FICHA INFORMATIVA

Guia da Shred-it para manter seguros os seus dados após as férias de verão

Os meses de verão são o período preferencial para os colaboradores tirarem as suas bem merecidas férias. No entanto, quando regressam, é uma boa prática corporativa recordar-lhes como devem lidar com dados confidenciais, essencial para reduzir os riscos de uma fuga de dados.

SABIA QUE... O custo médio de uma violação de dados é de €3,533,430? [1] E que 31% dos consumidores perderia a confiança numa empresa que sofresse uma violação de dados? [2]

Estas são algumas sugestões de segurança que os colaboradores devem seguir, consideradas boas práticas, após o regresso das suas férias:

1. Reduza a quantidade de dados armazenados num dispositivo móvel, mantendo apenas o que é essencial para as suas funções.
2. Mantenha-se atento ao trabalhar remotamente num café, aeroporto ou autocarro. Guarde os materiais de trabalho ou mude de lugar se alguém parecer suspeito.
3. Evite partilhar dispositivos eletrónicos com familiares, amigos e externos. Bloqueie-os quando não estiverem a ser usados. Mantenha os documentos sensíveis e confidenciais num local seguro.
4. Cuidado com os e-mails de phishing e sites maliciosos. Alguns elementos que podem alertá-lo incluem erros ortográficos, erros gramaticais, endereços de e-mail suspeitos e apelos urgentes à sua ação. Nunca envie por e-mail detalhes pessoais, como nomes, morada ou detalhes do cartão de crédito.
5. Siga os procedimentos da sua empresa para a destruição segura de dados em papel e em formato digital. Não coloque papel em caixotes do lixo nem em contentores de reciclagem. Não envie para o lixo dispositivos eletrónicos sem utilidade. Leve-os para o escritório após o verão e entregue-os para destruição segura e definitiva.
6. Não ligue dispositivos USB desconhecidos. Utilize apenas dispositivos aprovados pela empresa.
7. Num local público, não deixe os dispositivos móveis sozinhos ou visíveis no carro.
8. Atualize o software e instale os patches assim que possível. Estudos confirmam que 82% das fugas de dados registadas ocorreram devido a uma falha na atualização de patches. [3]
9. Reforce as senhas em todos os dispositivos e contas (passwords longas em termos de caracteres, incorporando números, letras e símbolos). Mais de 60% das violações envolvem senhas de acesso. [4]
10. Desligue o Wi-Fi e Bluetooth quando não forem necessários. Para enviar ou receber elementos confidenciais ou ligar-se à rede do escritório, utilize hotspots pessoais, uma rede virtual privada (VPN) ou redes Wi-Fi protegidas por senha. A ligação via Bluetooth criptografa os dados.

1 https://www.ibm.com/security/data-breach
2 Shred-it Data Protection Report 2020
3 Voke Media, Secure Operations Automation Market Snapshot report
4 https://www.verizon.com/business/resources/reports/dbir/

Para saber mais sobre as melhores práticas de segurança, visite Shredit.pt ou ligue para 808 200 246.

Protegemos o que importa.

Shred-it®
Uma Solução Stericycle®