Sair em segurança

Ao aceder à conta de e-mail ou outra conta (site de comércio electrónico, home banking ou plataforma) em que se exige o nome do utilizador e uma senha, clique sempre, para sair do site, no botão/link de nome Logout, Logoff, Sair, Desconectar ou equivalente. Pode parecer óbvio, mas simplesmente sair do site e fechar a janela do navegador de Internet pode ser arriscado, porque o sistema não recebeu a instrução de encerrar o acesso, naquele momento. Assim, alguém mal intencionado pode abrir o navegador de Internet e aceder às informações da conta, caso esta realmente não tenha sido fechada devidamente.

Ao entrar num site em que se exige o nome de utilizador e palavra-chave, o sistema recebe e regista esses dados, dando início a uma sessão de trabalho. Enquanto a sessão durar, essa informação está activa: o sistema reconhece o utilizador e permite a realização de tarefas inerentes ao seu perfil. Para terminar a sessão, o sistema precisa de receber e de registar essa intenção do utilizador. Se, em vez de se clicar no botão ou link «Sair» (ou equivalente), e apenas se fechar o navegador a sessão de trabalho não é encerrada. Se alguém utilizar o mesmo computador de seguida, pode abrir o navegador de Internet e aceder ao mesmo site sem que lhe sejam exigidos o nome de utilizador e palavra-chave. Para todos os efeitos, o sistema assume que continua em linha e o novo utilizador permanece com os dados do utilizador anterior, acedendo às suas tarefas e perfil.

(Texto adaptado)

REFERÊNCIA BIBLIOGRÁFICA

SeguraNet - *Utilização segura de palavras-chave*. [Em linha]. [Consult.17 de Janeiro de 2011]. Disponível em: WWW:<URL: http://www.seguranet.pt/educadores/>.

ESCOLA SECUNDÁRIA DR. JOAQUIM DE CARVALHO, FIGUEIRA DA FOZ

BIBLIOTECA ESCOLAR

BLOGUE: http://www.netbiblio.blogspot.com

E-mail: biblioteca@esjcff.pt

Escola Secundária Dr. Joaquim de Carvalho, Figueira da Foz
Biblioteca Escolar

Guia

SeguraNet

Palavras-chave

Palavras –chave

O que são e para que servem as palavras-chave?

Uma palavra-chave ou senha (ou password, em Inglês) é um conjunto de caracteres previamente convencionado, entre duas partes, como forma de reconhecimento.

As palavras-chave são muito utilizadas para autenticar os utilizadores e conceder-lhes privilégios ou para lhes permitir o acesso a informação personalizada, armazenada nos sistemas informáticos.

Memorização da palavra-chave

Quem navega na Internet encontra, muitas vezes, sítios que pedem o registo com palavra-chave. Para evitar a multiplicação de senhas e facilitar a sua memorização, há utilizadores que usam sempre a mesma. Mas tal não é recomendável: se alguém mal-intencionado descobrir a senha, num dos sítios, nos restantes ficarão indefesos.

Diversos utilizadores colocam um visto na secção "Memorizar senha". Quando acedem àqueles sítios, ao escreverem o nome de utilizador, a senha aparece automaticamente sob a forma de ••••••. Não é seguro confiar a memorização da palavra-chave ao programa de navegação (ou browser).

Para desactivar a opção de memorização da palavra-chave, siga os passos:

No Firefox: Ferramentas > Opções > Segurança > em Memorizar as senhas para sítios, retire o visto. Se clicar sobre o botão Mostrar senhas, poderá visualizar as que estão guardadas e removê-las. No final, clique Ok.

Se usar o Internet Explorer: Ferramentas > Opções da Internet > Conteúdo > no campo Conclusão Automática, clique em Definições > em Nomes de utilizador e palavras-chave em formulários, retire o visto. No final, clique Ok.

Alguns truques para criar palavras-chave

• Não se deve utilizar sempre a mesma palavra-chave para todas as situações. Se algum dos computadores ou sistemas on-line que usam esta palavra-chave ficar desprotegido, também toda a informação protegida por essa senha deve ser considerada comprometida. É fundamental usar palavras-chave diferentes para sistemas diferentes. Exemplo: Em sítios como bancos e lojas, use uma senha diferente para cada um.

• Crie palavras-chave longas. Cada carácter que se adiciona à palavra-chave multiplica várias vezes a protecção que ela fornece. Cada palavra-chave deve ter, no mínimo, uma extensão de 8 caracteres; o ideal seria que cada palavra-chave fosse formada por 14 caracteres ou mais.

• Combine letras, números e símbolos. Quanto maior for a variedade de caracteres que a palavra-chave contenha, mais difícil se torna descobri-la. Uma palavra-chave ideal combina a extensão com diferentes tipos de símbolos. Usar todo o teclado, não apenas os caracteres mais comuns. A palavra-chave será muito mais segura se escolhermos entre todos os símbolos no teclado, incluindo sinais de pontuação que não estejam na primeira fila do teclado e símbolos próprios da língua portuguesa (ç,ã,ê, etc).

• Não divulgue as suas palavras-chave. Não permita o acesso às suas palavras-chave por parte de amigos e membros da família (especialmente crianças mais novas) que poderiam facultá-las a alguém menos digno de confiança.

• Utilize palavras e frases que sejam fáceis de recordar, mas difíceis de descobrir.

• Não utilize o nome de utilizador ou os dados de início de uma sessão.

• Não utilize senhas fáceis de serem descobertas, como nome de parentes, data de aniversário, matrícula do carro, nº do BI ou do NIF ou informação pertencente aos que lhe são mais queridos. Estas serão das primeiras senhas que um criminoso tentará, para descobrir as palavras-chave.

• Não guarde as senhas num ficheiro ou em qualquer outro programa. Se necessitar de registar uma senha num papel (em casos extremos), destrua-o assim que a decorar.

• Não aceda à Internet como administrador do computador. Crie e use, preferencialmente, uma conta limitada de utilizador.

• Mude as senhas com regularidade.

• Nunca forneça palavras-chave por e-mail. Qualquer mensagem de e-mail que solicite dados pessoais, ou que peça para verificar os dados num sítio é de certeza uma fraude! Uma mensagem de e-mail pode ser interceptada e uma mensagem de e-mail que peça qualquer informação pode não ser do emissor que lá consta. Estes esquemas, conhecidos como esquemas de phishing, usam mensagens de e-mail fraudulentas para aliciar o utilizador a revelar os dados pessoais.

• Evite sistemas de armazenamento on-line. Se um utilizador mal intencionado encontra estas palavras-chave, armazenadas on-line, ou num computador de uma rede, ele passa a ter acesso a toda a informação.

• A utilização da senha em branco nem sempre é uma boa ideia. Por exemplo, um portátil que se transporte diariamente, provavelmente não está fisicamente seguro, pelo que, nesses casos, deve ter uma palavra-chave com elevado grau de segurança.