**Como criar boas palavras-chave**

Autor: CERT.PT- Serviço de Resposta a Incidentes de Segurança Informática

Todos os dias utilizamos *passwords* para acesso aos mais variados serviços ou aplicações. Uma password, senha, palavra-chave ou passe serve para aceder a estes serviços através de autenticação fidedigna de identidade e garantia pessoal de acesso. Estas são por norma privadas para o utilizador e devem ser bem salvaguardadas para evitar roubos de identidade e fraudes de identidade.

A salvaguarda de uma *password* começa logo na sua criação. Ao gerar asuasenha, o utilizador deve ler atentamente as regras de formulação da mesma. Esta deve ser tão complexa quanto a criticidade do serviço a que se destina. Pode usar uma palavra-chave fraca para aceder ao site de um jornal, mas é evidente que a palavra-chave que usa para o seu mail deve garantir maior segurança e a que usa para consultar ou movimentar a sua conta bancária deve ter uma complexidade ainda mais elevada.

Um cuidado a ter na criação de uma boa palavra-chave é o de não usar elementos pessoais associados a si ou conhecidos por mais pessoas que não o próprio, tais como: datas de nascimento, partes do nome e apelidos, morada, números de identidade, contribuinte, etc. É relativamente fácil obter esta informação a respeito de qualquer pessoa e testá-la em seguida como senha de acesso em qualquer serviço possivelmente subscrito pelo utilizador.

De evitar são ainda senhascriadas com a proximidade entre caracteres no teclado, como "QwerTAsdfG". Para além de serem já conhecidas, estas senhas são facilmente observáveis no momento da digitação. Para reforçar a proteção contra ataques conhecidos, aconselha-se a utilização do comprimento máximo admissível para senhas, definido pelo sistema de autenticação em causa e desaconselha-se a utilização de palavras encontradas em listas ou dicionários de língua portuguesa ou estrangeira.

Formular uma palavra-chave segura requer imaginação. Por um lado esta deve ser facilmente memorizável, por outro, deve ser difícil de adivinhar por terceiros. Uma forma de aumentar a robustez da senha é a combinação não sequencial de letras, números e símbolos Existem algumas dicas que podem ajudar a criar uma senha forte. Uma metodologia possível será identificar uma frase que lhe seja fácil de lembrar; Exemplo: “criar password forte em três passos para melhorar a segurança”. De seguida utilizar na sua *password* a primeira letra de cada palavra: “CPFETPPMAS”.

Finalmente poderá ainda substituir letras maiúsculas por minúsculas e letras por números e símbolos: “cPFe3ppm@s”.

---------------------------------------------------------------------------

**Mês Europeu da Ciber-Segurança**

Este artigo é da autoria de especialistas do CERT.PT- Serviço de Resposta a Incidentes de Segurança Informática (www.cert.pt) da FCCN-Fundação de Computação Científica Nacional (www.fccn.pt/pt) e insere-se na campanha "Uma dica por dia" integrada no Mês Europeu da Cibersegurança, que tem lugar em Outubro de 2013.

O Mês Europeu da Ciber-Segurança é uma iniciativa da ENISA - Agência Europeia para a Segurança das Redes e Informação (www.enisa.europa.eu) e o seu objectivo é informar os utilizadores sobre a importância da segurança da informação, bem como demonstrar algumas medidas simples para proteger os seus dados.

------------------------------------------------------------------------------

**Autor da Foto: Federico Caputo**

Nota: existe um ficheiro independente para download, com melhor resolução.

