Proteção de dados – O dia-a-dia

Amanhecer 7h-9h

Abertura de emails

Consultar o email a partir do seu telemóvel pode ser em alguns casos perigoso, já que pode não ser capaz de ver toda a informação do Remetente. Se não conhece a fonte, não o abra. Se suspeita que alguma coisa possa ser perigosa, ex, Phishing, quando chegar ao escritório reporte o mais rápido possível à equipa de IT ou reporte através do botão Report Phishing presente no ecrã.

Conversar

Tenha atenção ao que está a dizer e se está a falar muito alto. Podem estar pessoas próximas de si a ouvi-lo e algumas conversas mais sensíveis podem ser classificadas de "dados pessoais".

Usar o seu telemóvel para troca de emails

Verificar se os endereços de email, conteúdos e anexos estão corretos antes de enviá-los, é uma tarefa difícil de fazer no telemóvel. Se for possível, espere até chegar ao escritório. Caso contrário, tenha a certeza de que está a utilizar o sistema de email da sua empresa.

No escritório 9h-17h

Download de documentos

Durante o trabalho, pode encontrar uma app, um browser ou um sistema de IT que acredita que vai melhorar a performance do negócio e, por isso, terá vontade de subscrevê-lo ou fazer download. Todas as requisições de software (instalações ou aplicações web) têm de ser sempre aprovadas pela equipa de IT, de forma a evitar um virus ou outro tipo de problemas.

Envio seguro de emails a partir do escritório

Utilize apenas o sistema oficial de email da empresa para assegurar que os emails são vistos e enviados de forma segura, et assim quaisquer controlos adicionais (ex. Virus, rastreio de malware, monitorização) não deixarão de ser feitos. Siga todas as políticas de segurança da equipa de IT da sua empresa, no que respeita "screen-locks", proteção de "password" e armazenamento.

Visionamento de dados pessoais ou sensíveis

Já viu dados pessoais ou sensíveis? Assegure-se que os dados são seguros. Evite partilhá-los a não ser por uma razão justificada.

Tranferência de dados pessoais

E sobre o envio de dados a parceiros? Espere até saber que a sua empresa tem um contrato ou assinou um acordo de divulgação dos mesmos. Quando aprovada a transferência, utilize uma solução segura para partilhar essa informação.

Remover ou arquivar ficheiros antigos

Tem ficheiros ou relatórios antigos? Arquive ou apague-os se não precisa mais deles. Verifique com a equipa de IT sobre processos locais aprovados, incluindo quaisquer políticas de retenção de documentos, marcação e destruição.

Fim de tarde 17h-19h

Deixar informação "disponível"

Não deixe o seu PC aberto ou com o ecrã desbloqueado. Lembre-se de bloquear sempre o seu ecrã quando deixa o PC e desligue-o totalmente quando vai para casa.

Levar dados para fora do escritório

Pode necessitar de levar dados para fora do escritório quando trabalha em casa ou está numa viagem de negócios., especialmente se estão no seu PC. Não negligencie o seu uso, independentemente de onde está a utilizá-los. Tudo o que está numa USB ou numa pasta deve continuar a ser gerido, de acordo com os habituais processos da empresa.

Eliminação de dados confidenciais

Não deixe documentos confidenciais perdidios (tal como no comboio ou noutro lugar) – tenha a certeza que os guarda, ou se não precisa mais deles, triture-os ou coloque numa zona de lixo segura.

Estar online

No regresso a casa, pense duas vezes antes de se conectar a uma rede WiFi pouca segura (ex. Viagem de comboio, ou metro). Se pretende aceder a dados pessoais, use sempre VPN (Rede Privada Virtual) que encripta os dados mesmo que através de uma rede potencialmente segura.