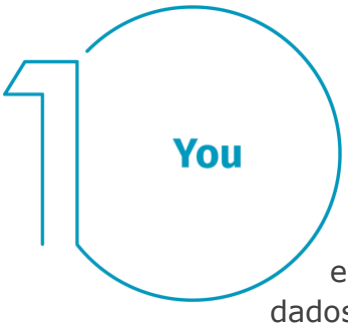
Os 5 principais passos para trabalhar em casa em segurança

Sabemos que trabalhar a partir de casa pode ser novidade para alguns de vocês e levantar problemas conforme se vão adaptando ao novo ambiente de trabalho. Um dos nossos objetivos é permitir-vos trabalhar a partir de casa da forma mais segura possível. Em baixo podem encontrar cinco passos para trabalhar de forma segura. A melhor parte é que estes passos, para além de ajudarem-vos a protegerem o vosso trabalho, também contribuirão para melhorarem a cibersegurança dos vossos lares para vocês e para as vossas famílias.



Vocês: antes de mais, a tecnologia não chega para nos proteger de forma completa – você são a vossa melhor defesa. Os atacantes descobriram que a forma mais fácil de obterem aquilo que desejam é atacar-vos diretamente ao invés dos vossos computadores ou outros dispositivos. Se eles pretenderem obter a vossa palavra-passe, os vossos dados do trabalho ou controlo sobre o vosso computador, tentarão enganar-vos para que lhes concedam acesso, muitas vezes criando um sentido de urgência. Por exemplo, podem ligar-vos a fazerem-se passar pelo apoio técnico da Microsoft, afirmando que o vosso computador está infetado. Ou talvez lhes enviem um e-mail a alertar-vos que não foi possível entregar uma encomenda, levando-vos a clicarem numa ligação maliciosa. Os indicadores mais comuns de um ataque de engenharia social incluem:

- Alguém que cria uma enorme sensação de urgência, muitas vezes através do medo, intimidação, uma crise ou um prazo importante. Os ciberatacantes são peritos na criação de mensagens convincentes que parecem oriundas de organizações de confiança como bancos, governos ou organizações internacionais.
- Pressão para contornar ou ignorar as políticas ou procedimentos de segurança, ou uma oferta demasiado boa para ser verdade (não, você não venceram a lotaria!).

- Uma mensagem de um amigo ou colega, mas onde a assinatura, o tom de voz ou o fraseamento parecem errados.

Em último caso, você são sempre a melhor defesa contra estes ataques.

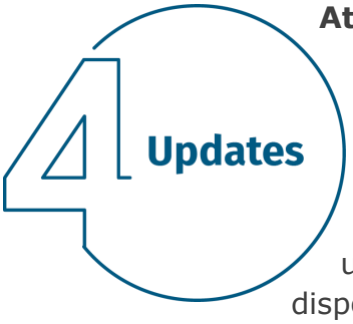
Rede doméstica: praticamente todas as redes domésticas começam com uma rede sem fios (ou Wi-Fi). É esta rede que vos permite ligarem os vossos dispositivos à Internet. A maior parte das redes domésticas sem fios são controladas por um router ou por um ponto de acesso sem fios dedicado. Ambos funcionam da mesma forma: através da transmissão de sinais sem fios que estabelecem ligações com os dispositivos domésticos. Isto significa que garantir a segurança das vossas redes sem fios é essencial para protegerem as vossas casas. Recomendamos os seguintes passos para garantirem a segurança das vossas redes:

- Alterem a palavra-passe original de administrador do dispositivo que controla a rede sem fios. A conta de administrador permite-vos configurarem as definições das vossas redes sem fios.
- Assegurem-se de que apenas pessoas da vossa confiança têm acesso às vossas redes sem fios. Para o fazer, recorram a uma segurança forte. Para este fim, será necessário utilizar uma palavra-passe para aceder às vossas redes sem fios e, uma vez estabelecida a conexão, as vossas atividades online são encriptadas.
- Certifiquem-se de que a palavra-passe que as pessoas usam para se ligarem às vossas redes sem fios é forte e que é diferente da palavra-passe de administrador. Lembrem-se que apenas precisam de inserir a palavra-passe uma vez em cada um dos vossos dispositivos, já que estes armazenam e recordam a palavra-passe.

Não têm a certeza de como levar a cabo estes passos? Perguntem ao vosso prestador de serviços de Internet, visitem o seu website, consultem a documentação incluída com o vosso ponto de acesso sem fios ou acedam ao website do fornecedor do equipamento.

Palavras-passe: quando um site vos pedir para criarem uma palavra-passe, criem uma palavra-passe forte. Quantos mais caracteres esta tiver, mais forte será. Usar uma frase-passe é uma das formas mais simples de vos assegurarem de que têm uma palavra-passe forte. Uma frase-passe não é nada mais do que uma palavra-passe composta por múltiplas palavras, tal como "*abelha mel licor.*" Usar uma frase-passe única significa usar uma diferente para cada dispositivo ou conta online. Assim, se uma frase-passe for comprometida, todas as outras contas e dispositivos continuarão em segurança. Não se recordam de todas as vossas frases-passe?

Usem um gestor de palavras-passe, um programa especializado que armazena em segurança todas as vossas frases-passe num formato encriptado (e que tem muitas outras funcionalidades úteis!). Por fim, ativem a verificação em dois passos (também chamada de autenticação de dois fatores ou multifator) sempre que possível. Utiliza a vossa palavra-passe, mas adiciona-lhe um segundo passo, como um código que vos é enviado para o vosso smartphone ou uma aplicação que gera o código. A verificação em dois passos é provavelmente o passo mais importante que podem tomar para protegerem as vossas contas online e é muito mais fácil do que possam pensar.



Atualizações: certifiquem-se de que os vossos computadores, dispositivos móveis, programas e aplicações estão a executar a versão mais recente do seu software. Os ciberatacantes procuram constantemente novas vulnerabilidades no software utilizado pelos vossos dispositivos. Quando descobrem estas vulnerabilidades, utilizam programas especiais para explorá-las e invadir os dispositivos que estão a utilizar. Entretanto, as empresas que criaram o software para estes dispositivos trabalham arduamente para corrigir as vulnerabilidades através de atualizações. Ao assegurarem-se de que os vossos computadores e dispositivos móveis instalam estas atualizações assim que possível, estão a dificultar bastante a tarefa de quem desejar invadi-los. Para se manterem atualizados, basta ativarem as atualizações automáticas sempre que possível. Esta regra aplica-se a praticamente todos os dispositivos ligados a uma rede, incluindo não só os dispositivos de trabalho, mas também TV, intercomunicadores de bebé, câmaras de segurança, routers domésticos, consolas de videojogos e até mesmo carros.

Crianças/convidados: algo com que muito provavelmente não necessitarão de se preocupar no escritório são crianças, convidados ou outros membros da família a usarem os vossos computadores profissionais ou outros dispositivos de trabalho. Certifiquem-se de que os vossos familiares e amigos compreendem que não podem usar os vossos dispositivos de trabalho, já que podem apagar ou modificar acidentalmente informações ou infetar acidentalmente o dispositivo.