atau opsi untuk menghapus perangkat atau akun dari jarak jauh jika hilang atau dicuri. Pilih opsi yang dibutuhkan, dan aktifkan.

**6. Periksa apakah ada akun lain yang terpengaruh**

Karena adakalanya email Anda digunakan untuk mengamankan akun lain, maka penting untuk memeriksa apakah ada akun lain yang terpengaruh. Pastikan Anda dapat masuk ke akun lain tersebut, dan pertimbangkan untuk merubah password dari akun itu. Jika Anda menghadapi kesulitan mengakses salah satunya, segera ambil tindakan untuk mereset password atau menghubungi layanan pelanggan penyedia layanan.

**7. Jalankan antivirus dan bersihkan perangkat**

Penyerang mungkin telah memperoleh akses ke akun Anda melalui malware atau celah keamanan yang ada pada perangkat Anda. Jika Anda menjalankan proses pemulihan akses ke akun email Anda, pastikan Anda terlebih dahulu menjalankan antivirus untuk mendeteksi dan menghapus spyware, keyloggers, dan jenis malware lainnya.

**8. Meminta bantuan**

Anda tidak sendiri. Menyerang akun Anda bisa sangat menegangkan. Jangan ragu untuk bertanya kepada teman atau kolega.

BAWASLU
BADAN PENGAWAS PEMILIHAN UMUM

# UPDATE

Peningkatan keamanan,
performa, efisiensi


Manusia butuh **suplemen**
agar tidak gampang **sakit**,
komputer butuh **"update"**
agar tidak gampang terkena **virus!**

# 3. PERLINDUNGAN TERHADAP PERANGKAT ANDA

## 3.1 PERBARUI SOFTWARE DAN SISTEM OPERASI SEMUA PERANGKAT ANDA

Menjaga sistem operasi, antivirus, dan software lain tetap mutakhir adalah hal yang sangat penting untuk memastikan keamanan perangkat Anda, dan pemeriksaan rutin untuk memastikan bahwa fungsi pembaruan otomatis berfungsi dengan baik dan benar harus senantiasa dilakukan.

**1. Perbarui Sistem Operasi Anda dan software lain secara berkala**

Sistem operasi dan software lainnya perlu diperbarui secara berkala untuk menutup celah kerentanan dan memastikan data Anda terlindungi.


**<u>Yang harus Anda lakukan:</u>**

**Perusahaan pengembang software secara teratur merilis tambalan *(patch)* dan pembaruan, terutama ketika mereka menemukan adanya celah keamanan pada software tersebut. Segera install tambalan dan pembaruan yang disediakan untuk menjaga perangkat Anda aman dari**

**ancaman terbaru. Sangat disarankan untuk mengaktifkan pembaruan otomatis sehingga proses pembaruan berlangsung secara teratur.**

Setelah periode waktu tertentu, system operasi akan mencapai apa yang disebut sebagai akhir masa hidup computer *(computer end-of-life)*. Ini adalah fase di mana pabrikan/pengembang software akan berhenti memberikan dukungan, termasuk menyediakan pembaruan maupun tambalan keamanan.

Anda harus hati-hati mempertimbangkan risiko yang ditimbulkan atas penggunaan komputer yang system operasinya sudah tidak disokong lagi oleh pabrikan, karena penyerang biasanya menyasar mesin-mesin yang masih menggunakan system operasi ini.

Misalnya, dukungan untuk Windows XP berakhir pada 8 April 2014, setelah 12 tahun Microsoft tidak lagi menyediakan pembaruan keamanan untuk sistem operasi ini. Microsoft Windows 7 mencapai akhir masa pakainya 14 Januari 2020 dan harus ditingkatkan ke Windows 10 juga.

Untuk ponsel Android, waktu dukungan sebenarnya jauh lebih pendek dan patch keamanan biasanya berhenti didistribusikan setelah 3 hingga 4 tahun.

**2. Memastikan antivirus Anda aktif dan up-to-date**

Antivirus garis depan pertahanan komputer Anda terhadap malware. Tidak perlu menginstal beberapa antivirus sekaligus dalam sebuah perangkat (mereka mungkin saling mengganggu). Install satu saja yang efektif dan Anda percayai.

Yang harus Anda lakukan: Menginstal antivirus saja tidak cukup, penting untuk memperbarui antivirus secara rutin.

## 3.2 AMANKAN PERANGKAT *MOBILE* ANDA

Telpon seluler (ponsel) telah menjadi “sahabat” terbaik banyak orang saat ini, memang sangat bermanfaat tapi juga mendatangkan risiko. Pasalnya, saat ini telpon genggam bukan saja sebagai alat komunikasi dan penyimpan data, tapi juga berfungsi sebagai dompet dan pusat jaringan sosial pengguna. Dengan fungsi-fungsi tersebut, menjaga keamanan ponsel pun menjadi semakin penting. Jika keamanan ponsel berhasil ditembus oleh peretas, maka yang terdampak bukan saja pemilik ponsel tersebut, namun juga lembaga tempat dia bekerja. Berikut adalah tips untuk mengamankan dan menghindari peretasan pada ponsel.

**1. Update ponsel secara berkala baik sistem operasi maupun aplikasi yang diinstall**

Lakukan update berkala untuk memastikan sistem operasi ponsel, program serta aplikasi yang terpasang di ponsel senantiasa yang paling terkini.

**2. Pasang pengunci layar untuk mencegah akses orang lain**

Pengunci layer berupa lockscreen, sidik jari, pengenalan wajah adalah “pagar” pertama untuk menjaga ponsel Anda, aktifkan lockscreen baik berupa PIN, pattern, sidik jari, pengunnci wajah pada ponsel. Jangan aktifkan pengaturan agar ponsel masuk mode standby dan terkunci secara otomatis setelah periode waktu tertentu (missal 30 detik).

**3. Hindari terhubung dengan jaringan Wi-Fi publik**

Koneksi pada Wi-Fi publik (café, hotel, mal, dsb) seringkali tidak aman karena tidak terlindungi dan dapat disusupi serangan Man-in-the-middle yang memungkinkan akses terhadap arus komunikai dan bahkan ponsel Anda.

**4. Jangan *root/jailbreak* ponsel untuk mengurangi resiko peretasan**

Root atau Jailbreak adalah proses menghilangkan batasan yang diberlakukan pada ponsel Android dan Apple. Melakukan root/jailbreak pada ponsel Anda akan memungkinkan aplikasi pihak ketiga untuk mengakses ponsel tersebut. Hal ini berpotensi membuat pihak lain mengetahui semua informasi yang tersimpan dan dikirimkan pada ponsel itu, bahkan untuk memata-matai aktivitas Anda.

**5. Hanya install aplikasi dari sumber resmi Play/Playstore**

Aplikasi yang ada Google Play (Android) atau Apple Appstore (iOS) lebih aman karena keduanya adalah layanan store resmi terpercaya yang memiliki aturan ketat untuk mencegah aplikasi jahat.

**6. Aktifkan enkripsi data/SD Card**

Enkripsi data adalah solusi dasar dalam melindungi informasi yang disimpan di ponsel Anda. Dengan enkripsi data, maka data di ponsel Anda akan diacak dengan kunci tertentu, jika ponsel Anda hilang, orang lain tidak bisa membaca data dalam ponsel tanpa decryption key.

**7. Aktifkan Find dan Wipe My Device**

Ketika ponsel hilang atau dicuri, Anda dapat mengunci ponsel dan bahkan menghapus data pada ponsel tersebut dari jarak jauh. Dengan cara ini, akses illegal terhadap informasi sensitif milik Anda dan lembaga Anda bisa terjaga.

**8. Aktifkan phone backup dan folder backup**

Untuk mengantisipasi serangan malware yang berakibat pada hilangnya data atau ketika ponsel tersebut hilang, buatkan backup data di tempat lain sehingga data tetap bisa diakses dan diperbarui. Mengaktifkan fitur backup otomatis di layanan cloud akan sangat membantu Anda saat pemulihan paska insiden. Baik Google (Drive) dan Apple (iCloud) menyediakan fitur backup data di cloud. Pastikan perangkat Anda terhubung dan dibackup pada layanan tersebut.

## 3.3 WASPADALAH DENGAN SOFTWARE BAJAKAN DAN TIDAK BERLISENSI

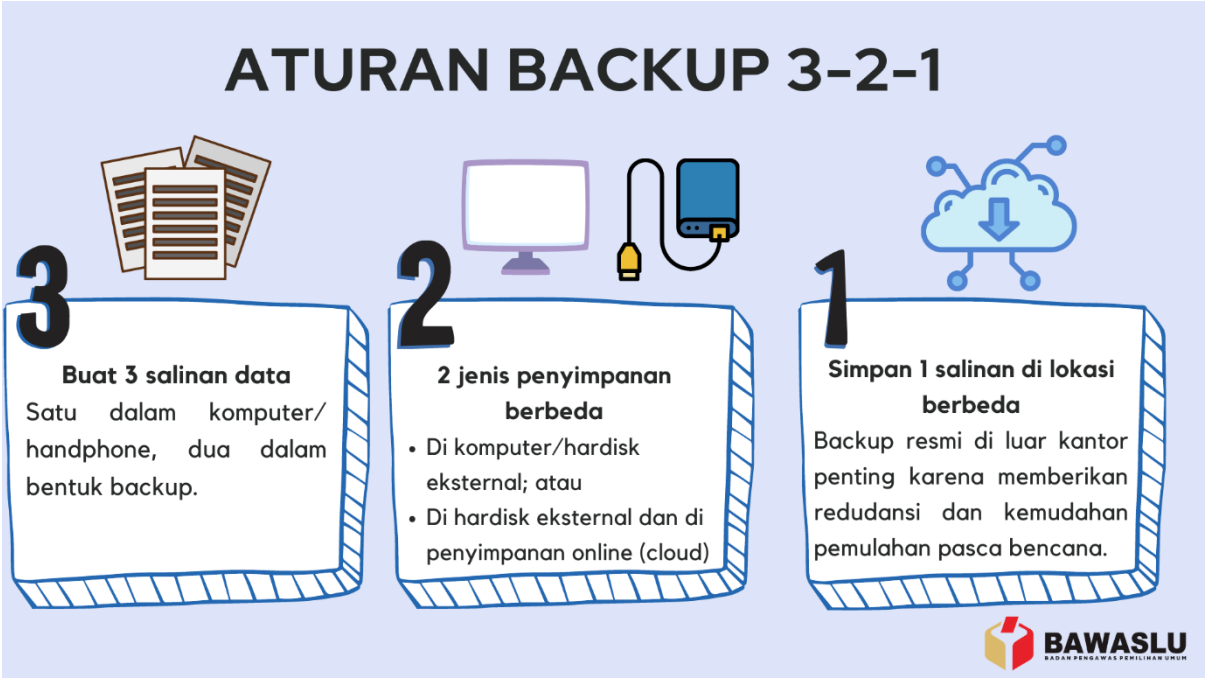
Software bajakan dapat secara diam-diam tanpa sepengetahuan Anda menginstal malware ke perangkat Anda yang akan menyebabkan masalah pada perangkat tersebut. Dalam situasi tertentu mungkin sulit untuk mendapatkan software berlisensi, dalam situasi tersebut, Anda sebaiknya mencari software alternatif yang bersifat open source dan gratis, dan berkoordinasi dengan bagian Anda untuk menganggarkan software berlisensi.

Selalu instal software dari situs web resmi. Ada banyak sekali situs web yang menyediakan Salinan file instalasi software, tapi banyak dari meraka yang tidak jelas keamanannya.

## 3.4 MENERAPKAN STRATEGI BACKUP YANG BAIK

**Pada suatu titik, Anda akan membutuhkan backup data Anda. Entah itu karena kerusakan perangkat atau karena serangan siber. Memang membutuh waktu, tenaga, dan dana yang tidak sedikit untuk membuat backup secara benar, namun usaha yang dikeluarkan jauh lebih sedikit daripada yang Anda perlukan untuk membuat ulang file Anda yang hilang, itu pun jika dimungkinkan.**

Pilih media penyimpanan backup, bisa berupa perangkat penyimpanan fisik (stik USB, hard drive portable/eksternal), sistem jaringan internal (biasanya dikelola oleh lembaga, ini adalah tempat di mana Anda dapat meletakkan file Anda di jaringan organisasi Anda), atau sistem berbasi cloud (misalnya Dropbox atau Google Drive).




**Untuk file Anda yang paling penting, coba terapkan aturan 3-2-1:**

- **3 - Simpan tiga salinan file penting, satu file utama (di komputer, laptop, atau ponsel) dan dua cadangan di media penyimpanan yang lain.**
- **2 - Gunakan dua jenis media yang berbeda; misalnya, satu komputer dan satu hard drive, atau satu hard drive dan satu penyimpanan berbasis cloud.**
- **1 - Menyimpan satu backup di luar kantor, memiliki backup file di lokasi yang berbeda di luar kantor adalah hal penting dan itu menyediakan: redundansi dan kemudahan pemulihan paska bencana. Memiliki backup di luar kantor memberikan tingkat redundansi jika backup di lokasi pertama gagal.**

Idealnya file Anda dibackup secara otomatis untuk mengurangi masalah keharusan mengingat untuk melakukan backup. Tapi Anda perlu memeriksa apakah backup otomatis berfungsi sebagai mana mestinya.

## 3.5 RISIKO PERANGKAT USB

Satu hal yang pasti, ketika sebuah perangkat USB hilang, maka hilang juga data yang ada di dalamnya. Kehilangan perangkat USB yang berisi data sensitif perusahaan dapat berujung pada pengumuman telah terjadi insiden keamanan, penyelidikan internal, dan mungkin teguran - atau bahkan hilangnya pekerjaan dan tututan atas Anda di pengadilan.

**Yang harus diperhatikan terkait perangkat USB:**

- **Berhati-hatilah agar perangkat USB Anda tidak hilang, tetap jaga agar tetap aman dan dalam kendali Anda.**
- **Jika memungkinkan gunakan password atau enkripsi pada perangkat USB tersebut.**
- **Segera hapus file yang sensitif setiap kali Anda selesai mentransfer file dan jangan simpan dalam USB stik tersebut.**

Sebuah penelitian menunjukkan bahwa hampir 50 persen orang yang menemukan flashdisk USB akhirnya memasukkan perangkat tersebut ke komputer mereka tanpa melakukan tindakan pencegahan apa pun. Dibutuhkan pakar keamanan dengan PC yang aman dan peralatan keamanan khusus untuk memeriksa apakah flash-drive USB yang ditemukan adalah aman. Jangan mencoba membukanya di laptop Anda.

**Yang harus Anda lakukan jika menemukan flash drive USB:**

- **Biarkan saja, atau taruh di tempat sampah.**
- **Jangan memasangnya di computer Anda. J**
- **Jangan langsung menggunakan flash-drive USB gratisam yang disediakan selama konferensi (materi acara bisa dikirimkan lewat email).**

Penting untuk menjaga dan menyimpan perangkat USB Anda, begitu juga menjaga reputasi Anda dan lembaga Anda bekerja. Keamanan dan privasi dapat dilanggar dan mungkin hal yang memalukan bisa terjadi jika Anda meminjamkan perangkat USB ke kolega dan ternyata di USB tersebut ada file-file pribadi Anda.

**Apa yang harus Anda lakukan:**
**Pertimbangkan memiliki area penyimpanan khusus untuk menjaga perangkat penyimpanan pribadi Anda terpisah dari yang Anda gunakan untuk bekerja, dan berhati-hatilah untuk memeriksa isi dari sebuah drive sebelum menyerahkannya kepada siapa pun.**

# Tips Bijak Menggunakan Sosial Media

# 7 TIPS

01 Tidak ada tombol delete di internet

02 Jangan sebarkan lokasi anda

03 Hanya terhubung atau berkomunikasi dengan orang yang Anda percaya

04 Perhatikan keberadaan anda di dunia maya

05 Pastikan beberapa hal tetap rahasia

06 Hargai privasi orang lain

07 Sampaikan apabila postingan tentang anda yang membuat tidak nyaman

BAWASLU
BADAN PENGAWAS PEMILIHAN UMUM

# 4. BAHAYA MEDIA SOSIAL

## 4.1 WASPADAI APA YANG ANDA TULISKAN SECARA ONLINE

Apa pun platform layanan media sosial yang Anda gunakan, pertimbangkan jenis informasi yang Anda bagikan dengan orang lain pada platform media social tersebut. Berikut adalah risiko umum terkait dengan penggunaan media sosial:

**1. Berbagi informasi sensitif pribadi.**

Berhati-hatilah tentang sebarapa jauh informasi pribadi (seperti nama lengkap, alamat, tanggal lahir, nomor telepon, atau tempat lahir Anda) yang Anda tampilkan di situs jejaring sosial. Semakin banyak informasi yang Anda posting, semakin mudah bagi penyerang atau orang lain untuk menggunakan informasi tersebut untuk mencuri identitas Anda, mengakses data Anda, atau melakukan kejahatan lain seperti menguntit.

**2. Konten yang salah**

Memasang konten/postingan yang meragukan: dapat berupa gambar, video, atau opini yang mungkin membuat Anda tampak tidak professional, kasar, dan dapat merusak reputasi Anda. Ingatlah bahwa apa yang diunggah di internet tidak akan pernah sepenuhnya terhapus, bahkan ketika Anda sudah menghapus konten tersebut.

**3. Membuka informasi lokasi/keberadaan Anda**

Melacak lokasi Anda. Banyak platform media sosial memungkinkan Anda untuk menggunakan fitur check in dan membagikan lokasi Anda, atau secara otomatis menambahkan lokasi Anda ke foto dan postingan. Tiba-tiba, informasi yang Anda bagikan kepada publik bahwa Anda sedang menghadari sebuah konferensi dapat digunakan untuk membuat email phishing terarah yang berisi tautan berbahaya kepada Anda.

# Tips Bijak Menggunakan Sosial Media

**Tidak ada tombol delete di internet**

Pikirkan baik-baik sebelum ada posting sesuatu. Bahkan jika postingan tersebut anda hapus, ada kemungkinkan orang lain telah melihat dan membuat tangkapan layar (screenshot) dari postingan anda.

**Jangan sebarkan lokasi anda**

Fitur check-in dengan geo-tagging lokasi di sosial media bukan fitur yang aman untuk digunakan. Hal tersebut bisa memberitahunkan penguntit di mana lokasi Anda atau memberikan informasi kepada pencuri bahwa Anda sedang tidak ada di rumah

**Hanya terhubung dengan orang yang Anda percaya**

Meskipun beberapa platform media sosial terkesan aman digunakan untuk berjejaring kerena pembatasan informasi pribadi yang ditampilkan, sebaiknya Anda tetap waspada dan hanya membuat koneksi dengan orang yang anda percaya

**Perhatikan keberadaan anda di dunia maya**

Jika memungkinkan, ubah pengaturan kerahasiaan dan keamanan yang sesuai dengan kenyamanan anda dalam berbagi informasi. Adalah hal yang wajar untuk membatasi bagaimana dan dengan siapa anda berbagi informasi


**Pastikan beberapa hal tetap rahasia**

Ada beberapa informasi yang sebaiknya tidak ditampilkan di media sosial. Misalnya, tanggal lahir lengkap dan foto-foto sensitif terkait keluarga, karena bisa memudahkan kegiatan pencurian data dan rekayasa sosial.

**Hargai privasi orang lain**

Hanya posting tentang orang lain, sebagaimana mereka posting tentang Anda.


**Sampaikanlah juga anda merasa tidak nyaman.**

Sampaikanlah jika seseorang posting sesuatu tentang anda yang membuat anda tidak nyaman atau merasa tidak pantas. Di sisi lain, tetaplah berpikiran terbuka jika ada yang mengutarakan ketidaknyamanannya terhadap postingan yang anda buat terkait orang tersebut.

BAWASLU
BADAN PENGAWAS PEMILIHAN UMUM

# 5. RUMAH ANDA ADALAH KANTOR BARU ANDA

Instansi dan perusahaan baik dari skala besar, menengah, maupun kecil telah mengadopsi praktik kerja dari rumah untuk memastikan kelangsungan bisnis selama pandemi COVID-19. Perubahan dalam kegiatan usaha selalu memiliki dampak risiko keamanan.

Cara kerja baru membutuhkan langkah-langkah keamanan baru; tetapi biasanya risiko ini seiring waktu akan berhasil dikelola dengan hati-hati. Sayangnya, penjahat siber telah terlebih dahulu melihat peluang di tengah pandemi, dan telah melancarkan serangkaian serangan.

Email phishing telah melonjak lebih dari 600% sejak akhir Februari dengan upaya untuk mengelabui pengguna agar menyerahkan informasi login dan informasi keuangan mereka, dan/atau secara tidak sengaja mengunduh malware ke komputer mereka.

## 5.1 PERCAKAPAN INSTAN (CHAT)

Aplikasi chat telah menjadi alat yang nyaman untuk mentransfer file, menyimpan catatan, dan dapat berfungsi sebagai penyimpanan berbasis cloud; oleh karena itu, keamanan chat merupakan komponen penting untuk mengamankan komunikasi. Indonesia pernah mengalami serangan siber yang menirukan akun chat pejabat penyelenggara pemilu di masa lalu. Bentuk serangan ini bisa jadi akan digunakan lagi di masa yang akan datang.

**Apa yang harus Anda lakukan:**

1. **Hati-hati terhadap serangan phishing di melalui aplikasi chat, seseorang dapat berpura-pura sebagai kolega atau atasan Anda. Bagikan informasi seperlunya dan gunakan media lain jika Anda ragu.**
2. **Aktifkan fitur otentikasi 2 langkah (2FA) jika memungkinkan. Setiap aplikasi chat saat ini sudah dilengkapin dengan fitur keamanan 2FA. Aktifkan PIN/2FA pada akun Whatsapp, Line, Telegram Anda.**

## 5.2 KONFERENSI VIDEO

Terlepas instruksi untuk kerja dari rumah akan menjadi tren jangka panjang atau tidak, konferensi video secara online telah menjadi aktivitas normal dan kemungkinan besar akan tetap menjadi metoda pelaksanaan kursus pelatihan, rapat online, dan komunikasi reguler. Kesimpulannya: Kebutuhan konferensi video akan selalu ada.

Ada beberapa risiko yang harus diperhatikan saat menggunakan layanan konferensi video:

1. Zoom-Bombing terjadi ketika peserta yang tidak diundang menggunakan konferensi video online untuk menyebarkan konten yang tidak pantas. **Apa yang harus Anda lakukan:** Pastikan Anda merahasiakan kata sandi, buat ruang tunggu sehingga Anda dapat mengizinkan peserta sebelum rapat dimulai.
2. Kerentanan keamanan masih ditemukan di Zoom, Microsoft Teams, dan pada dasarnya terus ditemukan. **Apa yang harus Anda lakukan:** Perbarui software dan atur ke pembaruan software otomatis jika memungkinkan.

3. Gunakan aplikasi yang direkomendasikan oleh instansi Anda. Ini penting karena beberapa percakapan Anda bisa jadi sifatnya sensitif.
4. Beberapa aplikasi konferensi video meminta Anda untuk mengunduh file .exe agar dapat bergabung dalam rapat online. **Apa yang harus Anda lakukan:** pastikan file yang diunduh berasal dari website resmi penyedia layanan konferensi video dan bukan dari website/orang lain.

## 5.3 MENGAMANKAN JARINGAN RUMAH ANDA

Bekerja dari rumah sebenarnya dapat menimbulkan risiko bagi lembaga. Di kantor biasanya ada bagian khusus uang mengurus soal keamanan siber. Tetapi ketika karyawan bekerja dari rumah, mereka harus mengurusnya sendiri. Dengan berkembangnya kebijakan bekerja dari rumah, kemungkinan rumah telah menjadi kantor kedua, risiko bertambah lagi ketikan karyawan menggunakan komputer pribadi mereka untuk pekerjaan.

Ada beberapa langkah penting untuk mengamankan wifi di rumah Anda, dan sebagian besar pengguna belum mungkin pernah mendengarnya, tetapi penting untuk memastikan bahwa tidak ada yang dapat mencegat jalur komunikasi rumah Anda atau mengalihkan kendali router rumah Anda kepada penyerang.

**Koneksi Wi-Fi Anda**

Seperti halnya aturan password untuk semua akun, password haruslah panjang (minimal 20 karakter) dan sulit ditebak. Jika sudah kuat, Anda tidak perlu terlalu sering mengubahnya. Periksa apakah Wi-Fi Anda menggunakan protokol enkripsi WPA2 yang sangat direkomendasikan. Penggunaan WEP dan WPA1 tidak disarankan karena tidak aman.

**Pengaturan router Anda**

Untuk mengkonfigurasi Wi-Fi, Anda perlu masuk ke settingan router Anda. Tergantung merk dan modelnya, Anda harus menggunakan browser untuk masuk ke salah satu alamat ini agar dapat mengakses bagian administrasi dari router Anda: https://192.168.0.1 , https://192.168.1.1 atau https://10.0.0.1.

Anda akan diminta untuk menyediakan username dan password saat login, jika Anda tidak mengetahuinya, bisa jadi username dan passwordnya masih standar bawaan pabrik (periksa situs web pabrikan, bisa jadi TP-Link, Cisco Linksys, ZTE, Huawei). Begitu Anda berhasil masuk ke halaman adminstrasi router, lakukan hal berikut ini:

**1. Ubah password standar administrator router dan nama jaringan Wi-FiJ**

Jika Anda belum melakukannya, maka sangat penting bagi Anda untuk mengubahnya segera untuk menjaga router dari serangan. Ini karena nama jaringan Wi-Fi bawaan pabrik masih menyertakan informasi merk dan model dari router, dan informasi tentang standar username dan password untuk masing-masing merk router banyak tersedia di internet sehingga memudahkan penyerang untuk melakukan peretasan terhadap router yang masih standar bawaan pabrik.

**2. Nonaktifkan akses jarak jauh**

Terkadang pabrikan memberikan opsi untuk terhubung dan melakukan pengaturan router Anda dari jarak jauh. Meskipun hal ini praktis bagi tim teknis untuk melakukan perbaikan dari jauh, namun ini juga memungkinkan peretas untuk masuk dan mengendalikan koneksi Anda dan pada dasarnya melakukan apa pun yang mereka inginkan dengannya.

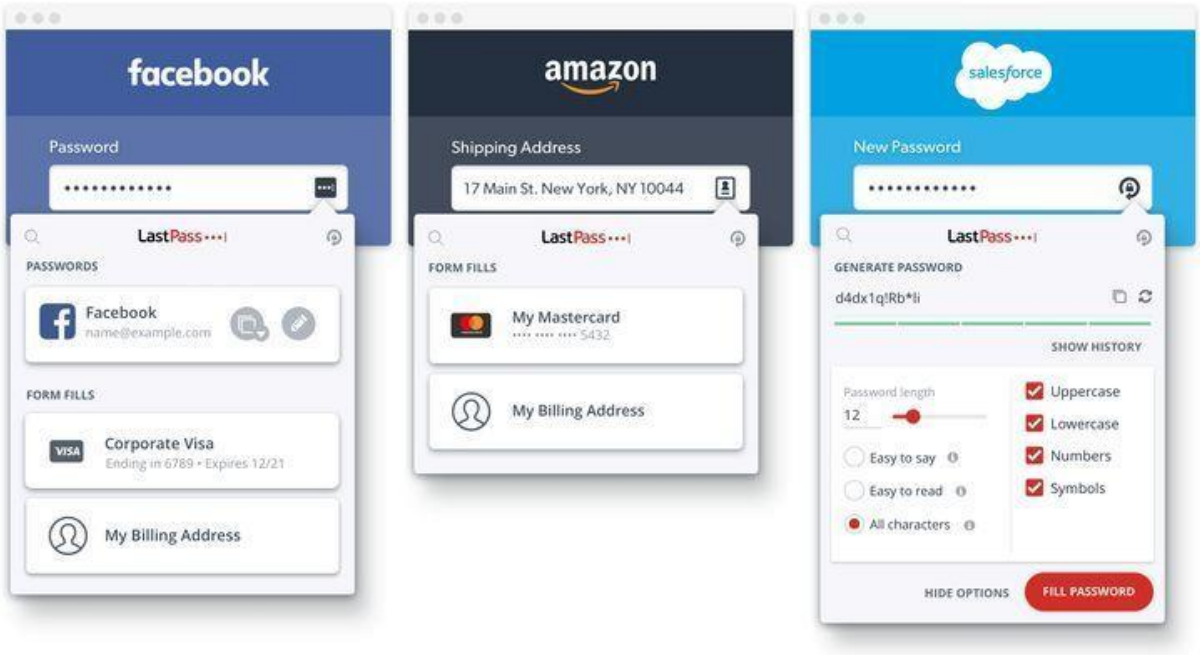
**3. Periksa pembaruan firmware**

Sama seperti komputer, produsen router juga senantiasa berusaha untuk mencari celah kerentanan dari router yang diproduksinya dan membuat penambalnya. Pada bagian administrator, ada menu khusus untuk melihat apakah ada pembaruan atas firmware router tersebut. Anda juga dapat merujuk ke situs web pabrikan untuk mengetahui firmware terkini.

# LAMPIRAN A

## CARA AKTIVASI DAN PENGGUNAAN LAST PASS

1. Unduh dan install ekstensi LastPass di browser Anda (Firewfox, Chrome)
2. Setelah terpasang, akan muncul ikon LastPass di toolsbar browser (bagaian kanan atas browser).
3. Klik ikon LastPass.
4. Pilih ‘Create an Account Now.’
5. Ketik alamat email dan buatlah password utama (master password) yang kuat.
6. Pada halaman utama, login menggunakan akun yang sudah dibuat.
7. Ketik username dan password.
8. Klik ikon Lastpass di dalam kolom password.
9. Klik ‘Save credentials for this site.’




Anda juga bisa masuk ke berbagai layanan dan aplikasi yang kalian pakai, lalu menyimpannya di Lastpass saat muncul pemberitahuan.

Setelah itu akun LastPass secara berkelanjutan menyimpan data Anda pada database penyimpanannya. Semua kata sandi dan informasi login Anda akan disimpan secara aman.

Ketika Anda mengunjungi website/layanan yang sudah didaftarkan di LastPass, maka secara otomatis LastPass akan memasukkan username dan password Anda.

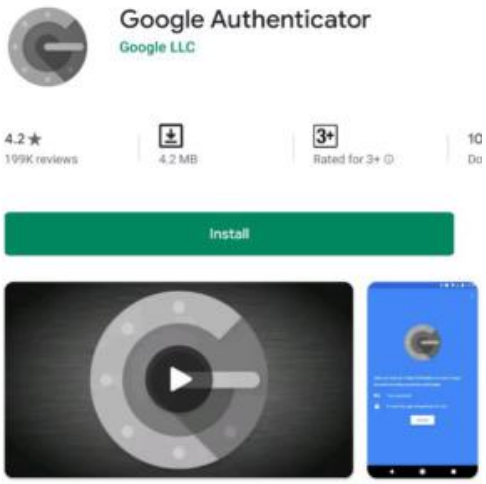
Jika Anda membutuhkan LastPass di perangkat yang lain, silakan unduh dan install dari Google Play atau Apple Appstore - sesuai perangkat yang Anda pakai. Nanti aplikasi akan melakukan sinkronisasi, sehingga Anda tidak perlu repot mengisi akun dan kata sandi di perangkat tersebut.

# LAMPIRAN B

## AKTIVASI DAN PENGGUNAAN GOOGLE AUTHENTICATOR DI AKUN GOOGLE

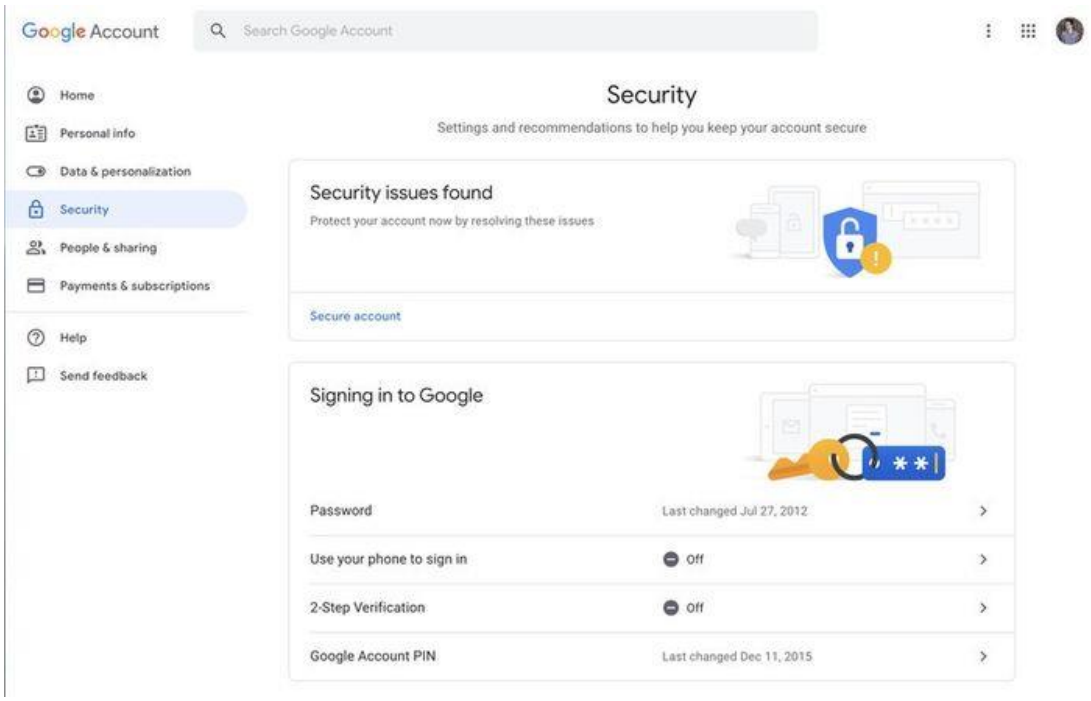
### A. Mempersiapkan Google Authenticator

1. Unduh dan install Google Authenticator dari Google Play Store (Android) atau Apple App Store (iOS) sesuai dangan ponsel Anda
2. Buka aplikasi Google Authenticator pada ponsel Anda dan
3. Login di Authenticator menggunakan akun Google Anda




### B. Aktivasi 2FA dengan Google Authenticator pada akun Google

1. Pada laptop, buka Akun Google melalui myaccount.google.com.




2. Di bagian atas, di panel navigasi, ketuk Security/Keamanan.
3. Di bagian "Login ke Google", ketuk Two Factor Authentication/ Verifikasi 2 Langkah. Anda mungkin akan diminta login.

4. Di bagian "Tambahkan langkah kedua lainnya untuk memverifikasi ini memang Anda", di bawah "Aplikasi Authenticator", ketuk Siapkan.
5. Ketika muncul pop up untuk memilih jenis perangkat Android atau iPhone, pilih perangkat yang Anda kehendaki. Sebuah kode barcode untuk perangkat tersebut akan ditampilkan.
6. Buka Aplikasi Google Authenticator pada ponsel Anda dan pilih scan barcode.
7. Dari ponsel, scan barcode yang ditampilan pada laptop (langkah no. 5). Setelah scan, akan muncul kode (6 digit) lalu klik tambah akun.
8. Kembali lagi ke laptop, jika sudah menambah akun, klik selanjutnya/next, akan muncul kotak untuk mengisi kode 6-digit dari Google Authenticator.
9. Masukan kode 6-digit yang ditampilkan oleh Google Authenticator pada kotak tersebut.
10. Klik verify dan selesai.