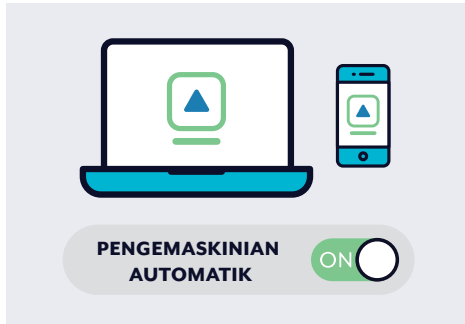


# PETUA UTAMA BAGI KESELAMATAN SIBER

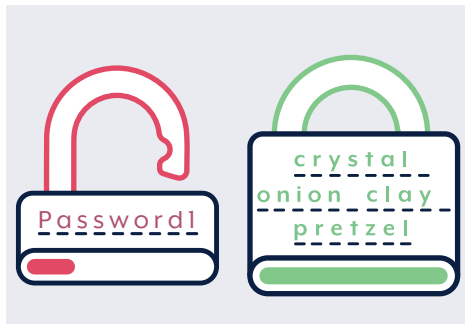
## CARA-CARA PRAKTIKAL UNTUK MELINDUNGI DIRI ANDA DALAM TALIAN

[cyber.gov.au/learn](http://cyber.gov.au/learn)



### Kemaskinikan app dan alat peranti anda

Pengemaskinian app dan alat peranti anda boleh memperbaiki sebarang isu dan menangani kebimbangan atau kelemahan keselamatan yang baharu. Ia juga boleh memasukkan ciri-ciri tambahan baharu kepadanya.



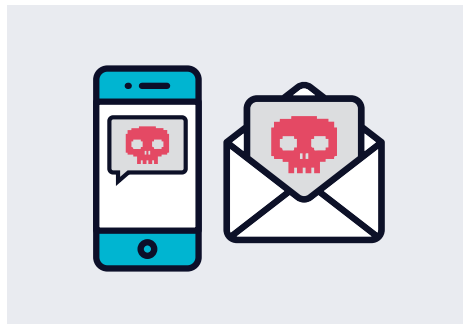
### Pasangkan frasa laluan yang kukuh

Bila MFA tidak disediakan, gunakan sebuah frasa laluan untuk meneguhkan akaun anda. Frasa laluan ialah sejenis kata laluan kuat yang menggunakan empat perkataan rawak atau lebih. Ini akan menyukarkan penjenayah siber untuk menekanya tetapi mudah bagi anda untuk mengingatnya.



### Aktifkan pengesahan pelbagai-faktor (Multi-factor authentication) (MFA)

MFA bermakna anda mempunyai lebih daripada satu kaedah pemeriksaan yang ditetapkan untuk membuktikan identiti anda pada sesebuah akaun. Contohnya, anda mungkin memerlukan sebuah kod yang dihantar melalui khidmat pesanan ringkas beserta frasa laluan anda. Ini menjadikannya lebih sukar bagi penjenayah siber untuk mengakses akaun-akaun anda.



### Kenali dan laporkan penipuan dalam talian (scam)

Penjenayah sering menggunakan e-mel, SMS, panggilan telefon dan media sosial untuk menipu orang dalam talian. Mereka biasanya berbuat demikian dengan menghubungi anda dan menyamar sebagai seorang individu atau organisasi yang anda kenali dan percaya.

Senantiasa berwaspada bila mengklikkan lampiran atau pautan dalam e-mel atau mesej.



### Pasangkan dan kerap lakukan salinan sandaran

Sebuah salinan sandaran ialah salinan digital maklumat anda yang paling penting sama ada ke dalam sebuah alat peranti simpanan luar atau ke sebuah server dalam internet seperti awan. Ia bererti anda boleh mendapatkan fail-fail anda kembali sekiranya sesuatu masalah terjadi.



### Tingkatkan keselamatan siber anda dengan ..

- Memikirkan tentang apa yang anda hantarkan dalam talian.
- Melayani perkhidmatan amaran percuma kami untuk menerima amaran tentang ancaman baharu.
- Bercakap tentang keselamatan siber dengan keluarga dan sahabat handai anda.
- Mengelakkan Wi-Fi awam bila anda membuat perbankan atau pembelian dalam talian.
- Melaporkan serangan atau insiden siber untuk menjaga keselamatan Australia.

Dapatkan maklumat lanjut di [cyber.gov.au/learn](http://cyber.gov.au/learn)

### Laporkan insiden keselamatan siber:

[Cyber.gov.au](http://Cyber.gov.au) | 1300 CYBER1 (1300 292 371)

Nombor ini tersedia untuk digunakan di dalam Australia sahaja.