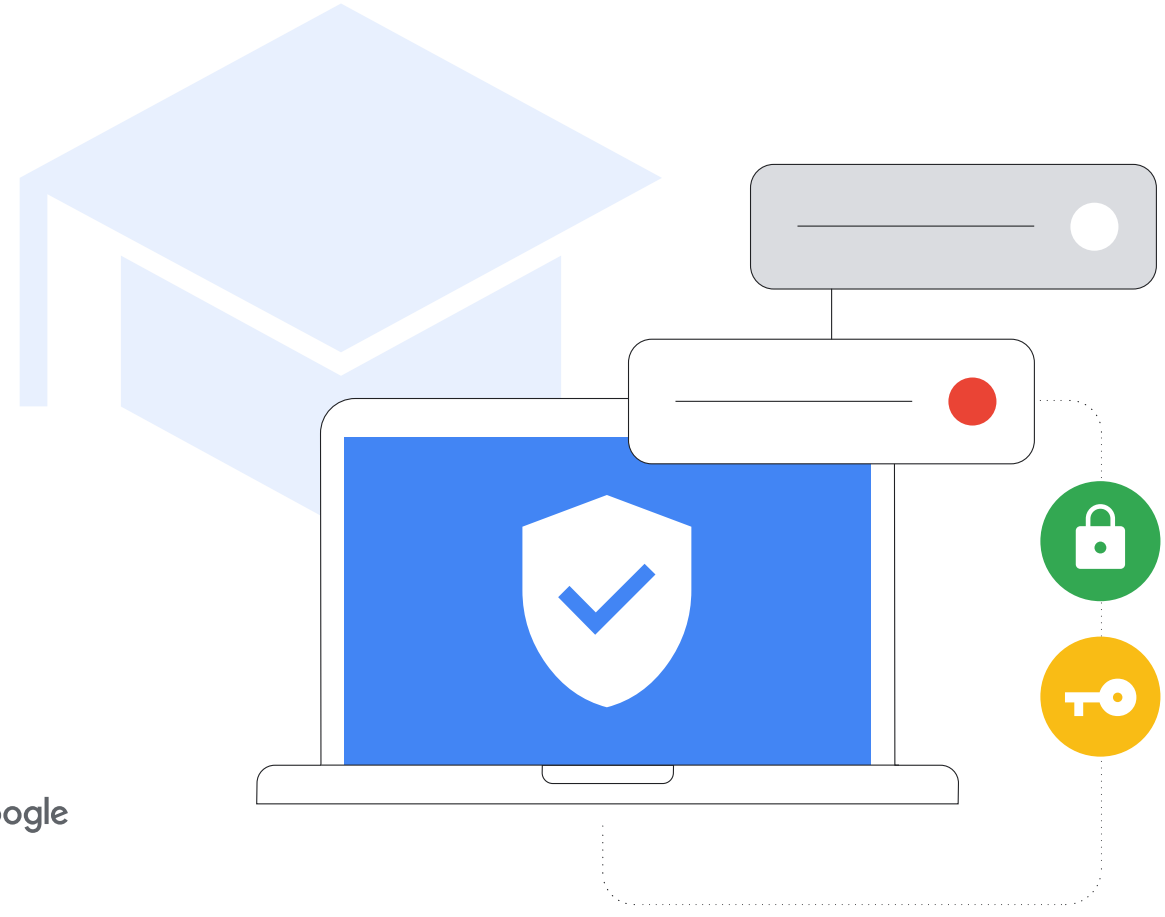
Google for Education

Buku Panduan Keselamatan Siber K-12

Dikemaskinikan pada bulan Ogos 2023



Safer with Google

Ringkasan Eksekutif

Seperti yang ditekankandalam laporan Protecting Our Future oleh CISA, pelaburan dalam keselamatan siber adalah sangat penting bagi institusi K-12 untuk melindungi pelajar, keluarga, guru, kakitangan dan komuniti mereka. Dokumen ini memberikan panduan dan amalan terbaik kepada pentadbir IT sekolah tentang cara menyediakan dan mengkonfigurasikan perkakasan serta perisian di institusi K-12 untuk mengukuhkan keselamatan siber. Dokumen ini mengandungi amalan terbaik umum dan juga panduan khusus untuk produk dan perkhidmatan Google. Misi Google untuk mengatur maklumat dunia dan menjadikan maklumat tersebut boleh diakses serta berguna kepada semua merupakan pendorong yang penting kepada usaha yang dilakukan oleh pasukan Google for Education: membina alatan yang direka bentuk untuk pengajaran dan pembelajaran. Kami akan berkongsi pelajaran daripada usaha tersebut dalam panduan ini.

Kami menyediakan amalan keselamatan terbaik mengikut topik yang memberikan gambaran lebih mendalam tentang konfigurasi, persediaan dan strategi pengurangan risiko. Kami juga menerangkan pendekatan Google terhadap keselamatan siber untuk perkhidmatan kami, terutamanya alatan pendidikan kami. Walaupun panduan terperinci yang kami berikan dalam dokumen ini terpakai secara umum kepada mana-mana produk atau perkhidmatan, kami percaya bahawa produk kami menawarkan perlindungan yang kukuh daripada serangan yang biasa berlaku sebaik sahaja digunakan.

Risiko

Institusi pendidikan merupakan sasaran utama bagi serangan siber, dan pelaku jahat berusaha untuk mengambil kesempatan terhadap persekitaran sekolah yang kaya dengan data untuk keuntungan mereka sendiri. 46% daripada sekolah yang belum disasarkan percaya bahawa lambat laun mereka akan diserang kerana serangan perisian tebusan kini semakin canggih — dan lebih sukar dibendung. 42% daripada sekolah ini berpendapat perisian tebusan kini sangat tersebar luas dan serangan ini tidak dapat dielakkan lagi. Keperluan sekolah untuk beralih kepada pembelajaran jarak jauh dengan pantas pada tahun 2020 merupakan penyumbang besar kepada jurang keselamatan siber, sekali gus mendedahkan sekolah kepada serangan siber.

Pertahanan

Serangan tersebut boleh dikurangkan. Walaupun tiada teknologi yang dapat menghapuskan risiko ini sepenuhnya, sektor pendidikan dan vendor teknologi pendidikan boleh bekerjasama untuk menggunakan serta melaksanakan amalan terbaik untuk menghasilkan pendekatan yang selamat, terjamin dan menyeluruh demi mengurangkan risiko anda dengan ketara. Melalui pelaksanaan langkah berjaga-jaga dan dasar yang betul untuk melindungi pengguna, menjadikan peranti selamat dan memastikan privasi data, institusi pendidikan boleh mengurus risiko dan mengurangkan serangan dengan lebih baik.

Syor Utama:

- **GUNAKAN PENGESAHAN YANG SELAMAT** untuk memastikan keselamatan maklumat sensitif, melindungi e-mel, fail dan kandungan lain serta menghalang pengguna yang tidak dibenarkan daripada mengakses sistem pendidikan. Gunakan amalan terbaik untuk pengesahan pengguna, termasuk kata laluan kukuh dan pengesahan 2 langkah (2SV), kunci laluan dan pengurus kata laluan apabila boleh, terutamanya bagi pentadbir IT dan kakitangan yang mengendalikan maklumat sensitif.
- **GUNAKAN TETAPAN KESELAMATAN YANG BERSESUAIAN** untuk memastikan keselamatan pengguna, data dan persekitaran anda. Walaupun produk Google dibina dengan ciri keselamatan secara lalai, pentadbir juga hendaklah menggunakan dan mengkonfigurasikan rangkaian serta sistem dengan betul untuk memastikan keselamatan. Untuk memastikan sekolah selamat, gunakan prinsip sifar keyakinan dan keistimewaan paling rendah: pengguna hanya boleh mendapat akses kepada perisian, data, aplikasi dan sistem yang mereka perlukan untuk bekerja dengan cekap.
- **KEMAS KINIKAN DAN TINGKATKAN SISTEM ANDA** untuk memastikan pengguna dilindungi daripada ancaman terbaharu. Gunakan sistem pengendalian (OS) dan penyemak imbas moden serta pastikan pengguna menggunakan versi perisian yang terkini pada semua peranti (atau versi stabil jangka masa panjang yang telah diluluskan) dan pastikan mereka mengemaskinikan perisian itu secara automatik. Peningkatan kepada penyelesaian yang lebih selamat, seperti Chromebook, boleh meningkatkan keselamatan. Tiada perisian tebusan pernah dikesan pada peranti ChromeOS.
- **GUNAKAN SISTEM PEMAKLUMAN DAN PEMANTAUAN MASA NYATA** untuk meningkatkan postur keselamatan anda dan mengurangkan kemungkinan masalah dengan pantas. Anda boleh menggunakan ciri ini yang terbina dalam perisian kerjasama dan komunikasi utama seperti Google Workspace for Education atau mengerah tugas penyelesaian log dan pemantauan keselamatan yang berasingan. Pastikan penjejakan aktiviti dibuat secara menyeluruh dalam semua rangkaian, peranti, aplikasi, pengguna dan data sekolah anda. Pantau log masuk akaun, perkongsian fail, jumlah e-mel (terutamanya percubaan pancingan data dan perisian hasad), aktiviti peranti dan perubahan konfigurasi. Pastikan penyelesaian pemakluman dan pemantauan sentiasa dikemaskinikan untuk menerima pemberitahuan tentang ancaman, peristiwa kritikal dan perubahan sistem.
- **LATIH GURU, KAKITANGAN DAN PELAJAR** tentang cara menggunakan peranti dan perisian dengan selamat, mengenal pasti dan melaporkan kemungkinan ancaman serta berkongsi data dengan sewajarnya untuk melindungi mereka daripada serangan yang paling biasa berlaku. Sekolah atau daerah boleh membuat bahan latihan berjenama di samping menggunakan bahan sedia guna yang tersedia untuk menghasilkan kit alat yang menyeluruh bagi sekolah.

1 https://www.cisa.gov/protecting-our-future-cybersecurity-k-12

Syor khusus untuk pengguna produk Google: Produk Google seperti Google Workspace for Education dan Chromebook boleh meningkatkan keselamatan siber sekolah anda dan menjadikan setiap syor ini mudah dilaksanakan. Gabungan produk ini menyediakan penyelesaian menyeluruh yang membantu untuk melindungi privasi pengguna dan memberikan keselamatan yang terbaik dalam industri kepada institusi anda.

Strategi ini, bersama-sama dengan bimbingan tambahan yang disediakan dalam dokumen yang seterusnya, membentuk asas yang terbaik untuk keselamatan institusi K-12.

Pendekatan Google terhadap Pendidikan

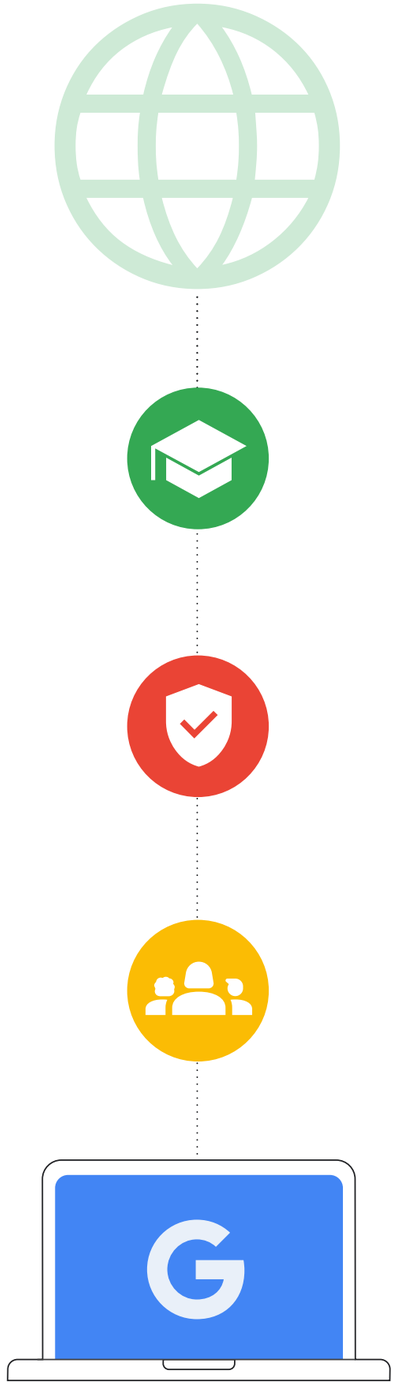
Misi Google adalah untuk menyusunmaklumat dunia dan menjadikan maklumat tersebut boleh diakses serta berguna kepada semua, lebih-lebih lagi dalam sektor pendidikan. Dalam pasukan Google for Education, kami mencapai misi tersebut dengan membina alatan seperti Chromebook dan Google Classroom yang membolehkan pelajar dan guru membuat, berkongsi dan menyusun kandungan mereka sendiri, di samping mengakses dan menggunakan sumber pendidikan serta alatan dalam talian dengan mudah lagi selamat.

Sekolah berhak untuk mendapat teknologi yang selamat secara lalai, direka bentuk untuk privasi, memastikan anda memiliki kawalan serta mengandungi kandungan dan maklumat yang boleh dipercayai. Dengan produk seperti Chromebook dan Google Workspace for Education, sekolah memperoleh penyelesaian keselamatan yang terbaik dalam industri dan mematuhi standard pendidikan global yang paling tinggi, pentadbir IT mendapat keterlihatan penuh dan kawalan yang lancar terhadap dasar data dan keselamatan mereka, manakala pelajar boleh melibatkan diri sepenuhnya dalam pembelajaran menerusi persekitaran digital yang lebih selamat selain menyediakan kandungan berdasarkan umur serta mengurangkan spam dan ancaman siber.

Kami telah mengutamakan ciri dan kawalan keselamatan yang terbina dalam, tahap standard privasi yang paling tinggi dan pilihan alatan keselamatan yang lebih proaktif untuk memastikan pembelajaran yang selamat untuk semua orang. Peranti ChromeOS membantu untuk mengurangkan ancaman yang dihadapi oleh sekolah, dan menjadi pertahanan terbaik untuk menentang ancaman utama kepada sekolah iaitu perisian tebusan, kerana tiada serangan perisian tebusan yang telah berjaya menjejaskan Chromebook.

Sementara itu, Google Workspace for Education ialah salah satu set komunikasi dan kerjasama berasaskan awan yang paling popular serta selamat di dunia. Untuk mendapatkan maklumat lanjut tentang cara setiap produk melindungi keselamatan siber berhubung dengan syor yang dinyatakan di sini, sila rujuk bahagian terakhir.

Dokumen ini dibahagikan kepada dua bahagian - bahagian pertama menyediakan bimbingan keselamatan praktikal dan umum untuk institusi K-12 tanpa mengira produk, manakala bahagian kedua menyediakan bimbingan konfigurasi khusus untuk institusi yang menggunakan produk Google for Education seperti Google Workspace for Education dan Chromebook. Kedua-dua bahagian menyediakan maklumat yang membantu untuk melindungi keselamatan anda dan pelajar anda dalam talian.



Pengenalan

Institusi K-12 - peranti dan juga rangkaian mereka - berisiko tinggi berdepan serangan siber. Institusi K-12 hendaklah melaksanakan ciri keselamatan yang terbaik untuk melindungi pelajar dan mencegah kehilangan data, perkhidmatan, sumber, masa dan wang yang boleh berlaku akibat daripada serangan ini. (Sumber)

Panduan ini merupakan alat yang mempromosikan amalan keselamatan siber terbaik yang harus dilaksanakan oleh pentadbir sekolah dan sistem sekolah untuk menjamin keselamatan persekitaran mereka dengan lebih baik. Dengan melaksanakan amalan terbaik ini, institusi K-12 boleh mengurangkan atau mencegah serangan siber yang serius dan menelan kos yang besar terhadap sistem pendidikan dan melindungi pelajar, keluarga, guru serta kakitangan.

Serangan siber yang menyasarkan sekolah semakin meningkat dari segi kekerapan dan kemudaratan. Menurut Pusat Sumber Keselamatan Siber K-12, terdapat lebih daripada 1,300 insiden siber yang didedahkan kepada umum yang melibatkan organisasi pendidikan di semua 50 negeri dari tahun 2016 hingga 2021. Pemimpin pendidikan masa kini mestilah melindungi data dan maklumat peribadi pelajar, guru dan kakitangan serta sistem dan maklumat institusi mereka. Tugas ini agak berat, terutamanya memandangkan pendidikan lazimnya lebih sukar mengikuti perkembangan keselamatan siber berbanding dengan sektor lain.

Serangan siber yang berjaya, termasuk perisian tebusan, pancingan data, perisian hasad dan pelbagai lagi, boleh menyebabkan pelanggaran data berskala besar bagi maklumat peribadi yang boleh dikenal pasti (PII), bayaran yang mahal (purata bayaran tebusan meningkat 5 kali sejak tahun 2020 kepada $812,260) dan menyebabkan gangguan berpanjangan kepada pengajaran dan operasi sekolah yang lain. Baru-baru ini, satu serangan perisian tebusan berjaya melumpuhkan seluruh sistem sekolah, lalu menyebabkan kesan riak kepada seluruh komuniti kerana pelajar tidak dapat pergi ke sekolah selama berhari-hari. Dengan sumber dan dana yang terhad, organisasi K-12 akan terus menjadi sasaran utama peluang serangan melainkan keselamatan siber ditingkatkan.

Perlaksanaan keselamatan siber yang terbaik adalah melalui komunikasi, kerjasama dan perkongsian. Dokumen ini telah disusun berdasarkan petua keselamatan Google, Rangka Kerja Keselamatan Siber Institut Piawaian dan Teknologi Kebangsaan (NIST) dan Kit Alat dan Syor Keselamatan Siber K-12 CISA tahun 2023 - sumber amalan keselamatan siber terbaik yang diterima secara meluas. Dokumen ini membincangkan langkah umum yang harus diambil atau dipertimbangkan oleh pentadbir IT, beberapa amalan terbaik dan panduan Google sendiri untuk produk kami serta merujuk petua dan perkhidmatan keselamatan yang ditawarkan oleh syarikat lain. Pentadbir hendaklah menyemak semua panduan keselamatan yang disediakan oleh syarikat yang berkaitan dan melaksanakan panduan terkini mereka, memandangkan syarikat yang bertanggungjawab itu dapat menerangkan produk mereka sendiri dan sebarang perubahan yang mungkin telah berlaku dengan lebih baik.

Sebelum melaksanakan syor yang disenaraikan di bawah, anda hendaklah juga mempertimbangkan faktor yang berikut:

Pertimbangan

1. **Melindungi populasi pelajar anda.**
Keperluan setiap sekolah berbeza-beza dan populasi tertentu mungkin memerlukan langkah tambahan untuk melindungi keselamatan dan privasi. Kebanyakan alatan teknologi pendidikan memiliki ciri yang membantu dari segi akses berdasarkan umur, seperti mengehadkan kandungan tidak sesuai atau memastikan data lokasi dan hubungan mereka kekal sulit.

2. **Jenis data yang anda simpan.**
Jika anda menyimpan data sensitif, anda mungkin mahu menyulitkan data atau menyimpan data tersebut di lokasi yang berasingan.

3. **Jenis peranti yang anda gunakan dan model kerah tugas anda.**
Peranti dan aplikasi yang berkaitan hendaklah dikemaskinikan secara automatik untuk memaksimumkan keselamatan, menyulitkan data dan mengasingkan akaun untuk memastikan pengguna hanya memiliki akses kepada maklumat mereka sendiri.

4. **Dasar sekolah, daerah atau wilayah anda.**
Sekolah anda mungkin telah menetapkan dasar yang khusus berkaitan dengan penggunaan teknologi. Anda perlu memastikan bahawa semua perlindungan disediakan mengikut dasar ini.

Setiap hari,
Gmail menghalang
100 juta
percubaan pancingan data.

Setiap minggu,
Google mengenal pasti
300,000
laman web yang tidak selamat.

Setiap hari,
74 juta
pengguna mendapatkan bantuan daripada Password Manager Google.

Setiap tahun,
700 juta
pengguna memperkukuh keselamatan mereka dengan Pemeriksaan Keselamatan.

Gunakan Pengesahan yang Selamat

Pengesahan yang selamat mestilah menjadi keutamaan tertinggi bagi sekolah dan institusi lain. Dalam suku tahun keempat 2022, akaun yang lemah dan tanpa bukti kelayakan mencakup 48% daripada semua faktor penjejasan dalam insiden pelanggaran. Pelaksanaan beberapa syor penting boleh membantu untuk mengesahkan identiti pengguna dan mengehadkan akses kepada maklumat yang bersesuaian dengan peranan setiap pengguna.

Pentadbir IT hendaklah menguatkuasakan penggunaan pengesahan 2 langkah (2SV) (juga dikenali sebagai pengesahan dua faktor (2FA)) dan beralih kepada pengesahan tanpa kata laluan (iaitu, kunci laluan) apabila boleh, terutamanya apabila seseorang mengakses sistem institusi pendidikan dari jauh. 2SV menambahkan lapisan keselamatan tambahan pada akaun dalam talian anda, yang lebih menyukarkan penyerang untuk memperoleh akses kepada akaun anda.

Terdapat banyak jenis peranti dan model kerah tugas yang digunakan oleh sekolah pada masa kini dan kebolehan teknikal dalam persekitaran K-12 adalah berbeza-beza. Keselamatan akaun dan peranti berbeza-beza mengikut peranan dan jenis pengguna dengan amalan terbaik yang ditetapkan: Pentadbir IT, guru dan kakitangan, pelajar sekolah menengah menggunakan peranti yang ditetapkan, dan pelajar sekolah rendah menggunakan peranti yang dikongsi. Kami membincangkan syor yang khusus untuk setiap kumpulan di bawah.

Terdapat beberapa jenis kaedah pengesahan yang merupakan amalan terbaik dalam kebanyakan keadaan:

- **Kata laluan kukuh:**
  Gesa pengguna untuk membuat kata laluan mereka sendiri semasa log masuk kali pertama yang mematuhi syarat teknikal minimum dari segi panjang dan kerumitan kata laluan. Ungkapan laluan yang lebih panjang memberikan elemen keselamatan tambahan disebabkan oleh panjang dan penggunaan aksara yang rumit. Pengguna tidak seharusnya dikehendaki untuk mengubah kata laluan mereka secara kerap kerana hal itu mendorong pengguna untuk menggunakan kata laluan yang lebih ringkas atau membuat perubahan tidak penting (seperti menukar satu aksara).
- **Pengesahan 2 langkah (2SV):**
  2SV melindungi akaun dengan langkah kedua - lazimnya sesuatu yang dimiliki oleh pengguna, seperti kunci keselamatan atau apl pada telefon mudah alih yang menghasilkan kod pengesahan satu kali. Walaupun sebarang bentuk 2SV meningkatkan keselamatan akaun, pentadbir hendaklah mengelakkan penggunaan kod pengesahan yang dihantar melalui teks atau panggilan kerana kaedah ini boleh terdedah kepada serangan berdasarkan nombor telefon.
- **Pengesahan tanpa kata laluan:**
  Kunci laluan ialah alternatif yang lebih selamat dan mudah berbanding dengan kata laluan. Pengguna boleh log masuk ke apl dan laman web menggunakan PIN, corak, penderia biometrik (seperti cap jari atau pengecaman wajah) atau ketik kunci keselamatan, yang tidak memerlukan mereka untuk mengingati dan mengurus kata laluan. Walaupun mungkin tidak bersesuaian dengan setiap konteks pendidikan, kaedah ini semakin kerap menggantikan bentuk pengesahan tradisional bahkan menjadikan log masuk lebih selamat dan pantas. Kunci laluan melindungi pengguna daripada serangan pancingan data memandangkan kaedah ini hanya berfungsi pada laman web dan apl berdaftar bagi kunci laluan tersebut.
- **Log Masuk Sekali (SSO):**
  SSO membenarkan pengguna mengakses berbilang aplikasi dan laman web dengan satu set bukti kelayakan. Apabila pengguna hanya perlu ingat satu set bukti kelayakan, mereka kurang cenderung untuk mencatat maklumat tersebut. Di samping itu, apabila sekolah tidak perlu mengurus berbilang set bukti kelayakan pengguna, mereka boleh menjimatkan kos untuk sokongan dan meja bantuan IT. Google Workspace for Education menyokong SSO secara natif, maka pengguna boleh menggunakan bukti kelayakan Google Account mereka untuk log masuk ke aplikasi pihak ketiga, atau mereka boleh menggunakan bukti kelayakan penyedia lain untuk log masuk ke Google Account mereka..
- **Pengurus kata laluan:**
  Pengurus kata laluan boleh membantu pengguna membuat kata laluan yang kukuh dan unik bagi semua akaun serta perkhidmatan yang digunakan oleh mereka semasa hari persekolahan dan hari bekerja mereka (apabila tidak menggunakan SSO). Kaedah ini tidak membantu pengguna log masuk ke sistem pengendalian peranti tetapi boleh mengurus kata laluan setelah pengguna log masuk. Pengguna Google boleh menggunakan Password Manager merentas Chrome pada sebarang platform, ChromeOS dan Android.

Keperluan unik pelbagai kumpulan akan meraih manfaat daripada subset atau gabungan khusus pendekatan pengesahan ini, mengikut peranan mereka dalam institusi pendidikan, jenis sistem dan data yang boleh diakses oleh mereka serta umur mereka.

Pentadbir Sekolah

Pentadbir mengawal sistem dan kebanyakan data bagi sebarang institusi K-12. Perlindungan akaun mereka adalah penting untuk menjamin keselamatan keseluruhan sistem, termasuk infrastruktur, data akaun dan peranti yang diberikan oleh institusi. Oleh hal yang demikian, mereka hendaklah menggunakan piawai emas pengesahan, termasuk menggunakan kata laluan kukuh, pengurus kata laluan yang mantap dan 2SV. Setiap langkah ini menyediakan lapisan perlindungan yang memberikan tahap keselamatan paling kukuh untuk akaun Pentadbir dan perkhidmatan perusahaan apabila digunakan bersama-sama.

- Pentadbir hendaklah menggunakan kunci keselamatan fizikal atau kaedah 2SV yang selamat dari segi kriptografi yang memerlukan peranti dipercayai dan gesaan. Perkara ini boleh termasuk perkhidmatan seperti Google Authenticator atau apl lain yang menghasilkan kod pengesahan satu kali. Chromebook yang dikeluarkan selepas tahun 2019 dengan cip TPM mengandungi butang kuasa yang boleh digunakan untuk pengesahan dua faktor.
- Pentadbir hendaklah menggunakan pengurus kata laluan yang boleh dipercayai dan menyokong 2SV untuk menyimpan kata laluan mereka untuk pelbagai perkhidmatan.

Guru dan kakitangan menggunakan peranti yang ditetapkan

Seperti pentadbir, guru dan kakitangan mempunyai akses kepada data sensitif tetapi mereka tidak mengawal infrastruktur digital dan memiliki kebolehan teknikal yang berbeza-beza.

- Guru dan kakitangan yang menggunakan Chromebook hendaklah diberi pilihan untuk log masuk dengan pengesahan biometrik, apabila dibenarkan di sisi undang-undang, seperti cap jari.
- Pentadbir hendaklah menguatkuasakan penggunaan 2SV dan beralih kepada pengesahan tanpa kata laluan apabila boleh dan apabila kakitangan mengakses sistem institusi pendidikan dari jauh.

Pelajar tahap atas menggunakan peranti yang ditetapkan (lazimnya gred 4 ke atas)

Pelajar sekolah tahap atas lebih berpengetahuan tentang cara melindungi diri mereka dan biasanya berupaya menggunakan mekanisme pengesahan yang lebih terlindung, yang bersesuaian dengan jenis perkhidmatan yang mungkin digunakan oleh mereka. Mereka hendaklah hanya memiliki akses kepada akaun mereka sendiri dan maklumat yang telah dikongsi dengan mereka..

- Pelajar yang menggunakan Chromebook hendaklah diberi pilihan untuk membuat PIN khusus peranti untuk mempercepat log masuk pada peranti tersebut. Pilihan biometrik mungkin tidak sesuai atau boleh dilaksanakan dalam kebanyakan persekitaran sekolah.
- Setiap pelajar hendaklah disokong untuk membuat kata laluan unik yang tidak mengandungi maklumat peribadi (contoh: nama, kelas tingkatan atau tarikh lahir). Pelajar hendaklah diajar tentang cara penggunaan ungkapan laluan boleh memberikan kerumitan dan pada masa yang sama, memastikan kata laluan mudah diingat.

Pelajar tahap rendah menggunakan peranti dikongsi (lazimnya gred K-3)

Pelajar tahap rendah masih lagi belajar tentang cara menggunakan teknologi pendidikan dan akan mendapat manfaat daripada pengesahan yang ringkas iaitu yang sesuai digunakan untuk perkhidmatan dan data yang terhad.

- Sekolah yang menggunakan kaedah kata laluan alternatif daripada pihak ketiga seperti kod QR atau log masuk gambar untuk pelajar tahap rendah dan mereka yang tidak dapat log masuk dengan kata laluan hendaklah melaksanakan langkah berjaga-jaga untuk keselamatan, memandangkan kaedah tersebut kurang selamat. Pentadbir hendaklah mengubah suai kata laluan pelajar dan mengemaskinikan kod apabila kod hilang atau didedahkan kepada orang lain.
- Sekolah hendaklah mendidik pelajar dan juga ibu bapa tentang kepentingan merahsiakan kata laluan dan menyimpan bukti kelayakan alternatif seperti kod QR dengan selamat.
- Untuk peranti yang ditetapkan seperti tablet, PIN khusus peranti boleh digunakan sebagai kaedah pengesahan alternatif yang selamat.

Gunakan Tetapan Keselamatan yang Bersesuaian

Peranti dan rangkaian sekolah merupakan sasaran yang memiliki keterlihatan dan nilai yang tinggi bagi penggodam di seluruh dunia, maka penggunaan langkah keselamatan yang sebaik mungkin adalah sangat penting untuk mencegah kehilangan perkhidmatan, sumber, masa dan wang. Pentadbir sistem hendaklah melaksanakan ciri keselamatan yang berkesan dan bersesuaian yang tersedia dalam produk yang digunakan oleh institusi mereka, tetapi mereka juga perlu memastikan sistem ini masih mudah untuk digunakan oleh guru, kakitangan dan pelajar. Tetapan keselamatan dan privasi yang penting hendaklah dikonfigurasikan supaya pengguna individu tidak boleh melumpuhkan atau mengubah suai tetapan tersebut, dan tetapan lain hendaklah ditetapkan dengan ciri perlindungan lalai oleh pentadbir. Pentadbir perlu menggunakan langkah keselamatan yang sebaik mungkin untuk mencegah kehilangan perkhidmatan, sumber, masa dan wang. Jika anda menggunakan Chromebook, anda boleh melihat syor kami tentang cara menetapkan dasar peranti pada bahagian terakhir.

Akhir sekali, terapkan "peminimuman data" dalam amalan anda dengan mengehadkan tujuan dan cara pengumpulan, penggunaan serta pendedahan maklumat peribadi individu kepada perkara yang benar-benar perlu dan sewajarnya untuk menyediakan perkhidmatan atau menepati konteks hubungan.

Aplikasi & Kemaskinian

Hadkan dan minimumkan apl yang boleh dipasang oleh pengguna anda kerana setiap aplikasi yang dipasang pada peranti berpotensi untuk menjadi vektor serangan yang boleh dieksploitasikan. Jika boleh, gunakan aplikasi daripada sumber yang boleh dipercayai. Sebagai contoh, sarankan pengguna menyemak lencana pengesahan pada Google Play Store untuk memastikan pengguna memuat turun aplikasi rasmi yang telah melalui semakan keselamatan. Sebarang pengubahsuaian OS atau perkakasan (memecah sekat atau mengakses akar) mencetuskan kelemahan keselamatan yang ketara dan hendaklah dielakkan.

Akses & Keterlihatan

Pentadbir hendaklah memastikan bahawa pengguna hanya memiliki akses kepada data, perisian, perkhidmatan dan sistem yang diperlukan oleh mereka untuk melaksanakan tugas atau belajar dengan berkesan. Tindakan ini mengehadkan akses yang tidak disengajakan dan menjejaki pengguna yang mempunyai akses kepada sumber tertentu. Berikan perhatian khas kepada data yang sangat sensitif, seperti PII pengguna dan sistem (seperti HR, senarai gaji, pemarkahan, keselamatan dan konfigurasi) dengan mengaudit pengguna yang boleh mengakses data tersebut dan keadaan yang membolehkan mereka berbuat demikian dengan mengehadkan akses kepada peranti milik sekolah, dan memastikan hanya kakitangan yang khusus memiliki akses.

Semak dasar perkongsian data anda dalam alatan kerjasama untuk mencegah perkongsian yang tidak wajar atau berlebihan dan akses yang tidak dibenarkan. Hadkan atau sekat perkongsian di luar persekitaran anda (terutamanya untuk pelajar) dan laksanakan dasar yang memantau perkongsian kandungan sensitif.

Kehilangan atau Kecurian Peranti

Kehilangan peranti tidak seharusnya menyebabkan anda kehilangan data. Pentadbir hendaklah menstandardkan rancangan untuk memastikan akses kepada maklumat dan dokumen sekiranya berlaku kehilangan atau kecurian peranti, seperti mengekalkan dokumen dalam persekitaran awan. Muat turun dan cetak kod sandaran bagi proses 2SV anda untuk mencegah gangguan akses akaun.

Apabila peranti dilaporkan hilang atau dicuri, pastikan peranti tersebut dikunci dari jauh sekiranya boleh, dan akaun yang berkaitan dikunci atau dibenderakan untuk memastikan akaun tersebut tidak digunakan untuk mendapat akses tanpa kebenaran. Chromebook boleh dipadamkan dari jauh sekiranya hilang dan akaun Google Workspace for Education boleh dipantau untuk mengesan aktiviti yang mencurigakan atau digantung (dikunci) jika perlu.

Perlindungan Lanjutan untuk Pengguna Berisiko Tinggi

Bagi pengguna dengan keterlihatan yang tinggi dan memiliki maklumat sensitif (termasuk pentadbir Google Workspace for Education), Google menyediakan Program Perlindungan Lanjutan (APP). APP memberi pengguna perlindungan tambahan daripada serangan bertumpu seperti percubaan pancingan data, muat turun yang berbahaya dan pelanggaran kata laluan. APP direka bentuk khusus menghalang serangan dalam talian yang menyasarkan Google Account dan menggunakan pengesahan yang kukuh serta kunci keselamatan secara automatik selain mengehadkan akses pihak ketiga kepada data akaun. Penyedia akaun dalam talian yang lain juga menyediakan perlindungan akaun yang kukuh untuk pengguna berisiko tinggi. Pentadbir dan kakitangan hendaklah sentiasa menggunakan perlindungan tersebut jika mereka mempunyai akses kepada maklumat peribadi atau sistem teknologi.

Kemas Kinikan dan Tingkatkan Sistem Anda

Salah satu perkara paling penting yang boleh dilakukan oleh sesiapa sahaja untuk melindungi diri mereka adalah dengan memastikan sistem pengendalian dan aplikasi peranti mereka sentiasa dikemaskinikan. Perkara ini lebih penting bagi institusi K-12 kerana mereka memainkan peranan penting dalam pendidikan dan kehidupan harian kanak-kanak. Kebanyakan serangan perisian hasad dalam konteks pendidikan dan juga konteks risiko tinggi lain adalah berasaskan Windows, termasuk SolarWinds, serangan perisian tebusan Daerah Sekolah Bersatu Los Angeles, penggodaman Daerah Sekolah Little Rock, pelanggaran data Pelayan Microsoft Exchange, serangan perisian tebusan Daerah Sekolah Albuquerque dan pencerobohan agensi persekutuan Microsoft yang berlaku baru-baru ini. Hal ini satu lagi contoh penggunaan produk dan perkhidmatan awan yang memudahkan tugas pentadbir dengan mengurangkan platform serangan dan memastikan sistem serta aplikasi mereka kekal dikemaskinikan secara automatik.

Tingkatkan kepada Sistem Pengendalian Moden dan Pastikan Sistem Terkini

Versi terkini sebarang sistem pengendalian (OS) biasanya mengandungi ciri keselamatan baharu untuk membantu pengguna menghalang vektor serangan yang diketahui. Anda hendaklah mendayakan kefungsian kemaskinian automatik dalam OS peranti atau sekiranya kemaskinian automatik adalah mustahil, muat turun dan pasang tampung serta kemaskinian daripada vendor yang dipercayai sekurang-kurangnya setiap bulan.

Chromebook dijalankan pada ChromeOS, maka peranti tersebut menerima kemaskinian automatik secara kerap dengan tampung keselamatan terkini untuk membolehkan penerimagunaan inovasi keselamatan terkini dengan pantas dan peranti tersebut mengesahkan integriti sistem pengendalian baca sahaja sebelum mengebut. Chromebook juga menyulitkan semua data yang disimpan pada peranti, yang memberikan perlindungan daripada akses tanpa kebenaran dan menjalankan setiap halaman web serta aplikasi dalam kotak pasir yang berasingan supaya jika satu laman web atau apl dijangkiti perisian hasad, serangan tersebut tidak dapat merebak kepada bahagian peranti yang lain.

Sekiranya sekolah anda tidak bersedia untuk beralih kepada Chromebook, ChromeOS Flex ialah versi ChromeOS yang dibuat untuk memodenkan peranti sekolah anda. ChromeOS Flex memberi semua orang pengalaman pengajaran dan pembelajaran moden serta disatukan yang memiliki keupayaan pengurusan keselamatan dan berasaskan awan yang terbina dalam dan proaktif. Flex boleh menyediakan perlindungan automatik dan menyekat boleh laku serta apl hasad tanpa menggantikan perkakasan sedia ada anda.

Tingkatkan kepada Penyemak Imbas Moden dan Pastikan Penyemak Imbas Tersebut Terkini

Anda hendaklah memastikan bahawa penyemak imbas juga dikemaskinikan dan selamat. Penyemak imbas moden menawarkan ciri keselamatan lanjutan dan boleh menggesa pengguna untuk mendayakan ciri tersebut dengan mudah atau dikonfigurasikan oleh pentadbir agar menghidupkan ciri ini secara lalai pada komputer institusi - hal ini membolehkan penyemak imbas tersebut melindungi kerahsiaan maklumat sensitif semasa dalam transit pada Internet. Penyemak imbas ini hendaklah sentiasa dikemaskinikan. Sama ada anda bekerja, belajar atau melakukan aktiviti dalam talian yang lain, penyemak imbas moden yang dikemaskinikan akan:

- **Menggunakan keselamatan yang mantap** termasuk pengasingan laman dan perlindungan penyemakan imbas selamat untuk menghalang pengguna daripada melayari laman web yang berbahaya secara tidak sengaja
- **Mendayakan kemaskinian automatik** untuk memastikan penyemak imbas anda menerima kemaskinian keselamatan dengan pantas
- **Memastikan sambungan adalah selamat.** Penyemak imbas moden hendaklah menggunakan keselamatan lapisan pengangkutan, dan pengguna boleh mengklik bersebelahan URL dan memastikan sambungan ditandai sebagai selamat

Chrome telah dibina dengan mengutamakan keselamatan, dengan ciri keselamatan seperti penyemakan imbas selamat yang dihidupkan secara lalai. Terdapat pengurus kata laluan disepadukan yang boleh melakukan autolengkap kata laluan semasa anda menyemak imbas web, sekali gus membolehkan anda menggunakan kata laluan kukuh dengan mudah.

Gunakan Sistem Pemakluman dan Pemantauan Masa Nyata

Sistem pemakluman dan pemantauan masa nyata boleh membantu sekolah mengenal pasti dan bertindak balas terhadap ancaman dengan pantas sebelum berlaku kerosakan. Anda perlu memastikan alatan keselamatan dijalankan pada latar, di samping mengumpulkan dan membuat log peristiwa keselamatan daripada seluruh sistem anda. Alatan AI khususnya dapat menyemak sejumlah besar data yang dikumpulkan dan mencari anomali serta corak, yang boleh digunakan untuk mengesan ancaman dengan lebih cepat dan mudah, serta memproses dan menangani kerentanan. Perkara ini membolehkan pengutamaan aktiviti yang perlu disemak oleh pentadbir atau kakitangan IT.

Sekolah boleh menggunakan ciri pemakluman dan pemantauan yang terbina dalam perisian kerjasama dan komunikasi utama mereka, seperti Google Workspace for Education atau menggunakan penyelesaian Maklumat dan Peristiwa Keselamatan (SIEM) yang berasingan.

Sistem pemakluman dan pemantauan masa nyata boleh menjejaki pelbagai aktiviti merentas rangkaian, peranti, aplikasi, pengguna dan data sekolah, seperti log masuk pengguna, akses kepada fail, kemungkinan pencerobohan, kecurian data yang berjaya atau percubaan pencurian data dan aktiviti pentadbir.

Sekiranya sistem mengesan sebarang aktiviti yang mencurigakan, sistem itu boleh menghantar makluman kepada kakitangan IT sekolah. Perkara ini membolehkan pentadbir menyiasat masalah itu dan mengambil tindakan untuk mengurangkan ancaman tersebut.

Selain itu, alatan pemakluman dan pemantauan boleh digunakan untuk mendapatkan pemahaman yang lebih mendalam tentang ancaman yang dihadapi oleh sekolah. Dengan menganalisis data daripada sistem masa nyata ini, sekolah boleh mengenal pasti aliran dan corak yang boleh membantu mereka melindungi institusi mereka dengan lebih baik.

Berikut ialah beberapa amalan terbaik dalam menggunakan sistem pemakluman dan pemantauan (termasuk SIEM):

Yang berikut ialah beberapa amalan terbaik tentang penggunaan sistem pemakluman dan pemantauan (termasuk SIEM):

1. **Tetapkan matlamat keselamatan anda**
   Kenal pasti maklumat dan sistem yang paling penting kepada sekolah dan jenis ancaman yang menimbulkan risiko paling besar. Kemudian, kenal pasti data yang perlu anda kumpulkan untuk memantau ancaman tersebut.

2. **Kumpulkan data yang tepat & Konfigurasikan dengan betul**
   Anda perlu mengumpulkan data yang tepat dan mengkonfigurasikan aplikasi untuk menangani matlamat keselamatan anda yang paling berkaitan. Ini mungkin termasuk data daripada tembok api, penapis kandungan, sistem pengesanan pencerobohan, pelayan web dan peranti keselamatan yang lain, berserta dengan perisian komunikasi dan kerjasama, Sistem Maklumat Sekolah dan Sistem Pengurusan Pembelajaran.

3. **Siasat dan berikan respons terhadap makluman**
   Apabila sistem pemantauan anda menjana makluman, anda perlu menyiasat masalah tersebut dan mengambil tindakan yang sewajarnya. Perkara ini mungkin melibatkan usaha menghimpunkan berbilang pasukan untuk menyiasat punca makluman, menentukan sama ada makluman itu positif palsu atau mengambil langkah untuk mengurangkan ancaman tersebut, seperti menggantung akaun, menetapkan semula kata laluan pengguna, mengasingkan atau memadamkan e-mel, mengubah kebenaran fail atau menghapuskan data peranti.

Latih Guru, Kakitangan & Pelajar

Institusi K-12 hendaklah meningkatkan kesedaran dan tabiat keselamatan komuniti sekolah, dengan menggunakan kempen dan perkongsian untuk memperkasakan pengguna mereka. Mendidik guru, kakitangan dan pelajar tentang kepentingan keselamatan adalah penting untuk membantu mereka melindungi diri sendiri dalam talian dan membantu untuk menghalang ancaman keselamatan siber yang serius. Ajar mereka cara menggunakan produk dan perkhidmatan yang ditetapkan merentas institusi, cara mengesan dan melaporkan ancaman seperti e-mel pancingan data dan paling penting, tindakan yang perlu diambil untuk menghalang serangan ini. Sekolah dan daerah hendaklah meningkatkan kesedaran dan tabiat keselamatan komuniti sekolah, menggunakan kempen dan perkongsian untuk memperkasakan pengguna mereka.

Cara menggunakan Peranti dan Perisian dengan Selamat

Pentadbir boleh bekerjasama dengan guru dan pakar untuk membangunkan kurikulum keselamatan siber pada tahap yang bersesuaian dengan umur untuk membantu pelajar memahami cara menggunakan peranti, perisian dan sistem dengan selamat. Penghasilan bahan latihan berjenama sekolah atau daerah membantu untuk mengkontekskan syor untuk guru dan pelajar anda, tetapi anda juga boleh memanfaatkan bahan sedia guna yang tersedia, seperti Be Internet Awesome yang boleh didapati melalui Safety.Google dan Khan Academy, kemudian menyesuaikan bahan tersebut mengikut keperluan anda. Program ini boleh membantu pengguna anda kekal selamat tanpa mengira lokasi mereka - di sekolah atau dalam komuniti mereka.

Mengenal Pasti Ancaman

Melatih guru, kakitangan dan pelajar untuk mengenal pasti ancaman merupakan langkah yang penting untuk memastikan mereka kekal selamat. Mengajar kanak-kanak cara mengenal pasti sama ada sesuatu merupakan ancaman atau tidak adalah penting kerana mereka mungkin tidak tahu cara mengetahui sama ada sesuatu perkara itu sah. Terdapat beberapa jenis ancaman yang patut dikenal pasti oleh mereka dan mereka hendaklah mengetahui cara melaporkan ancaman tersebut. Pentadbir hendaklah memfokuskan topik yang difikirkan akan memberikan pulangan pelaburan yang paling tinggi. Latihan penting bukan hanya untuk mengajar pengguna mengenal pasti ancaman tetapi juga untuk mengambil tindakan. Ancaman lazim yang patut dikenal pasti oleh pengguna termasuk perisian tebusan, pancingan data, kejuruteraan sosial, perisian hasad dan komplot - namun begitu, jika ada ancaman tertentu tersebar dengan lebih luas dalam sesebuah institusi, sebaik-baiknya beri pendidikan kepada komuniti sekolah tentang ancaman tersebut.

Perkongsian Data dan Fail dengan Selamat

Guru dan kakitangan hendaklah dilatih tentang perkongsian fail dan data yang wajar serta cara mengenal pasti permintaan yang tidak wajar melalui e-mel. Perkara yang paling penting ialah mereka hendaklah memastikan maklumat peribadi sensitif hanya dikongsi atau diproses apabila perlu dan dengan lapisan perlindungan tambahan bagi data tersebut, seperti tidak membenarkan data itu dikongsi melalui e-mel atau dengan pihak luar. Mereka hendaklah menggunakan keupayaan pencegahan kehilangan data (disertakan dengan ChromeOS dan Workspace for Education) untuk memberikan amaran dan menghalang pengguna akhir daripada berkongsi fail yang mengandungi data sensitif (seperti nombor keselamatan sosial) atau menyalin dan menampal kandungan sensitif di luar domain.

Pelaksanaan Pendekatan Google: Peranti dan Perkhidmatan untuk Pendidikan

Pemerolehan perisian ialah salah satu alatan paling berkuasa yang boleh melindungi daerah sekolah. Perisian hendaklah memiliki seni bina yang kukuh dan direka bentuk untuk meminimumkan risiko kerentanan, dengan ciri keselamatan terbina dalam setiap lapisan. Dengan mewajibkan sekolah membeli perisian yang selamat, atau perisian daripada syarikat yang mempunyai rekod reputasi keselamatan yang telah terbukti, risiko siber yang lebih meluas boleh dikurangkan dengan ketara. Sebagai contoh, di Google, kami telah mengukuhkan ChromeOS kami dan pada masa yang sama kami terus mengerah tugas lebih banyak penyelesaian proaktif lagi pintar yang memanfaatkan keupayaankepakaran pembelajaran mesin, awan dan identiti.

Google Workspace for Education

Google Workspace for Education ialah set alatan dan perkhidmatan Google yang disesuaikan supaya sekolah dapat bekerjasama, melancarkan pengajaran dan memastikan pembelajaran kekal selamat. Produk dan perkhidmatan Google for Education melindungi pengguna, peranti dan data secara berterusan daripada ancaman rumit yang semakin meningkat, selain menyediakan alatan seperti pusat makluman dan keselamatan, Vault untuk e-Penemuan, pengurusan identiti dan akses serta pencegahan kehilangan data.

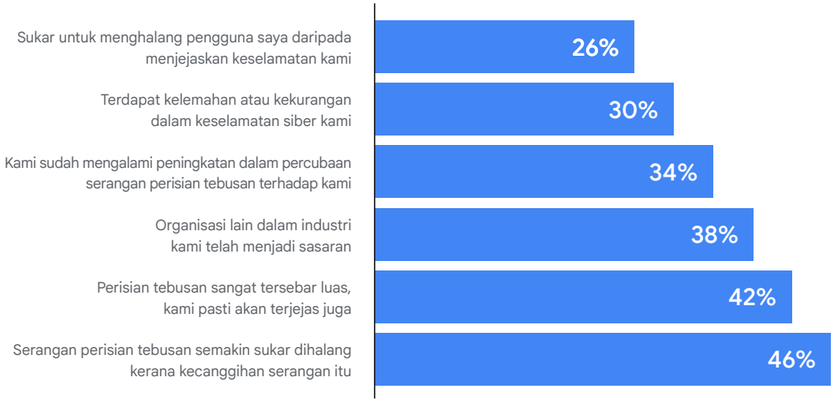
Kami telah menyusun bahan bantuan sekiranya anda baru sahaja mula menggunakan Google Workspace for Education, dan kebanyakan bahan tersebut boleh membantu anda menyediakan alatan mengikut syor dalam panduan ini. Untuk mendapatkan bantuan memulakan penggunaan Google Workspace for Education, lihat panduan persediaan IT Permulaan Pantas ini.

Google komited untuk menghasilkan produk yang membantu usaha melindungi privasi pelajar dan guru serta memberikan keselamatan yang terbaik dalam industri kepada institusi anda. Anda boleh meyakini produk dan perkhidmatan Google for Education akan melindungi pengguna, peranti dan data secara berterusan daripada ancaman rumit yang semakin meningkat. Bahagian ini memberikan panduan kepada pentadbir IT sekolah tentang syor keselamatan apabila menggunakan produk Google for Education.

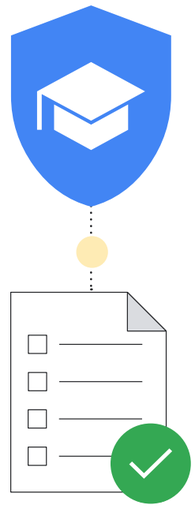
Senarai Semak Keselamatan

Semak senarai semak keselamatan untuk mengetahui lebih lanjut tentang cara memperkukuh keselamatan dan privasi institusi anda. Sekolah yang menggunakan Google Workspace for Education edisi Standard dan Plus boleh juga menggunakan halaman Kesihatan Keselamatan untuk memantau konfigurasi tetapan Konsol pentadbiran anda. Sebagai contoh, anda boleh menyemak status tetapan seperti pengiriman semula e-mel automatik, penyulitan peranti, tetapan perkongsian Drive dan pelbagai lagi. Sekiranya perlu, anda boleh membuat pelarasan pada tetapan domain anda berdasarkan garis panduan dan amalan terbaik keselamatan umum, sambil menyeimbangkan garis panduan ini dengan keperluan perniagaan dan dasar pengurusan risiko organisasi anda.

Sebab sektor pendidikan dijangka akan terjejas



Sumber: https://assets.sophos.com/X24WTUEQ/at/g523b3nmgcfk5r5hc5sns6q/sophos-state-of-ransomware-in-education-2021-wp.pdf



Berikut ialah beberapa petua berguna lagi untuk memastikan anda memaksimumkan perlindungan yang terbina dalam Google Workspace for Education:

Sediakan Unit Organisasi (UO)

Tiada sesiapa akan mengatakan bahawa semua orang dalam akaun Google Workspace for Education anda perlu mempunyai tetapan yang sama. Unit organisasi ialah kumpulan pengguna yang membolehkan anda menentukan perkhidmatan, tetapan dan kebenaran yang berbeza kepada pengguna yang berbeza - sebagai contoh, penggunaan 2SV untuk guru serta kakitangan, dan pengesahan bersesuaian dengan umur untuk pelajar sekolah rendah. Sediakan unit organisasi yang berasingan untuk kakitangan, guru dan pelajar untuk menggunakan dasar pada setiap kumpulan pengguna secara berasingan. Struktur yang direka bentuk dengan baik adalah amat penting untuk mengurus akaun Google Workspace for Education anda secara berkesan dan fleksibel.

Sediakan Dasar Kata Laluan dan Perlindungan Akaun Pentadbir

Seperti yang kita bincangkan, pengesahan pengguna merupakan perkara yang penting untuk memastikan institusi anda kekal selamat. Oleh sebab itu, kami telah menyediakan cara yang fleksibel untuk Pentadbir mengurus pengesahan yang akan membolehkan anda memastikan pengguna memiliki perlindungan akaun yang bersesuaian dan selamat. Tetapkan dasar kata laluan untuk memastikan pengguna membuat kata laluan kukuh dan pertimbangkan untuk mewajibkan penggunaan 2SV jika sesuai, berdasarkan kumpulan yang disyorkan dalam bahagian Log Masuk Selamat. Anda boleh menguatkuasakan penggunaan 2SV untuk subset pengguna (memberi mereka masa untuk menyediakan ciri tersebut) dan melaksanakan 2SV menggunakan pelbagai kaedah, termasuk kunci keselamatan (paling selamat), gesaan Google (menggunakan apl Google pada Android dan iOS), penjana apl pengesahan (seperti Google Authenticator) serta mesej teks atau panggilan telefon (walau bagaimanapun, kaedah ini paling tidak selamat).

Sekiranya organisasi anda menggunakan Pembekal Pengenalan (IdP) selain Google, anda boleh menyediakan Log Masuk Sekali (SSO) melalui Pembekal Pengenalan pihak ketiga. Anda masih boleh menggunakan 2SV dengan SSO bagi akaun bukan pentadbir luar biasa jika mahu.

Hidupkan atau Matikan Perkhidmatan

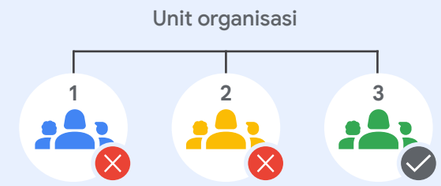
Pentadbir boleh mengawal perkhidmatan Google yang boleh diakses oleh pengguna dengan akaun Google Workspace for Education mereka daripada Konsol Pentadbir Google. Anda boleh mengawal akses kepada perkhidmatan Google seperti Calendar, Drive dan Meet dengan menghidupkan atau mematikan perkhidmatan mengikut unit organisasi (OU) (anda juga boleh menghidupkan perkhidmatan apabila menggunakan kumpulan). Anda juga boleh menyemak perbezaan antara perkhidmatan teras Workspace dengan perkhidmatan tambahan sebelum mendayakan perkhidmatan tambahan seperti YouTube, Google Maps dan Blogger. Pentadbir digalakkan untuk menetapkan akses kepada perkhidmatan Google berdasarkan umur. Sila ambil maklum bahawa pengguna yang ditetapkan sebagai berumur bawah 18 tahun dikenakan sekatan secara automatik pada sesetengah perkhidmatan Google apabila mereka log masuk ke akaun Google Workspace for Education mereka.

Anda juga boleh menggunakan Akses Peka Konteks (tersedia dalam Workspace for Education Standard dan Plus) untuk membenarkan atau menyekat akses kepada apl Google seperti Gmail, Drive dan Calendar berdasarkan alamat IP, asal geografi, dasar keselamatan atau OS peranti. Sebagai contoh, anda boleh membenarkan Drive untuk desktop hanya pada peranti milik syarikat di negara/wilayah tertentu.

Kaedah untuk memberi pengguna akses kepada perkhidmatan

Dalam konsol Pentadbir Google, anda boleh mematikan akses unit organisasi kepada perkhidmatan Google, seperti Google Drive. Jika ada pengguna dalam unit organisasi itu perlu menggunakan Drive, anda mempunyai 2 pilihan:

1. Pindahkan pengguna itu ke unit organisasi yang telah menghidupkan akses kepada Drive.
2. Tambahkan pengguna pada kumpulan akses dan hidupkan akses kepada Drive untuk kumpulan itu. Setiap ahli boleh mengakses perkhidmatan, walaupun akses kepada perkhidmatan tersebut dimatikan bagi unit organisasi mereka.



Akses kepada Google Drive dimatikan bagi unit organisasi 1 dan 2.

Akan tetapi **sekumpulan pengguna** dalam unit organisasi 1 dan 2 boleh menggunakan Google Drive

Sumber: https://support.google.com/a/answer/9050643?sjid=4805599982673626852-NA

Tetapkan Dasar Perkongsian Data Dan Peraturan Pengekalan

Sebagai pentadbir, anda boleh mengawal sama ada pengguna boleh berkongsi fail dan folder Google Drive dengan orang di luar organisasi anda. Tindakan ini boleh membantu untuk mencegah perkongsian data dan fail yang tidak disengajakan atau secara meluas, sekali gus mencegah kebocoran data. Pengasingan fail dan pemacu, pembentukan unit organisasi dan pengendalian mengikut prinsip keistimewaan paling rendah adalah penting untuk menghalang penyerang daripada menular dalam seluruh rangkaian sekiranya mereka sudah menyusup masuk ke satu akaun. Semakin kurang akses bakal penyerang kepada data dan rangkaian, semakin sedikit kerosakan yang boleh dicetuskan.

Matikan perkongsian fail luar bagi pelajar (atau hadkan perkongsian luar kepada domain yang dibenarkan sahaja) dan tetapkan "Penyemak akses" kepada "Penerima sahaja". Sekiranya anda membenarkan sesetengah atau semua pengguna untuk berkongsi fail di luar domain anda, hidupkan amaran apabila pengguna berbuat demikian. Selain itu, lumpuhkan penerbitan fail pada web dan minta kolaborator luar untuk log masuk dengan Google Account.

Selain itu, pelanggan Workspace for Education Standard dan Plus boleh menggunakan Khalayak Sasaran dan Peraturan Kepercayaan untuk menetapkan syor serta pengehadan perkongsian pada tahap yang lebih terperinci. Sebagai contoh, dengan Khalayak Sasaran, anda menetapkan khalayak perkongsian pautan lalai bagi guru kepada "guru dan kakitangan" dan bukannya semua orang di institusi anda. Dengan Peraturan Kepercayaan, anda boleh menyekat pelajar sekolah rendah daripada berkongsi fail dengan pelajar sekolah menengah.

Semak dasar drive kongsi untuk memastikan hanya pengguna yang sewajarnya boleh membuat drive kongsi dan menghalang pengguna luar daripada mengakses drive kongsi. Anda disyorkan agar hanya membenarkan pentadbir (atau kakitangan dan guru) untuk membuat drive kongsi dan mengurus akses drive kongsi dengan teliti.

Pertimbangkan untuk mengehadkan keterlihatan Directori dan perkongsian kenalan jika boleh, sama ada dengan melumpuhkan perkongsian kenalan bagi sesetengah atau semua pengguna, atau dengan membuat direktori tersuai untuk mengehadkan pengguna yang boleh dilihat oleh pengguna tertentu.

Sediakan dasar pencegahan kehilangan data (DLP) dalam Drive dan Gmail untuk mengesan serta menyekat maklumat sensitif. Terdapat dasar prabina yang boleh dimanfaatkan untuk melindungi maklumat sensitif biasa (seperti nombor akaun bank atau kad kredit). Anda juga boleh membuat dasar tersuai berdasarkan kata kunci, senarai perkataan dan ungkapan nalar (Regex).

Urus Tetapan Gmail

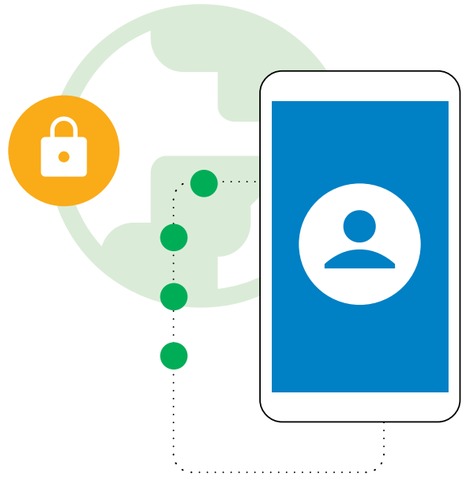
Gmail ialah salah satu perkhidmatan teras dalam Google Workspace for Education, dan terdapat banyak tetapan yang boleh dimanfaatkan oleh pentadbir untuk melindungi institusi serta pengguna mereka. Elakkan spam, penipuan dan pancingan data dengan pengesahan Gmail. Sesuaikan tetapan penapis spam, termasuk menghendaki pengesahan pengirim bagi semua pengirim yang diluluskan dan melumpuhkan pintasan penapis spam bagi pengirim dalaman.

Lumpuhkan akses POP/IMAP jika boleh dan dayakan pengimbasan mesej prapenghantaran dipertingkatkan di samping perlindungan pancingan data dan perisian hasad lanjutan. Sekiranya anda membenarkan e-mel luar bagi sesetengah atau semua pengguna, anda boleh mendayakan amaran penerima luar.

Pelanggan Google Workspace for Education Standard dan Plus juga boleh membantu untuk melindungi daripada perisian hasad dan perisian tebusan dengan menyediakan peraturan untuk mengesan lampiran yang berbahaya menggunakan Kotak Pasir Keselamatan.

Aplikasi Pihak Ketiga

Gunakan aliran kerja kelulusan terbina dalam untuk meluluskan aplikasi pihak ketiga yang mengakses data akaun melalui API. Langkah ini membantu untuk menghalang data yang tidak dibenarkan daripada dikongsi dengan aplikasi pihak ketiga yang tidak diluluskan untuk kegunaan sekolah.



Laporan Dan Pemantauan

Sebagai pentadbir, anda boleh melihat laporan dan log peristiwa dalam konsol Pentadbir Google untuk menyemak aktiviti dalam organisasi anda seperti kemungkinan risiko keselamatan, individu yang log masuk serta waktu mereka log masuk selain memahami cara pengguna membuat dan berkongsi kandungan. Anda boleh melihat data tahap domain di samping butiran tahap pengguna yang lebih terperinci melalui graf dan jadual. Lihat laporan dan log audit (termasuk pusat makluman) untuk mengenal pasti risiko keselamatan, menganalisis penggunaan perkhidmatan, mendiagnosis masalah konfigurasi, menjejaki aktiviti pengguna dan pelbagai lagi.

Pentadbir Google Workspace for Education Standard dan Plus boleh memanfaatkan Papan Pemuka Keselamatan untuk melihat ikhtisar laporan keselamatan yang berbeza, mengenal pasti aliran bahkan membandingkan data semasa dengan data sejarah, seperti perkongsian fail dalam Drive, aktiviti spam, pancingan data serta perisian hasad dalam Gmail, log masuk akaun pengguna yang mencurigakan dan aktiviti peranti yang mencurigakan. Kebanyakan log penggunaan, aktiviti dan audit — termasuk peristiwa log Admin, Drive, Meet dan Chat — serta laporan keselamatan tersedia selama enam bulan.

Manfaatkan Pusat Keselamatan

Pentadbir Google Workspace for Education Plus dan Standard boleh menggunakan pusat keselamatan, yang menyediakan maklumat dan analitis keselamatan lanjutan serta keterlihatan dan kawalan tambahan terhadap masalah keselamatan yang menjejaskan domain anda.

Pusat keselamatan termasuk Alat Penyiasatan Keselamatan, yang boleh membantu pentadbir untuk mengenal pasti, menentukan keutamaan dan mengambil tindakan terhadap isu keselamatan serta privasi seperti serangan pancingan data, perkongsian fail yang tidak wajar, aktiviti pengguna dan peranti yang mencurigakan malah pelbagai isu lagi.

Google Workspace ialah set komunikasi dan kerjasama asli awan yang paling selamat di dunia

0

kerentanan perisian dieksploitasi secara aktif pada Workspace sejak bulan November 2021*

50%

potensi penjimatan bagi premium insurans keselamatan siber melalui penggunaan Google Workspace

2x pengurangan

insiden keselamatan bagi organisasi yang menggunakan Workspace berbanding dengan Microsoft 365

2.5x pengurangan

insiden keselamatan bagi organisasi yang menggunakan Workspace berbanding dengan Microsoft Exchange

*Menurut CISA, jumlah ini adalah ketara lebih rendah berbanding dengan vendor produktiviti yang lain dalam ruang ini.

Google Chromebook untuk Pendidikan

Chromebook merupakan komputer yang amat selamat, boleh diskalakan dan mudah digunakan untuk pelajar dan guru hasil daripada ciri keselamatan Chromebook yang terbina dalam dan sedia digunakan sebaik sahaja dikeluarkan dari kotak. Serangan perisian tebusan terhadap mana-mana peranti ChromeOS perniagaan, sekolah atau pengguna tidak pernah dilaporkan. Chromebook membantu untuk melindungi sekolah daripada ancaman yang sentiasa berubah dengan ciri yang terkini, dan kemaskinian dilakukan secara automatik pada latar, maka pengguna boleh segera kembali melakukan kerja.

Kemaskinian OS dan aplikasi secara automatik, dengan perlindungan perisian hasad yang terbina dalam

Penyerang sentiasa cuba mengambil kesempatan terhadap pepijat dan lohong gelung dalam sistem pengendalian, penyemak imbas serta apl popular untuk memasang perisian hasad dan mencuri data pengguna. Untuk melindungi anda dan pengguna anda, Chromebook mengemaskinikan OS serta aplikasi anda kerana komputer ini dibina agar selamat secara lalai dengan kemaskinian keselamatan - dan aplikasi awan tidak memerlukan kemaskinian perisian seperti apl setempat. Cip keselamatan pada Chromebook yang direka bentuk oleh Google membantu untuk memastikan peranti selamat, melindungi identiti pengguna dan memastikan integriti sistem.

Chromebook dalam kumpulan anda akan menjalankan kemaskinian perlindungan perisian hasad yang terkini secara automatik. Pelajar dan pendidik dilindungi daripada ancaman siber dengan ciri keselamatan yang terbina dalam seperti penyulitan data, but disahkan, kotak pasir serta kemaskinian automatik. .

Data pengguna disimpan dengan selama

Apabila anda log masuk ke Chromebook dengan Google Account anda, semua data anda disimpan dalam fail yang disulitkan, sekali gus memastikan tiada sesiapa yang menggunakan peranti boleh melihat data anda atau log masuk ke aplikasi menggunakan akaun anda. Hal ini membolehkan pelajar berkongsi peranti dalam bilik darjah, maka pihak sekolah dapat mengurangkan jumlah kos perkomputeran dengan mudah dan selamat. Untuk mendapatkan ciri keselamatan lanjutan, Peningkatan Pendidikan Chrome, iaitu satu lesen pengurusan peranti, menawarkan keterlihatan yang dipertingkatkan.

Dasar keselamatan peranti diurus pengguna dari jauh

Pentadbir sekolah boleh mengkonfigurasikan dasar ChromeOS dan memasang/mengemaskinikan aplikasi dari jauh menggunakan konsol Pentadbir Google. Dengan hanya satu klik butang, seorang pentadbir IT boleh mengemaskinikan dasar dan konfigurasi ratusan ribu Chromebook dalam masa yang singkat.

Hal ini memastikan:

- Pelajar hanya boleh mengakses kandungan dan aplikasi yang diluluskan oleh sekolah
- Semua aplikasi dan sambungan dikemaskinikan dengan pembetulan keselamatan terbaharu
- Pengguna tidak boleh menyalin, memindahkan atau berkongsi data sekolah di luar peranti
- Buat keputusan terdorong data dengan syor keselamatan yang disesuaikan daripada Google untuk menangani ancaman keselamatan
- Urus dasar keselamatan dan pengurusan identiti dan akses secara berpusat untuk semua pengguna terus dalam konsol Pentadbiran

Beberapa dasar diserlahkan yang mungkin perlu dikonfigurasikan oleh pentadbir ialah:

Dasar Peranti

- **Mod Tetamu**
  Anda disyorkan melumpuhkan mod Tetamu peranti anda untuk memastikan pelajar dan guru log masuk menggunakan bukti kelayakan mereka sendiri dan bukannya menggunakan peranti secara awanama
- **Sekatan log masuk**
  Anda mungkin tidak mahu pelajar dan guru anda log masuk ke Chromebook sekolah anda menggunakan akaun Gmail peribadi mereka. Kuat kuasakan sekatan log masuk agar terhad kepada domain Workspace anda sahaja bagi peranti yang digunakan secara eksklusif oleh pelajar.
- **Pelaporan pengguna dan peranti**
  Pentadbir mungkin perlu menghidupkan pelaporan pengguna dan peranti agar mereka dapat mengumpulkan metrik tentang kekerapan Chromebook digunakan, pengguna yang menggunakan peranti tersebut dan keadaan perkakasan.
- **Pendaftaran semula paksa**
  Chromebook milik sekolah mestilah kekal berada di sekolah melainkan pentadbir melucutkan peruntukan peranti tersebut. Pentadbir hendaklah mendayakan pendaftaran semula paksa Chromebook supaya Chromebook sentiasa didaftar semula sekiranya data dihapuskan atau cuba dicuri.

Dasar Pengguna

- **Mod Inkognito**
  Pelajar hendaklah dipersiapkan untuk berjaya apabila mereka menggunakan Chromebook sekolah. Perkara ini termasuk mengehadkan mereka kepada penyemak imbas yang telah disahkan supaya penapis kandungan web boleh menghalang mereka daripada mengakses laman web yang tidak sesuai. Pentadbir hendaklah melumpuhkan mod Inkognito supaya pelajar tidak dapat memintas penapis web.
- **Mod proksi**
  Walaupun sesetengah sekolah mungkin menggunakan proksi untuk penapisan web, anda perlu menghalang pengguna anda daripada mengubah sendiri tetapan proksi mereka.
- **Berbilang akses log masuk**
  Sekiranya pengguna dibenarkan untuk log masuk ke akaun kedua semasa menggunakan Chromebook dan akaun Workspace sekolah anda, hal ini mungkin membolehkan pengguna menyusup keluar data/maklumat sensitif pelajar atau sekolah kepada akaun kedua. Pentadbir mungkin perlu menyekat berbilang akses log masuk.
- **Sejarah penyemak imbas**
  Bagi pelajar, sebaik-baiknya lumpuhkan keupayaan mereka untuk mengosongkan sejarah penyemakan imbas. Sekiranya insiden keselamatan Internet berlaku, log sejarah Internet boleh membantu semasa siasatan.

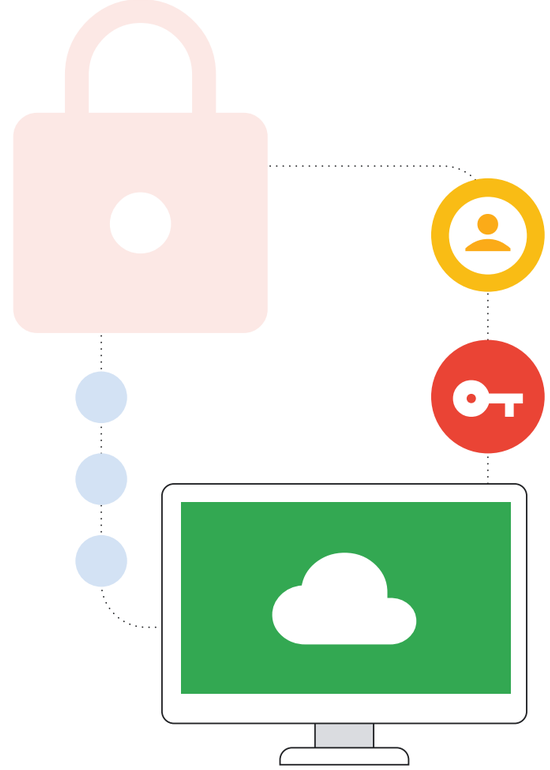
Senarai ini ialah titik mula yang bagus untuk memastikan rangkaian anda selamat daripada jenis kesilapan paling lazim yang menjurus kepada insiden siber yang ketara. Dasar keselamatan tambahan lain yang disyorkan boleh ditemukan dalam Senarai Semak Keselamatan kami.

Pengurusan titik akhir bagi penggunaan yang selamat pada bila-bila masa, di mana-mana sahaja

Sistem pengurusan dasar jarak jauh ChromeOS membolehkan pentadbir sekolah menggunakan tetapan keselamatan dan menjalankan alatan keselamatan seperti sistem penapisan kandungan pada peranti, bukan pada pelayan rangkaian sekolah. Tindakan ini memastikan pelajar dapat menikmati manfaat keselamatan yang sama pada Chromebook sekolah di rumah seperti semasa mereka berada di dalam bilik darjah. Hal ini semakin penting ketika sekolah beralih kepada buku teks digital dan alatan pembelajaran dalam talian. Tambahan pula, pelajar perlu membawa komputer pulang ke rumah agar mereka dapat menyiapkan tugasan.

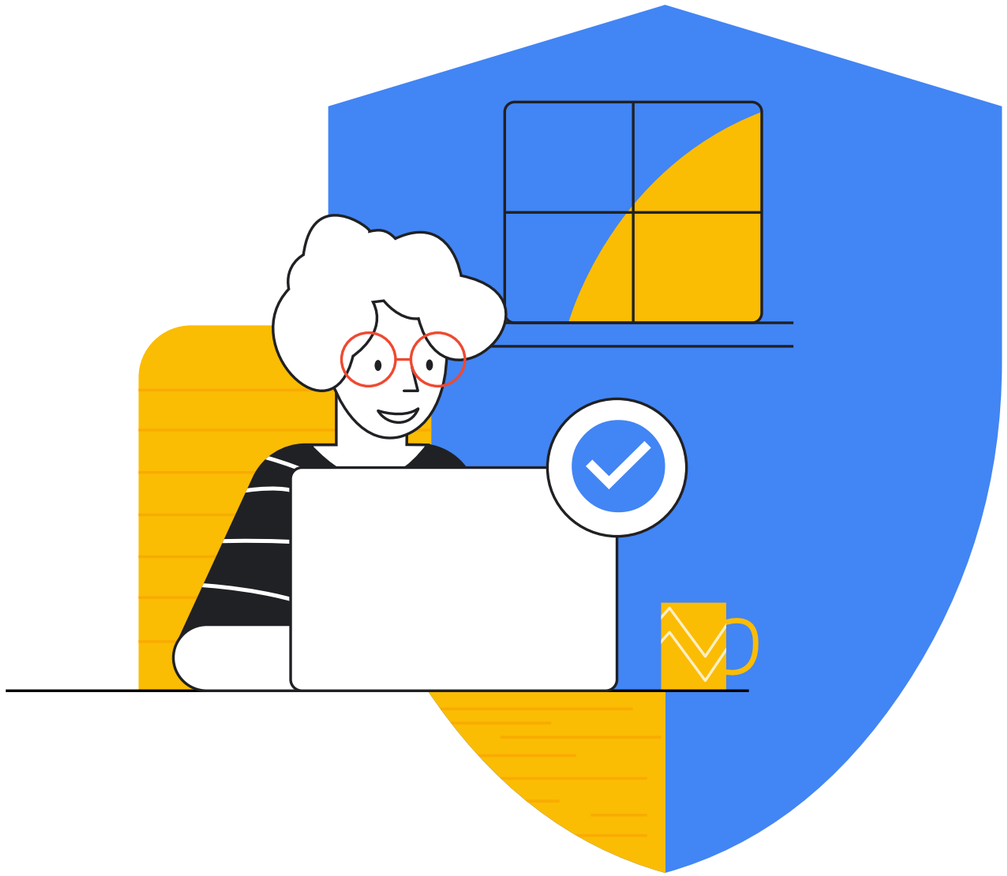
Kesimpulan

Cabaran untuk melindungi institusi K-12 daripada insiden siber ialah usaha yang rumit tetapi pelaburan tersebut amat berbaloi untuk melindungi diri anda, pelajar, guru, kakitangan dan ekosistem dalam talian yang lebih luas. Item yang dibincangkan dalam dokumen ini ialah permulaan yang baik, namun begitu sekolah perlu menyesuaikan syor tersebut dengan keperluan unik mereka dan terus mengikuti perkembangan landskap ancaman yang sentiasa berubah serta teknologi baharu. Sumber ini merupakan asas yang mantap bagi sebarang program keselamatan K-12 dan menyediakan sumber untuk langkah seterusnya yang boleh diambil serta item tindakan yang boleh dilaksanakan. Google juga menyediakan pelbagai sumber, latihan dan pakar keselamatan siber yang terlatih untuk membantu sekolah serta organisasi mengikut buku panduan ini dan menggunakan teknologi seperti AI. Disesuaikan untuk Pendidikan, produk Google menyediakan penyelesaian sedia guna bagi pelbagai kesulitan keselamatan siber yang digariskan dalam dokumen ini. Kami teruja untuk bekerjasama dengan anda dalam mereka bentuk dan melaksanakan program keselamatan anda.



Senarai Sumber

- Google. “Tips to Stay Safe & Secure Online”. Pusat Keselamatan Google, https://safety.google/security/security-tips/. Diakses pada 6 Oktober 2022.
- NIST. “Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1”. = NIST Technical Series Publications, 16 April 2018, https://doi.org/10.6028/NIST.CSWP.04162018. Diakses pada 6 Oktober 2022.
- Microsoft. “Program Microsoft AccountGuard”. Program Microsoft AccountGuard, https://www.microsoftaccountguard.com/en-us/. Diakses pada 6 Oktober 2022.
- Google. “Program Perlindungan Lanjutan”. Program Perlindungan Lanjutan Google, https://landing.google.com/advancedprotection. Diakses pada 6 Oktober 2022.
- Google. “Pusat Keselamatan Google”. Pusat Keselamatan Google - Sentiasa Lebih Selamat Dalam Talian, https://safety.google. Diakses pada 6 Oktober 2022.
- Meta. “Basics: Help Secure Your Account”. Help Secure Your Account, https://www.facebook.com/gpa/resources/basics/security. Diakses pada 6 Oktober 2022.
- Meta. “Facebook Protect”. Facebook, https://www.facebook.com/gpa/facebook-protect. Diakses pada 6 Oktober 2022.
- NIST. “SP 800-124 Rev. 1: Guidelines for Managing the Security of Mobile Devices in the Enterprise”. NIST Technical Series Publications, https://doi.org/10.6028/NIST.SP.800-124r1. Diakses pada 6 Oktober 2022.
- Kunci laluan: https://developers.google.com/identity/passkeys
- CISA Protecting Our Future Cybersecurity K-12 Report https://www.cisa.gov/protecting-our-future-cybersecurity-k-12
- Laporan GAO https://www.gao.gov/products/gao-20-644
- Untuk mendapatkan maklumat lanjut tentang cara Google for Education boleh membantu anda melindungi institusi anda, lihat Pusat Privasi dan Keselamatan Google for Education.
- Laporan Pancingan Data Zcaler



Google for Education