CYBERSECURITY AWARENESS MONTH

LIHAT DIRI ANDA DI SIBER (SEE YOURSELF IN CYBER)

Setiap oran g memainkan peranan dalam keselamatan siber...tidak kira peranan anda.

Lakukan bahagian anda untuk memastikan keselamatan siber anda dan Syarikat kami selamat dengan mengikuti empat tindakan utama.

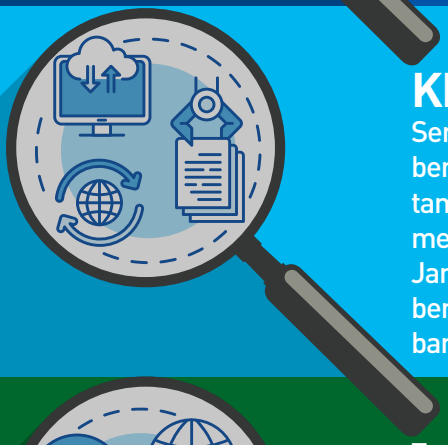
DAYAKAN PENGESAHAN BERBILANG FAKTOR

Juga dikenali sebagai pengesahan dua faktor dan pengesahan dua langkah, pengesahan berbilang faktor, Adalah langkah keselamatan yang memerlukan sesiapa sahaja melog masuk ke akaun untuk navigasi proses dua langkah bagi membuktikan identiti mereka. Ia menjadikannya dua kali lebih sukar untuk penjenayah mengakses akaun dalam talian. Dengan menambah satu lagi langkah mudah apabila log masuk ke akaun, pengesahan berbilang faktor meningkatkan keselamatan akaun anda dengan ketara.

GUNA KATA LALUAN YANG KUKUH

Kata laluan adalah penting jika anda ingin menyimpan maklumat dengan selamat. Berikut ialah beberapa cara mudah untuk melindungi akaun anda melalui amalan kata laluan yang lebih baik. Tidak kira akaun, semua kata laluan harus dibuat dengan mengambil kira tiga perkataan ini.

- Panjang – Sekurang-kurangnya 12 aksara
- Unik – Setiap akaun memerlukan kata laluan uniknya sendiri
- Kompleks – Gunakan gabungan huruf besar dan kecil, nombor dan aksara khas. Sesetengah tapak web akan membenarkan anda memasukkan ruang.



KEMAS KINI PERISIAN

Sentiasa pastikan perisian anda dikemas kini apabila kemas kini tersedia dan jangan berlengah. Kemas kini ini membetulkan masalah perisian am dan menyediakan tampung keselamatan baharu yang mungkin dimasuki oleh penjenayah. Apabila memuat turun kemas kini perisian, dapatkan hanya daripada syarikat yang menciptanya. Jangan sekali-kali menggunakan versi perisian yang digodam, cetak rompak atau tidak berlesen kerana ini selalunya mengandungi perisian hasad dan menyebabkan lebih banyak masalah daripada diselesaikan.

MENGENALI DAN MELAPORKAN PANCING DATA

Tanda-tanda yang boleh menjadi halus, tetapi sebaik sahaja anda tahu percubaan pancingan data, anda boleh mengelak daripada terjatuh. Berikut ialah beberapa petua yang cepat mengenai cara mengesan e-mel pancingan data palsu dengan jelas: Mengandungi tawaran yang terlalu bagus untuk menjadi kenyataan; Bahasa yang mendesak, membimbangkan atau mengancam; Tulisan yang direka dengan buruk dengan ejaan yang salah dan tatabahasa yang buruk; Salam yang samar-samar atau sangat generik; Permintaan untuk menghantar maklumat peribadi; Terdesak untuk klik pada hiperpautan atau lampiran yang tidak dikenali; Permintaan perniagaan yang pelik atau kasar; Menghantar alamat e-mel yang tidak sepadan dengan syarikat asalnya.

MAUSER
Packaging Solutions