

INTRODUÇÃO

O presente número da newsletter do Centro Nacional de Cibersegurança, debruça-se sobre algumas práticas preventivas para uma utilização mais segura do ciberespaço, aquilo que designamos por ciberhigiene. O objetivo passa por sensibilizar o leitor para alguns cuidados a ter, sendo que os tópicos que se seguem representam um conjunto de medidas que devemos executar para minimizar alguns dos desafios com que nos deparamos diariamente no universo digital.

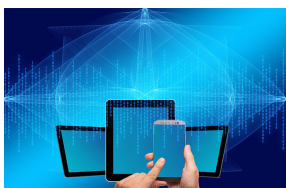
CIBERESPAÇO: AS MEDIDAS PREVENTIVAS PARA OS SEUS UTILIZADORES



Costuma fazer ciberhigiene?

A ciberhigiene é quase tão importante como a higiene pessoal que fazemos diariamente. Trata-se de um conjunto de práticas, na sua maioria rotineiras, que devemos seguir para garantir a limpeza tecnológica dos nossos equipamentos e sistemas pessoais.

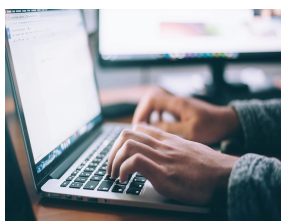
[+ ver mais](#)



Atualização dos sistemas, diz-lhe alguma coisa?

Esta é uma das problemáticas mais importantes da cibersegurança, a da desatualização dos sistemas operativos e das respetivas aplicações que diariamente utilizamos. Se não fizermos atualizações, as fragilidades e dificuldades de desempenho que os fabricantes identificaram e já resolveram, não são aplicadas. Estas atualizações são importantes também ao nível da estabilidade e da fiabilidade global dos sistemas.

[+ ver mais](#)



O que faria se perdesse toda a sua informação?

Esta é uma pergunta que nos leva a refletir sobre a verdadeira importância de backups - que devemos fazer aos dados do computador, tablet, smartphone, memória da máquina fotográfica, entre outros. Fazer backups, ou cópias de segurança com alguma regularidade, é umas das preocupações que todos nós, enquanto utilizadores frequentes do ciberespaço, devemos ter.



O que é um backup?

Quando falamos em backups, referimo-nos a uma cópia dos arquivos importantes guardados em dispositivos eletrónicos, como por exemplo, computadores fixos ou portáteis. Os arquivos em questão podem ser fotografias e vídeos pessoais, documentos de importância do trabalho, e-mails, dados de acesso, listas de contactos, etc.

[+ ver mais](#)



Cuidado com os emails forjados

Uma ação tão simples como abrir uma mensagem de e-mail, pode tornar-se uma experiência pouco agradável, tendo em conta que o e-mail é um dos principais meios de propagação de vírus. Neste sentido, fatores como, links, ficheiros anexados, mensagens HTML e scripts incluídos (no envio ou receção de e-mails), podem servir de via para aplicações mal-intencionadas - o conhecido malware.

[+ ver mais](#)



A importância da palavra chave

A palavra-passe é fundamental para a proteção dos sistemas, sendo esta a primeira forma de se defender contra o cibercrime. A palavra-chave, juntamente com a sua identificação, fazem parte integrante da sua identidade digital. Para criar uma palavra-passe segura, esta deve preencher alguns requisitos, tais como:

- **Criar** uma palavra-passe comprida, composta por números, letras e símbolos; use letras minúsculas e maiúsculas; pode usar várias mnemónicas para ser mais simples de memorizar;
- **Utilizar** uma palavra-passe exclusiva para cada uma das suas contas com maior importância (por exemplo, as contas de e-mail ou do banco online);
- **Guardar** as palavras-passe num local secreto, que seja dificilmente avistado por terceiros; escreva as mnemónicas que usou e não a palavra-chave diretamente;
- **Configurar** as suas opções de recuperação de palavra-passe e mantê-las atualizadas.