

# As melhores dicas para permanecer seguro e produtivo enquanto trabalha em casa



## Estabeleça uma rotina

- Esteja preparado para trabalhar – tomar banho e vestir-se irá ajudá-lo a preparar-se para começar a trabalhar.
- Crie um espaço de escritório - para se sentar à mesa ou secretária numa cadeira normal.
- Mantenha o dia normal de trabalho onde for possível - se o trabalho normalmente começar entre as 8-10 da manhã e o almoço for algures entre as 12-14H, mantenha este horário.
- Começar o dia com um check-in de equipa - demora apenas 15 minutos a comunicar a sua agenda e a conversar com os colegas - a interação com a equipa é essencial.

## Cuidado com as redes Wi-Fi públicas

O Wi-Fi público é muito inseguro; está a partilhar uma rede aberta com estranhos, pelo que deve tratar cada ligação Wi-Fi pública como comprometida ou insegura.

- Se utilizar Wi-Fi público, evite a ligação a quaisquer websites que requeiram dados pessoais ou sensíveis, incluindo aplicações que possa utilizar para o trabalho. Se precisar de aceder a qualquer um destes sites sensíveis enquanto estiver fora, utilize o seu dispositivo móvel.
- Sempre que possível, utilize uma rede privada virtual de confiança, ou VPN. Isto aumentará grandemente a sua privacidade e segurança enquanto estiver numa rede Wi-Fi partilhada. Uma VPN encripta os seus dados para que mesmo que alguém os intercete numa rede pública não consiga ver a informação.

## Assistente digital

Pode ter um amigo digital em casa, um Amazon Alexa, Google Home, Apple Siri ou Microsoft Cortana. Este amigo digital alguma vez interrompeu a sua conversa ou falou ao acaso apesar de não lhe ter sido pedido? É provável que a resposta seja sim.

Uma vez que um assistente digital está constantemente a ouvir, está extremamente atento, e não é um funcionário da empresa vinculado por qualquer acordo de confidencialidade, deve ser aplicada a precaução adicional para além do que se pratica no escritório.

- Ao efetuar uma chamada confidencial enquanto trabalha a partir de casa, desligue o microfone e a câmara do assistente digital para evitar a partilha de material potencialmente sensível.
- Se achar difícil adotar uma abordagem 'conforme necessário' para desligar o assistente, recomendamos que dê ao seu assistente digital o dia de folga enquanto trabalha e que o desative no início do dia.

O risco não advém apenas da partilha excessiva com o fabricante do assistente digital, existe também o risco de alguém poder ter acesso à sua conta, ou pior, infligir uma quebra de dados ao fabricante e ter acesso a todas as interações anteriores registadas.

## Aplicações de videoconferência/ comunicação

Os mais recentes eventos levaram enormes faixas da população ativa a tornarem-se trabalhadores à distância e um aumento da procura de videoconferências, ferramentas de colaboração em linha e sistemas de chat. Esta mudança inesperada para o trabalho à distância foi notavelmente rápida, mas também limitou o tempo para testar sistemas e educar os utilizadores sobre como utilizar estas ferramentas com segurança.

### Algumas dicas para melhor proteger os seus dados e privacidade enquanto utiliza software de videoconferência:

- Verifique o seu ambiente para assegurar-se de que o fluxo de vídeo que está a partilhar não contém informação sensível.
- Permita apenas participantes específicos, acrescentando os seus endereços de correio eletrónico ao convite quando agendar a chamada.
- Defina uma palavra-passe para a reunião, normalmente uma opção ao criar a reunião, que acrescenta uma palavra-passe gerada aleatoriamente que os convidados terão de introduzir. Uma palavra-passe numérica pode ser utilizada para autenticar os utilizadores que se ligam por telefone.
- Não insira a palavra-passe na ligação da reunião.
- Mantenha os participantes numa "sala de espera" e aprove cada ligação.
- Force o tráfego encriptado. Não tome como certo que os sistemas têm esta opção ativada por defeito para comunicações vídeo.
- Limite a capacidade de partilha de ecrã ao anfitrião, ou a uma pessoa que o anfitrião seleccione.
- Tire tempo para percorrer todas as opções nas definições do sistema de videoconferência - podem existir características adicionais para garantir ainda mais a sua reunião.
- Por último, verifique a política de privacidade do serviço que está a utilizar. Se é gratuito, deve ser motivação suficiente para verificar se a empresa está a recolher, vender ou partilhar os seus dados para financiar a prestação do seu serviço "gratuito".

## A IoT e a rede WiFi de sua casa

Tudo e todos parecemos estar ligados à Internet nos dias de hoje, desde fechaduras de portas, controladores de voz domésticos inteligentes, campainhas de porta, interruptores de luz e muito mais. Estes dispositivos podem abrir vulnerabilidades na segurança da sua rede doméstica e potencialmente colocar o seu empregador em risco quando trabalha a partir de casa. Se os dispositivos forem deixados com senhas padrão e software desatualizado, oferecem aos cibercriminosos e hackers a oportunidade de os explorar.

O mesmo se aplica ao seu router doméstico. Este deve ser mantido atualizado e protegido com uma palavra-passe forte como centro da sua rede e a primeira linha de defesa para proteger os dispositivos IoT. Não atribua à rede informações identificáveis, o seu vizinho não precisa de saber de quem é a rede, nomeando-a, por exemplo, "Casa do Ricardo". Use um nome obscuro e considere tornar o nome privado para que apenas alguém que conheça o nome e a palavra-passe possa aceder ao mesmo.

- Altere os nomes de utilizador e palavras-passe por defeito em todos os dispositivos, incluindo os seus routers.
- Se não utilizar funcionalidades da web, desative-as em todos os dispositivos da Internet.
- Certifique-se de que todos os seus dispositivos da Internet de coisas, incluindo os routers, são mantidos atualizados com os mais recentes firmware ou patches que são fornecidos.
- Certifique-se de que todos os dispositivos IoT que utiliza estão a encriptar os dados enviados através da rede

## Passwords

Se o seu empregador tiver ativado a sua conta para permitir o trabalho em casa, então precisa de se certificar de que faz a sua parte e criar palavras-passe fortes mas memoráveis, ou frases-passe. Um método é inventar uma frase, que pode até ser uma letra de canção, uma citação de filme ou um evento desportivo e pegar em letras de cada palavra como aqui mostrado. Inserindo números e símbolos e aí tem uma senha mestra forte mas memorável.

**Half Moon Bay Cougars 4 San Mateo Mavericks 2  
Becomes - HMBC4!smm2#**



## 2FA

O seu empregador pode exigir uma autenticação mais forte para que possa aceder às aplicações ou à rede da empresa. A autenticação de dois fatores funciona de forma muito semelhante ao seu cartão multibanco, que requer algo que tem e algo que conhece, o PIN. Muitas empresas utilizam agora autenticação de dois fatores para o acesso ao seu correio eletrónico, VPN da sua empresa, Google Apps, Office 365 e muito mais. Enquanto o seu banco pode utilizar códigos SMS para fornecer este nível de segurança, o seu empregador pode utilizar uma aplicação móvel para autenticação de dois fatores ou permitir a autenticação push para o seu dispositivo. Isto é mais seguro do que utilizar SMS ou mensagens de texto, porque os SMS utilizam o seu serviço de rede móvel.

## Emails de SPAM

Nos últimos tempos, tem havido um fluxo de emails SPAM que tentam criar medo e preocupação devido à recente pandemia. Embora nos possamos sentir tentados a abrir alguns, eles são tipicamente utilizados para publicidade, phishing, propagação de malware, etc. Se o spam chegar à sua caixa de entrada, apague-o

## Encriptar os seus dispositivos móveis

Os dispositivos que utiliza para fins profissionais contêm certamente informação valiosa para um cibercriminoso. Na fatalidade de perder um smartphone ou o seu computador portátil empresarial o risco de segurança da sua empresa aumenta significativamente. Sem encriptação nestes dispositivos, toda a informação neles contida será facilmente acedida, como por ex.: emails, credenciais, documentos, fotografias, acessos à rede empresarial (VPN), entre muitos outros dados sensíveis.

A encriptação dos dispositivos que utiliza profissionalmente vai assegurar que em caso de perda ou roubo físico dos equipamentos, toda a informação neles contida estará inacessível, evitando fugas de informação sensível que podem comprometê-lo e à sua empresa.

## Emails de phishing

Os cibercriminosos utilizam o correio eletrónico para fingir ser uma empresa ou serviço, pedindo-lhe que faça algo, geralmente com urgência. Eles esperam que depois clique no link e preencha as informações solicitadas. Um método ainda mais direto e direcionado é chamado spear phishing. Em vez de ir atrás de muitas vítimas por uma pequena recompensa, o criminoso vai atrás de um número menor ou de vítimas individuais de alto valor. O objetivo é normalmente obter acesso a um sistema reunindo as suas credenciais, ou instalar malware no seu computador.

### Algumas das melhores dicas para evitar o phishing são:

- Verifique quem é realmente o remetente do e-mail.
- Verifique o e-mail e procure erros gramaticais e ortográficos.
- Passe o rato por cima do link para ver para onde vai. Se alguma vez tiver alguma dúvida, não clique na ligação. Em vez disso, introduza manualmente o URL da empresa no seu navegador.
- Contacte a sua equipa de segurança/apoio informático em caso de dúvida.

## Email da empresa comprometido

O Business Email Compromise, ou BEC, pode acontecer por meio de um ataque de spear phishing que visa membros da liderança ou da equipa financeira da empresa. O perpetrador tentará fazer-se passar por executivos para convencer os destinatários do correio eletrónico a transferir dinheiro rapidamente ou realizar uma tarefa para uma operação supostamente crítica para a organização. Na realidade, o dinheiro ou credenciais para contas são transferidos para os cibercriminosos.

A utilização de ferramentas de colaboração apenas internas pode ajudar a proteger contra instruções ou transações não autorizadas. Por exemplo, os sistemas de videoconferência e chat devem ser utilizados como parte formal do sistema de aprovação para que a validação seja feita "pessoalmente", mesmo quando remota.

