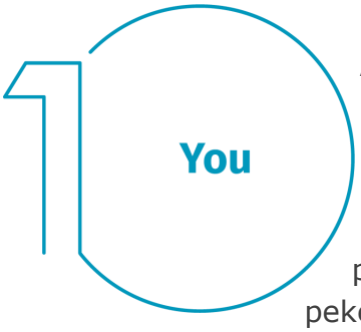
SANS SECURITY AWARENESS

5 Langkah Terbaik Bekerja Aman dari Rumah

Kami tahu bahwa bekerja dari rumah bisa jadi hal baru bagi Anda dan mungkin agak sulit saat menyesuaikan diri dengan lingkungan baru Anda. Salah satu tujuan kami adalah untuk membuat Anda bisa bekerja seaman mungkin dari rumah. Berikut lima langkah mudah untuk bekerja dengan aman. Bagian terbaiknya adalah semua langkah ini tidak hanya membantu mengamankan pekerjaan, tetapi juga membantu Anda dan keluarga lebih aman saat Anda menciptakan rumah aman dunia maya.



Anda: Yang pertama dan paling penting, teknologi saja tidak cukup untuk sepenuhnya melindungi Anda. Andalah pertahanan terbaik. Penyerang telah mempelajari bahwa cara termudah untuk mendapatkan yang mereka mau adalah mengincar Anda, bukan komputer Anda atau perangkat lainnya. Jika mereka ingin kata sandi, data pekerjaan, atau kendali komputer Anda, mereka akan berusaha mengelabui Anda untuk memberikannya pada mereka, sering kali dengan menciptakan kesan mendesak. Misalnya, mereka dapat menelepon dan berpura-pura sebagai dukungan teknis Microsoft dan mengatakan bahwa komputer Anda terinfeksi. Atau mungkin mereka mengirim email peringatan bahwa ada paket yang tidak bisa dikirim, mengelabui Anda untuk mengeklik tautan berbahaya. Indikator paling umum dalam serangan rekayasa sosial mencakup:

- Seseorang yang membuat kesan sangat mendesak, sering kali dengan rasa takut, intimidasi, krisis, atau tenggat penting. Penyerang siber pintar membuat pesan meyakinkan yang seolah-olah datang dari organisasi tepercaya, seperti bank, pemerintah, atau organisasi internasional.
- Tekanan untuk memintas atau mengabaikan kebijakan atau prosedur keamanan, atau tawaran yang tidak masuk akal (maaf, Anda tidak menang lotre!)
- Pesan dari teman atau rekan kerja yang tanda tangan, nada suara, atau pilihan katanya berbeda dari biasanya.

Pada akhirnya, pertahanan terbaik melawan serangan ini adalah Anda.

JaringanRumah: Hampir semua jaringan rumah dimulai dari jaringan nirkabel (sering disebut Wi-Fi). Inilah yang membuat semua perangkat Anda bisa terhubung ke Internet. Sebagian besar jaringan nirkabel rumah dikendalikan oleh router Internet atau jalur akses nirkabel khusus. Cara kerja keduanya sama: dengan memancarkan sinyal nirkabel yang terhubung ke perangkat rumah. Ini artinya, mengamankan jaringan nirkabel merupakan bagian penting dalam melindungi rumah Anda. Kami menyarankan langkah berikut untuk mengamankannya:

- Ubah kata sandi administrator default dari perangkat yang mengendalikan jaringan nirkabel Anda. Akun administrator adalah yang Anda gunakan untuk mengubah pengaturan untuk jaringan nirkabel Anda.
- Pastikan hanya orang terpercaya yang dapat terhubung ke jaringan nirkabel Anda. Lakukan ini dengan mengaktifkan keamanan yang kuat. Dengan mengaktifkannya, diperlukan kata sandi agar orang bisa terhubung ke jaringan nirkabel Anda, dan setelah terhubung, aktivitas online mereka dienskripsi.
- Pastikan kata sandi yang digunakan untuk terhubung ke jaringan nirkabel Anda merupakan kata sandi yang kuat dan berbeda dari kata sandi administrator. Ingat, Anda hanya perlu memasukkan kata sandi sekali untuk tiap perangkat, karena perangkat menyimpan dan mengingat kata sandinya.

Kurang yakin tentang cara melakukan langkah-langkah ini? Bertanyalah pada Penyedia Layanan Internet Anda, buka situs web mereka, periksa dokumen jalur akses nirkabel Anda, atau buka situs web vendor.

Kata Sandi: Saat situs meminta Anda membuat kata sandi: buatlah sandi yang kuat, semakin banyak karakternya, semakin kuat. Frasa sandi adalah cara termudah memastikan Anda memiliki kata sandi yang kuat. Frasa sandi tidak lebih dari sekadar kata sandi yang dibuat dari beberapa kata, seperti "*bee honey bourbon.*" Menggunakan frasa sandi unik berarti menggunakan frasa sandi berbeda untuk tiap perangkat atau akun online. Dengan begitu, jika satu frasa sandi dibobol, semua akun dan perangkat Anda lainnya masih aman. Tidak bisa mengingat semua frasa sandi?

Gunkan pengelola sandi, program khusus yang secara aman menyimpan semua frasa sandi Anda dalam format terenskripsi (dan memiliki banyak fitur bagus lainnya juga!) Yang terakhir, mengaktifkan verifikasi dua tahap (yang juga disebut autentikasi dua faktor atau multi faktor) bila memungkinkan. Verifikasi ini menggunakan kata sandi Anda, tetapi juga menambahkan langkah kedua, seperti kode yang dikirim ke ponsel pintar Anda atau aplikasi yang membuat kodenya untuk Anda. Verifikasi dua langkah mungkin adalah langkah paling penting yang dapat diambil untuk melindungi akun online Anda, dan lebih mudah dari yang Anda kira.

Pembaruan: Pastikan tiap komputer, perangkat seluler, program, dan aplikasi Anda menggunakan versi perangkat lunaknya yang terbaru. Penyerang siber senantiasa mencari kerentanan baru dalam perangkat lunak yang perangkat Anda gunakan. Ketika mereka menemukan kerentanan, mereka menggunakan program khusus untuk memanfaatkannya dan meretas perangkat yang sedang Anda gunakan. Sementara itu, perusahaan yang menciptakan perangkat lunak untuk perangkat ini bekerja keras untuk memperbaikinya dengan mengeluarkan update. Dengan memastikan komputer dan perangkat seluler Anda memasang update ini segera, Anda mempersulit orang untuk meretas Anda. Untuk tetap update, cukup aktifkan pembaruan otomatis jika memungkinkan. Aturan ini berlaku untuk seluruh teknologi yang terhubung ke jaringan, termasuk tidak hanya perangkat kerja, tetapi juga TV, monitor bayi, kamera keamanan, router rumah, konsol game, atau bahkan mobil Anda.

Anak-anak/Tamu: Hal yang paling tidak perlu Anda khawatirkan di kantor adalah anak-anak, tamu, atau anggota keluarga lain yang mungkin menggunakan laptop kerja atau perangkat kerja Anda lainnya. Pastikan keluarga dan teman memahami bahwa mereka tidak dapat menggunakan perangkat kerja Anda, karena mereka dapat secara tidak sengaja menghapus atau mengubah informasi, atau bahkan lebih buruk, tidak sengaja menginfeksi perangkat tersebut.