https://www.cncs.gov.pt/pt/como-cifrar-e-proteger-ficheiros-e-mensagens-de-email/

# COMO CIFRAR E PROTEGER FICHEIROS E MENSAGENS DE EMAIL

## Porquê cifrar e proteger?

Os conteúdos que enviamos por *email* ou que guardamos nos nossos dispositivos ou num servidor em "nuvem" podem ser apetecíveis para eventuais agentes maliciosos. A violação de dados é uma das consequências mais comuns dos ciberataques. Por isso, uma das formas de prevenir os efeitos nefastos provocados por um incidente de cibersegurança é cifrar estes dados ou criar pastas com acesso restrito, adicionando uma camada de proteção para lá de todos os outros cuidados essenciais à cibersegurança.

O ato de cifrar consiste em transformar um conteúdo legível em algo ilegível, mas passível de ser reconvertido em algo legível através de uma chave. Pode não ser necessário aplicar esta técnica a todos os conteúdos que guardamos ou partilhamos, mas em relação a alguns pode valer a pena. Por exemplo, alguns ficheiros contêm dados pessoais relativos a contas bancárias ou exames médicos. Outros são fotografias ou vídeos da vida privada. Estes tipos de conteúdos podem ser especialmente protegidos para o caso de os nossos dispositivos ou a nossa conta numa plataforma em "nuvem" serem comprometidos.

Também existem alguns *emails* mais sensíveis do que outros. Por vezes, partilhamos ficheiros com dados pessoais ou escrevemos mensagens com informação crítica do ponto de vista pessoal ou profissional. Nestes casos pode ser importante criar a tal camada adicional de segurança. Nada é protegido a 100%, e este tipo de cuidado pode ser contornado por técnicas muito sofisticadas, mas quanto mais dificultarmos o acesso aos nossos dados e dispositivos, melhor. Por isso, sugere-se um conjunto de fontes das marcas mais utilizadas onde é possível encontrar tutoriais simples e curtos que ajudam a cifrar e proteger ficheiros e mensagens de *email* de acordo com os produtos em questão.

## Como cifrar e proteger ficheiros num dispositivo:

a. O sistema operativo Windows é um dos mais comuns. Por isso, consulte estas páginas da Microsoft onde encontra tutoriais simples sobre como cifrar ficheiros no Windows: aqui e aqui.
b. Os computadores da marca Apple, igualmente muito conhecidos, utilizam um sistema operativo próprio, o macOS, o qual também permite que se cifrem ficheiros, quer no computador, quer em dispositivos amovíveis. Para o efeito, consulte estas páginas: aqui, aqui e aqui.
c. O sistema operativo para *smartphones* Android, da Google, muito utilizado, fornece um serviço chamado "pasta segura", o qual protege os ficheiros que coloca no seu interior, através de um PIN com 4 dígitos. Para saber como: aqui.
d. No caso dos *smartphones* da marca Apple, os Iphones, que utilizam o sistema operativo iOS, existe um serviço que permite proteger as suas notas através de uma palavra-passe, do Face ID ou do Touch ID. Siga as instruções: aqui.

**Nota**: existem diversas aplicações no mercado que permitem realizar operações que cifram ficheiros. Caso adquira uma, como critérios, escolha as que sejam vendidas em plataformas reconhecidas, que respondam às suas necessidades e que tenham boas críticas de utilizadores e especialistas. Também existem programas de fonte aberta que podem ser boas opções.

## Como cifrar mensagens de *email:*

a. Caso utilize como plataforma de gestão de *email* o serviço Outlook, da Microsoft, poderá aprender a cifrar os seus *emails:* aqui.
b. Na eventualidade de utilizar o serviço de *email* Gmail, da Google, encontra-se disponível um tutorial nesta página: aqui.
c. Para quem utiliza o ambiente Exchange no iOS, da Apple, e pretenda cifrar um *email,* pode seguir os seguintes passos: aqui.

**Nota**: em qualquer destes casos que permitem cifrar as mensagens de *email* é necessário que a aplicação suporte a norma S/MIME, a qual permite utilizar um conjunto de especificidades de segurança no envio

de *emails.* Para mais detalhes, consulte a seguinte página (em inglês): aqui.
Esta camada de proteção não substitui outras tecnologias essenciais para a segurança do *email,* como o protocolo TLS.
Para um aprofundamento desta matéria e deste tipo de funcionalidades, aconselhamos uma leitura (em inglês) sobre o sistema PGP (Pretty Good Privacy).

Aviso: todas as páginas partilhadas foram consultadas pela última vez no dia 3 de maio de 2022. Eventuais desatualizações podem resultar de inovações dos produtos em causa. As escolhas destes exemplos resultam da sua popularidade de uso e não de critérios relacionados com a cibersegurança.

*Acedido em 03-05-2022*