Checklist Keamanan dan Privasi Data Digital untuk Personal

No.	Kategori	Persyaratan	Penjelasan	Keterangan	*Checklist*
1.	Keamanan autentikasi	Menggunakan *password* yang kuat	▪ Jika *password* terlalu pendek, atau berisi kata-kata kamus, tempat atau nama, maka *password* tersebut dapat dengan mudah dibobol melalui serangan *brute force*, atau ditebak (*guessing*). ▪ Cara membuat *password* yang kuat: ○ Membuat *password* panjang 12+ karakter; ○ Menggunakan *passphrase*, yang terdiri dari banyak kata; ○ Menggunakan *password generator* untuk membuat *password* acak yang panjang dan kuat. ○ Menguji kekuatan *password* dengan *tools* untuk mendapatkan gambaran seberapa cepat *password* dapat dibobol, misalnya HowSecureIsMyPassword.net		
2.	Keamanan autentikasi	Jangan menggunakan *password* yang sama	Jika *password* yang sama digunakan di beberapa akun dan ketika salah satu akun mengalami kebocoran data, maka penjahat siber dapat dengan mudah mendapatkan akses tidak sah ke akun yang lain.		
3.	Keamanan autentikasi	Menggunakan aplikasi *password manager* yang aman	*Password manager* adalah aplikasi yang menghasilkan, menyimpan, dan mengisi otomatis kredensial *login*. Semua *password* akan dienkripsi dengan 1 *password* utama. Contohnya: Bitwarden, KeePass, LessPass, Padloc, ProtonPass, Pass.		
4.	Keamanan autentikasi	Menghindari berbagi *password*	Hindari berbagi *password* karena akan memudahkan akun untuk disusupi. Jika benar-benar perlu berbagi *password* saat bekerja dalam tim dengan akun bersama, maka harus menggunakan *password manager*.		
5.	Keamanan autentikasi	Mengaktifkan autentikasi dua faktor (*two factor authentication/*2FA)	▪ 2FA adalah metode autentikasi 2 lapis yang menggunakan kombinasi dari 2 faktor yang berbeda: faktor pengetahuan (*what you know*) dan faktor kepemilikan (*what you have*). Faktor kepemilikan dapat berupa token *software* dan token *hardware*. ▪ Token *software* sering berupa *one time password* (OTP), yang terdiri dari 4-8 digit *password* sekali pakai yang kedaluwarsa setelah jangka waktu tertentu. Token *software* dapat berupa: ○ Pesan yang dikirim melalui SMS, telepon, dan *email*.		

No.	Kategori	Persyaratan	Penjelasan	Keterangan	*Checklist*
			○ Kode yang dibangkitkan aplikasi autentikator, misalnya Google Authenticator, Authy, Microsoft Authenticator, LastPass Authenticator, dan Duo. ▪ Token *hardware,* dapat berupa key fob, kartu ID, dongle. Jika *password* bocor, maka penjahat siber tidak akan bisa masuk ke akun karena tidak memiliki akses ke informasi apa pun yang dibagikan atau dihasilkan oleh perangkat.		
6.	Keamanan autentikasi	Menyimpan kode cadangan (*backup code*) pada 2FA dengan aman	Ketika mengaktifkan 2FA, pengguna akan diberikan kode cadangan yang dapat digunakan jika metode 2FA hilang, rusak, atau tidak tersedia. Kode cadangan harus: ▪ Disimpan di tempat yang aman untuk mencegah kehilangan atau akses tidak sah; ▪ Dicetak di atas kertas atau disimpan tempat yang aman di *disk* (*harddisk* eksternal atau *harddisk* terenkripsi). ▪ Jangan menyimpan kode cadangan di *password manager*.		
7.	*Browsing web*	Memblokir iklan	Pengguna harus menggunakan *ad-blocker* karena: ▪ Dapat meningkatkan privasi pengguna: *ad-blocker* memblokir pelacak yang diterapkan iklan. Ketika iklan ditampilkan di halaman *web*, terdapat kemampuan untuk melacak pengguna, yaitu mengumpulkan data pribadi pengguna dan kebiasaannya, yang kemudian dapat dijual, atau digunakan untuk menampilkan iklan yang lebih tertarget. ▪ Membuat halaman *web* dimuat lebih cepat: menggunakan lebih sedikit data. ▪ Mencegah *malvertising*: *malware* yang menggunakan iklan situs *web* berbahaya atau yang dibajak, serta memasukkan iklan berbahaya ke dalam jaringan iklan yang sah untuk mengirimkan muatan berbahaya yang dapat berinteraksi langsung dengan pengguna atau menjalankan *script* tersembunyi. Contoh *ad-blocker* adalah uBlock Origin, yaitu *addon* pada *browser* yang bersifat *open source*.		
8.	*Browsing web*	Memastikan situs *web* yang sah	Pengguna diharapkan memeriksa kembali apakah URL-nya benar ketika masuk ke akun daring apa pun:		

No.	Kategori	Persyaratan	Penjelasan	Keterangan	*Checklist*
			▪ Menyimpan situs yang sering dikunjungi dengan *bookmark* ▪ Mengamati apakah terdapat tanda-tanda umum bahwa situs *web* tidak aman: ○ Terdapat peringatan (*warning*) pada *browser*; ○ Terjadi pengalihan (*redirect*); ○ Terdapat *spam* di situs *web*; dan ○ Terdapat *pop-up* pada situs *web*. ▪ Memeriksa situs web menggunakan alat seperti: ○ Virus Total (https://www.virustotal.com/gui/home/url); ○ IsLegitSite (https://www.islegitsite.com/); ○ URL Void (https://www.urlvoid.com/).		
9.	*Browsing web*	Hati-hati dengan *malware* pada *browser*	Sistem atau *browser* dapat disusupi oleh *spyware, miners, browser hijackers, malicious redirects, adware* dll. agar pengguna dapat tetap terlindungi dari *malware*: ▪ Mengabaikan *pop-up*; ▪ Waspada terhadap apa yang diklik; ▪ Jangan lanjutkan ke situs *web* jika browser memperingatkan bahwa situs tersebut berbahaya.		
10.	*Browsing web*	Menggunakan *browser* yang menghormati privasi pengguna	▪ Firefox dan Brave adalah *browser* yang aman, menghormati privasi, *open source*, mudah digunakan dan tersedia di semua sistem operasi. ▪ Hindari Google Chrome, Edge, dan Safari karena *browser* yang mengumpulkan data penggunaan dan mengizinkan pelacakan invasif.		
11.	*Browsing web*	Menghapus *addon browser* yang tidak perlu	*Addon* pada *browser* dapat melihat, mencatat, atau mengubah apa pun yang dilakukan pengguna pada *browser*. Situs *web* dapat melihat *addon* yang telah terpasang, dan dapat menggunakannya untuk menyempurnakan *signature*, agar dapat melacak pengguna dengan lebih akurat.		
12.	*Browsing web*	Memperbarui *browser*	Kerentanan *browser* terus-menerus ditemukan dan ditambal, jadi penting untuk selalu memperbaruinya, untuk menghindari eksploitasi *zero-day*.		
13.	*Browsing web*	Memeriksa HTTPS	Jika pengguna memasukkan informasi di situs *web* non-HTTPS, maka data dikirim tidak terenkripsi, sehingga dapat dibaca oleh siapa saja		

No.	Kategori	Persyaratan	Penjelasan	Keterangan	*Checklist*
			yang menyadapnya. Jangan memasukkan data apa pun di situs *web* non-HTTPS.		
14.	*Browsing web*	Menggunakan penyamaran (*incognito*)	Saat menggunakan komputer orang lain, pastikan menggunakan dalam mode *private*/*incognito* yang akan mencegah penyimpanan riwayat *browser* dan *cookie*.		
15.	*Browsing web*	Mengelola *cookie*	Menghapus *cookie* secara teratur adalah salah satu langkah untuk membantu mengurangi pelacakan oleh situs web. *Cookie* juga dapat menyimpan token *session* yang jika diambil, maka akan memungkinkan seseorang mengakses akun pengguna tanpa kredensial.		
16.	*Browsing web*	Memblokir pelacak (*tracking*) pihak ketiga	Memblokir pelacak akan membantu menghentikan situs web, *advertisers*, *analytics*, dan lainnya melacak pengguna di *background*. Contoh *tools* untuk memblokir pelacak, yaitu Privacy Badger dan uBlock Origin.		
17.	*Email*	Memiliki lebih dari satu alamat *email*	Pertimbangkan untuk menggunakan alamat *email* yang berbeda untuk komunikasi yang penting dan komunikasi biasa. Pembagian ini dapat mengurangi jumlah kerugian yang disebabkan oleh pelanggaran data (*data breach*), dan juga mempermudah pemulihan akun yang disusupi.		
18.	*Email*	Menjaga kerahasiaan alamat *email*	Jangan bagikan *email* utama secara publik, karena alamat *email* sering kali menjadi titik awal serangan *phishing*.		
19.	*Email*	Mengamankan akun *email*	Menggunakan *password* yang kuat, mengaktifkan 2FA, dan berhati-hati ketika *login* pada akun *email* karena akun *email* menyediakan titik masuk yang mudah ke semua akun *online* yang lain.		
20.	*Email*	Menonaktifkan *loading* otomatis pada *remote content*	Pesan *email* dapat berisi *remote content* seperti gambar atau *stylesheet* yang sering kali dimuat secara otomatis dari *server*. Pengguna harus menonaktifkan fitur ini karena dapat memperlihatkan alamat IP dan informasi perangkat, dan sering digunakan untuk pelacakan.		
21.	Perpesanan (*messaging*)	Menggunakan aplikasi perpesanan yang memberikan *end-to-end encryption*	*End-to-end encryption* adalah sistem komunikasi di mana pesan dienkripsi pada perangkat dan tidak didekripsi hingga mencapai penerima yang dituju. Hal ini memastikan bahwa isi pesan tidak dapat membaca jika disadap begitu pula jika disimpan *di* server pusat.		

No.	Kategori	Persyaratan	Penjelasan	Keterangan	*Checklist*
22.	Perpesanan (*messaging*)	Menggunakan aplikasi perpesanan yang tepercaya	Pastikan aplikasi perpesanan *open source*, stabil, dipelihara secara aktif, dan didukung oleh pengembang tepercaya.		
23.	Perpesanan (*messaging*)	Memeriksa *setting* keamanan	Memeriksa pengaturan keamanan, seperti menggunakan *password* yang kuat, mengaktifkan 2FA, verifikasi kontak, pemberitahuan keamanan, dan enkripsi.		
24.	Perpesanan (*messaging*)	Memeriksa pengaturan privasi	Memeriksa pengaturan privasi seperti *read receipt*, *online* terakhir, dan pemberitahuan pengetikan, serta fitur privasi lainnya.		
25.	Perpesanan (*messaging*)	Pastikan perangkat dan jaringan yang digunakan sudah aman	Terdapat beberapa titik di mana komunikasi digital dapat dipantau atau disadap, yaitu perangkat, jaringan, penyedia aplikasi perpesanan, dan *server*. Oleh karena itu, pengguna harus memastikan perangkat dan jaringan yang digunakan sudah aman.		
26.	Perpesanan (*messaging*)	Pastikan grup *chat* aman	Risiko kompromi meningkat jika semakin banyak peserta dalam suatu grup karena meningkatnya *attack surface*. Periksa secara berkala apakah semua peserta di grup adalah pihak yang sah.		
27.	Media sosial	Mengamankan akun media sosial	Memeriksa pengaturan keamanan, seperti menggunakan *password* yang kuat dan mengaktifkan 2FA.		
28.	Media sosial	Memeriksa pengaturan privasi	Sebagian besar media sosial memungkinkan pengguna mengontrol pengaturan privasi. Pengaturan disesuaikan dengan perasaan nyaman dengan data apa yang diungkapkan dan kepada siapa.		
29.	Media sosial	Pertimbangkan semua interaksi sebagai sesuatu yang publik	Banyak metode untuk melihat konten *private* pengguna di media sosial. Oleh karena itu, sebelum mengunggah, mem-*posting*, atau mengomentari apa pun, pikirkan "Bolehkah saya melakukan ini jika hal ini bersifat publik?"		
30.	Media sosial	Pertimbangkan semua interaksi sebagai sesuatu yang permanen	Hampir setiap kiriman, komentar, foto, dan lainnya di media sosial terus-menerus dicadangkan oleh berbagai layanan pihak ketiga, yang mengarsipkan data ini dan menjadikannya dapat diindeks dan tersedia untuk umum hampir selamanya.		
31.	Media sosial	Tidak terlalu banyak mengungkap informasi	Informasi profil pengguna menciptakan tambang emas informasi bagi *hacker* karena semua data dapat membantu melakukan *profiling* calon korban penipuan *phishing*. Oleh karena itu, hindari berbagi terlalu banyak informasi.		

No.	Kategori	Persyaratan	Penjelasan	Keterangan	*Checklist*
32.	Media sosial	Berhati-hati dengan informasi yang di-*upload*	Pembaruan status, komentar, *check-in*, dan media dapat secara tidak sengaja mengungkapkan lebih banyak hal daripada yang diinginkan. Hal ini terutama berlaku untuk foto dan video, yang mungkin menampilkan berbagai hal di latar belakang.		
33.	Media sosial	Tidak membagikan *email* dan nomor telepon	Memposting alamat *email* atau nomor telepon akan memberikan lebih banyak informasi bagi para *hacker* dan penipu untuk digunakan melakukan kejahatan *online.*		
34.	Media sosial	Tidak memberikan izin (*permission*) yang tidak perlu	Secara *default*, banyak aplikasi media sosial yang meminta izin untuk mengakses kontak, log panggilan, lokasi, riwayat pesan, dll. Jika aplikasi media sosial tidak membutuhkan akses ini, jangan berikan.		
35.	Media sosial	Hindari mempublikasi-kan data geolokasi saat masih berada di tempat tersebut	Jika berencana membagikan konten apa pun yang mengungkapkan suatu lokasi, maka tunggulah hingga meninggalkan tempat tersebut. Hal ini sangat penting untuk diperhatikan terutama ketika pengguna sedang melakukan perjalanan, di restoran, kampus, hotel/resort, gedung publik atau bandara.		
36.	Jaringan	Menggunakan jaringan yang aman	Perhatikan keamanan jaringan yang digunakan, hindari penggunaan WiFi publik tanpa menggunakan VPN karena berisiko terjadi pelanggaran data (*data breach*).		
37.	*Smartphone*	Mengaktifkan fitur enkripsi *smartphone* ke SD *card*	Untuk menjaga data SD *card* aman dari akses fisik, maka gunakan enkripsi *file*. Artinya, jika SD *card* hilang atau dicuri, maka data didalamnya tidak dapat diakses.		
38.	*Smartphone*	Mengaktifkan fitur *remote wipe* pada *smartphone*	Untuk menjaga data *smartphone* aman dari akses fisik, maka aktifkan fitur *remote wipe* yang disediakan oleh aplikasi Find My Device (Android) dan Find My (iPhone).		
39.	*Smartphone*	Mematikan fitur konektivitas yang tidak digunakan	Saat tidak menggunakan WiFi, Bluetooth, NFC dll, maka matikan fitur tersebut. Terdapat beberapa ancaman umum yang menggunakan fitur ini.		
40.	*Smartphone*	Pertahankan jumlah aplikasi seminimal mungkin	*Uninstall* aplikasi yang tidak diperlukan atau digunakan secara rutin. Karena aplikasi sering kali berjalan di *background*, tidak hanya memperlambat perangkat, tetapi juga mengumpulkan data.		
41.	*Smartphone*	Memperhatikan izin aplikasi	Jangan berikan izin pada aplikasi (*permission*) yang tidak diperlukan.		

No.	Kategori	Persyaratan	Penjelasan	Keterangan	*Checklist*
42.	*Smartphone*	Hanya instal aplikasi dari sumber resmi	Aplikasi di Apple App Store dan Google Play Store di-*scan* dan di-*sign* secara kriptografis, sehingga mengurangi kemungkinan *malware*.		
43.	Komputer personal	Selalu memperbarui sistem komputer	Pembaruan sistem berisi perbaikan/tambalan untuk masalah keamanan, meningkatkan kinerja, dan terkadang menambahkan fitur baru. Lakukan pembaruan saat diminta oleh sistem.		
44.	Komputer personal	Mengenkripsi *harddisk* komputer	Menggunakan BitLocker untuk Windows, FileVault di MacOS, atau LUKS di Linux, untuk mengaktifkan enkripsi *disk*. Hal ini mencegah akses tidak sah jika komputer hilang atau dicuri.		
45.	Komputer personal	Mencadangkan (*back u*p) data penting	Mempertahankan cadangan terenkripsi mencegah kehilangan karena *ransomware*, pencurian, atau kerusakan.		
46.	Komputer personal	Berhati-hatilah memasukkan perangkat USB ke komputer	Perangkat USB dapat menimbulkan ancaman serius, seperti USB Rubber Ducky, USB Killer, atau USB yang mengandung *malware.*		
47.	Komputer personal	Mengaktifkan kunci layar (*screen lock*) saat kondisi *idle*	Mengunci komputer saat pergi dan mengatur agar memerlukan *password* saat melanjutkan dari *screensaver* atau mode *sleep* untuk mencegah akses tidak sah.		
48.	Komputer personal	Menonaktifkan Cortana (Windows) atau Siri (Mac)	*Voice-controlled assistants* dapat mempunyai dampak privasi karena data dikirim kembali untuk diproses. Nonaktifkan fitur tersebut atau batasi kemampuan untuk mendengarkan.		
49.	Komputer personal	Meninjau aplikasi ter-*install*	Minimalkan aplikasi yang terinstal untuk mengurangi kerentanan dan menghapus *cache* aplikasi secara berkala.		
50.	Komputer personal	Mengelola izin (*permission*) aplikasi	Mengontrol aplikasi mana yang memiliki akses ke lokasi, kamera, mikrofon, kontak, dan informasi sensitif lainnya.		
51.	Komputer personal	Melarang penggunaan data dikirim ke *cloud*	Membatasi jumlah informasi penggunaan atau *feedback* yang dikirim ke *cloud* untuk melindungi privasi.		
52.	Komputer personal	Menghindari metode membuka kunci (*unlock*) yang cepat	Menggunakan *password* yang kuat daripada biometrik atau PIN yang pendek untuk membuka kunci komputer guna meningkatkan keamanan.		

No.	Kategori	Persyaratan	Penjelasan	Keterangan	*Checklist*
53.	Komputer personal	Matikan komputer, daripada *standby*	Matikan perangkat saat tidak digunakan, terutama jika *disk* dienkripsi, untuk menjaga keamanan data.		
54.	Keamanan fisik	Menghancur-kan dokumen sensitif	Merusak dokumen sensitif sebelum dibuang untuk melindungi dari pencurian identitas dan menjaga kerahasiaan.		
55.	Keamanan fisik	Menggunakan perimeter keamanan	Memastikan keamanan fisik lokasi penyimpanan perangkat informasi pribadi, meminimalkan akses eksternal dan menggunakan sistem deteksi intrusi, seperti *alarm*.		
56.	Keamanan fisik	Memastikan perangkat aman secara fisik	Menggunakan perlengkapan untuk mendukung keamanan fisik seperti kunci Kensington, penutup *webcam*, dan layar privasi pada perangkat.		
57.	Keamanan fisik	Menjauhkan perangkat dari jendela rumah	Mencegah perangkat agar tidak terlihat dari luar untuk mengurangi risiko pencurian.		
58.	Keamanan fisik	Melindungi entri PIN dari orang lain atau kamera	Melindungi entri PIN dari orang lain dan kamera, serta bersihkan *screen touch* setelah digunakan.		
59.	Keamanan fisik	Memeriksa mesin ATM dari *skimmer*	Memeriksa ATM dan perangkat publik terhadap perangkat *skimmer* dan tanda-tanda gangguan sebelum digunakan.		
60.	Aspek manusia	Memverifikasi penerima	*Email* dapat dengan mudah dipalsukan, sehingga perlu melakukan verifikasi keaslian pengirim, terutama untuk informasi yang sensitif.		
61.	Aspek manusia	Jangan mudah percayai pada notifikasi *popup*	*Popup* palsu dapat disebarkan oleh penjahat siber, oleh kare itu selalu periksa URL sebelum memasukkan informasi apa pun pada *popup*.		
62.	Aspek manusia	Jangan meninggalkan perangkat tanpa pengawasan	Perangkat tanpa pengawasan dapat disusupi bahkan dicuri sehingga informasi di dalam perangkat bisa bocor.		
63.	Aspek manusia	Mencegah *camfecting* (peretasan pada perangkat)	Melindungi komputer dari gangguan kamera dengan menggunakan penutup *webcam* dan pemblokir mikrofon. Bisukan *home assistants* saat tidak digunakan atau sedang mendiskusikan masalah sensitif.		

No.	Kategori	Persyaratan	Penjelasan	Keterangan	*Checklist*
64.	Aspek manusia	Melindungi diri dari peselancar bahu (*shoulder surfer*)	Menggunakan *privacy screen* di laptop dan *smartphone* untuk mencegah orang lain membaca layar ketika berada di ruang publik.		
65.	Aspek manusia	Mendidik diri sendiri tentang serangan *phishing*	Berhati-hatilah terhadap upaya *phishing* dengan cara:. memverifikasi URL, memahami konteks pesan yang diterima, dan menerapkan praktik keamanan yang baik seperti menggunakan 2FA dan tidak menggunakan *password* berulang.		
66.	Aspek manusia	Meng-*install software* tepercaya dari sumber tepercaya	Hanya mengunduh *software* dari sumber yang sah dan memeriksa *file* dengan *tools* seperti Virus Total (https://www.virustotal.com/gui/home/upload) sebelum instalasi.		