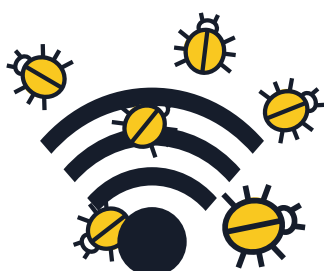
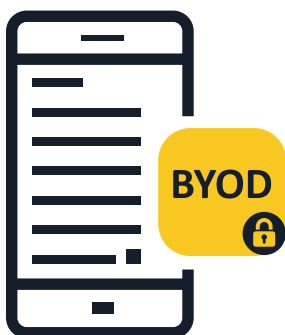


SOFTWARE MALICIOSO EM DISPOSITIVOS MÓVEIS

SUGESTÕES E CONSELHOS PARA EMPRESAS



1 Informe os seus colaboradores acerca dos riscos dos dispositivos móveis

- O trabalho com dispositivos móveis esbate as linhas que separam o uso profissional do uso pessoal. As empresas podem ser gravemente afetadas por um ataque que vise inicialmente o dispositivo móvel de um indivíduo. O dispositivo móvel é um computador e deve ser protegido como tal.

2 Implemente uma política empresarial BYOD (Bring-your-own-device, Traga o seu próprio dispositivo)

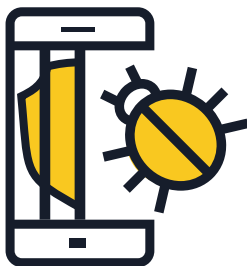
- Os colaboradores que utilizem os seus próprios dispositivos móveis para aceder a dados e sistemas da empresa (mesmo que se limitem a enviar e-mails, agendar compromissos ou aceder à base de dados de contactos) devem seguir as políticas da empresa. Escolha com cuidado as tecnologias a utilizar para gerir e proteger os dispositivos móveis, e incentive o pessoal a tomar as devidas precauções.

3 Inclua as políticas de segurança para dispositivos móveis no plano de segurança geral da empresa

- Se um dispositivo não cumprir as políticas de segurança, não deverá permitir a respetiva ligação à rede da empresa nem o acesso aos dados corporativos. As empresas devem implementar as suas próprias soluções de Gestão de dispositivos móveis (MDM, Mobile Device Management) ou Gestão de mobilidade empresarial (EMM, Enterprise Mobility Management).
- Como complemento, é imperativo instalar uma solução de Defesa contra ameaças a dispositivos móveis (Mobile Threat Defence). Esta permitirá uma maior visibilidade e consciência contextual das ameaças a aplicações, redes e sistemas operativos.

4 Evite utilizar redes públicas de Wi-Fi para aceder aos dados da empresa

- Regra geral, as redes públicas de Wi-Fi não são seguras. Se um colaborador aceder aos dados da empresa utilizando uma ligação Wi-Fi gratuita de um aeroporto ou café, os dados podem ser expostos a utilizadores mal-intencionados. Aconselhamos as empresas a adotar e desenvolver políticas de "utilização eficaz" nesta matéria.



5 Mantenha os sistemas operativos e as aplicações dos dispositivos atualizados

■ Aconselhe os seus colaboradores a descarregar as atualizações dos sistemas operativos dos respetivos dispositivos móveis sempre que tal for solicitado. Em especial, para quem utiliza o Android, pesquise os fornecedores de dispositivos móveis e fabricantes de telemóveis para conhecer as respetivas políticas de atualização. A instalação das atualizações mais recentes garante não só uma maior proteção do dispositivo, como também um melhor desempenho do mesmo.

6 Instale aplicações apenas de fontes seguras

■ As empresas devem permitir apenas a instalação de aplicações de fontes oficiais nos dispositivos móveis ligados à rede utilizada pelas próprias empresas. Como opção, pondere criar uma loja de aplicações da empresa, através da qual os utilizadores finais podem aceder, descarregar e instalar aplicações autorizadas pela empresa. Consulte o seu fornecedor de segurança para obter informações de configuração ou defina as suas próprias configurações.

7 Evite o jailbreak

■ O jailbreak é o processo de remoção dos limites de segurança impostos pelo fornecedor do sistema operativo, obtendo acesso total ao sistema operativo e às funções do dispositivo. Se fizer jailbreak no seu próprio dispositivo, pode reduzir drasticamente a respetiva segurança, abrindo brechas na segurança que podem não ser tão óbvias. Não devem ser permitidos dispositivos com privilégios root no ambiente empresarial.

8 Pondere alternativas de armazenamento na nuvem

■ É frequente os utilizadores de dispositivos móveis quererem aceder a documentos importantes, não apenas através dos seus PC de trabalho, mas também a partir de telemóveis ou tablets particulares fora do escritório. As empresas devem avaliar a criação de um sistema de armazenamento seguro, baseado na nuvem, e de serviços de sincronização de ficheiros para satisfazer estas necessidades de forma segura.

9 Encoraje o seu pessoal a instalar uma aplicação de segurança móvel

■ Todos os sistemas operativos correm o risco de serem infetados. Se estiver disponível, certifique-se de que os colaboradores utilizam a uma solução de segurança móvel que detete e evite software malicioso, spyware e aplicações malignas, além de incluir outras funções de privacidade e antirroubo.