



## PRÁTICAS 2

### ALGUMAS PRECAUÇÕES BÁSICAS DE NAVEGAÇÃO NA INTERNET

Por considerarmos da maior utilidade estes conselhos práticos fornecidos aos professores, resolvemos divulgá-los para que os pais possam também estar atentos à sua aplicação, transmitindo-os ao resto da família.

Aqui encontrará alguns procedimentos e informações, que visam ajudá-lo a uma navegação mais segura na Internet, em particular para prevenir a recolha invisível de dados pessoais ou a utilização fraudulenta da identidade de outrem.

Ao longo do desenvolvimento do Projecto Dadus, iremos continuar a abordar questões relativas à Internet e serão explorados temas específicos sobre o uso correcto das tecnologias ao nosso dispor e os cuidados práticos a observar para nos protegermos.

#### ▣ **Palavras-passe (*passwords*)**

Navegar pela Internet significa também fazermos uma colecção de palavras-passe. Elas são indispensáveis para a nossa autenticação como utilizador autorizado ou registado e, conseqüentemente, poderemos aceder aos conteúdos desejados, enviarmos a nossa

informação ou gerirmos uma área pessoal, como a caixa de correio electrónico, o perfil no Hi5, as informações fiscais, a conta bancária, etc.

Por isso mesmo, as palavras-passe valem hoje tanto como as informações que elas protegem e há criminosos que se dedicam a apanhar ou a descobrir palavras-passe.

Em primeiro lugar, não devemos escrever palavras-passe em computadores que não controlamos (cibercafés, salas de aeroporto, conferências, sistemas partilhados), pois tal não é considerado seguro. Toda a navegação que se fizer a partir desses pontos deve ser anónima. Esses computadores não devem ser usados para verificar contas de correio electrónico, aceder a contas bancárias, salas de conversação, correio profissional, ou qualquer outra conta que implique a introdução de nome de utilizador e palavra-passe.

Com efeito, as palavras-passe são a primeira linha de defesa da nossa privacidade. Por isso, a primeira coisa a fazer é arranjar palavras-passe fortes, diferentes umas das outras e secretas:

- **FORTES:** (1) usar uma palavra-passe que seja difícil de descobrir e preferencialmente ilógica (não pôr o seu nome ou o do seu filho, a sua data de nascimento ou outra informação fácil de adivinhar), que tenha pelo menos oito caracteres (acima de 14 seria o ideal), misturando números, letras e símbolos diferentes, maiúsculas e minúsculas e evitando sequências ou caracteres repetidos (2) Mudar regularmente a palavra-passe para minimizar os riscos de utilização indevida, caso alguém a tenha descoberto. Normalmente, os sites têm uma área, que pode ser descrita como “a minha conta”, “área pessoal” ou “os meus dados pessoais” onde poderá alterar periodicamente a sua palavra-passe. (3) Não aceitar a memorização automática da sua palavra-passe, por muito jeito que isso lhe possa dar, pois se alguém entrar no seu computador (física ou remotamente), tem a vida muito facilitada, pois a palavra-passe está gravada no computador. Tal é especialmente válido para computadores partilhados por diferentes pessoas.

- **DIFERENTES:** usar palavras-passe diferentes para todos os sítios onde precisa de entrar com senha. Se usar sempre a mesma palavra-passe e ela for descoberta, toda a sua informação ficará comprometida. É muito difícil memorizar todas as palavras-passe e pode sempre socorrer-se de uma cábula, pelo menos para aquelas que usa menos. No entanto, é importante que resguarde as anotações que fizer em lugar seguro. Para ser mais fácil recordar-se da palavra-passe, poderá usar palavras ou frases fáceis para si de memorizar mas difíceis para outros de descobrir.
- **SECRETAS: (1)** as palavras-passe devem ser, regra geral, individuais. Contudo, de acordo com as idades das crianças, o entendimento familiar pode ir no sentido de os pais conhecerem as palavras-passe dos filhos. O contrário deve ser evitado a todo o custo, pois as crianças podem transmiti-las a terceiros. Mas, em princípio, as palavras-passe não devem ser partilhadas entre colegas ou com outras pessoas, da mesma forma que não se divulga o código do cartão Multibanco ou o segredo do cofre.  
**(2)** Nunca se deve divulgar palavras-passe por correio electrónico nem responder a pedidos de verificação da palavra-passe recebidos por e-mail. Essa é uma forma fraudulenta de obtenção de palavras-passe (um dos esquemas do chamado *phishing*), com o objectivo de roubo de identidade.

### Fechar a sessão (*logout*)

Intimamente relacionado com as palavras-passe e precisamente para evitar que outros se façam passar por nós ou que acessem a conteúdos pessoais, é imprescindível mecanizar nos internautas a acção de “fechar sessão”.

Sempre que se termina ou interrompe temporariamente uma sessão na Internet – para a qual foi necessário introduzir palavra-passe (como por exemplo, na caixa de

correio electrónico, numa rede social, num fórum de discussão, num blog, no *netbanking*) – deve carregar-se na opção “terminar sessão” ou “fechar sessão”.

Por vezes, também pode aparecer a opção “sair”, mas tal pode não corresponder ao fechar da sessão, mas sim ao sair do site. Ora, se outra pessoa abrir o mesmo site a partir do mesmo computador (como pode acontecer, em particular, nas escolas, nos locais de trabalho, em casa ou em computadores de acesso público) sem que o utilizador anterior tenha fechado a sua sessão, o novo utilizador terá acesso à sessão do anterior utilizador.

Desse modo, acederá a toda a informação pessoal que aí se encontrar e pode continuar a navegar como se fosse a outra pessoa.

Por outro lado, se alguém conseguir entrar remotamente no seu computador, o que pode acontecer quando se está ligado à Internet e não se está tecnicamente bem protegido (e não há protecções infalíveis), pode também facilmente aceder à área pessoal de qualquer site que utilize e do qual tenha saído sem terminar a sua sessão. É necessária especial atenção no que diz respeito à caixa de correio electrónico, pois podem ser enviadas mensagens electrónicas (*e-mails*) em seu nome.

## Cookies

Os *cookies* são ficheiros de texto, colocados no computador do utilizador, quando este visita um *site* na Internet, para permitir reconhecer o visitante quando este volta ao mesmo *site*.

Os *cookies* contêm a informação necessária para reconhecer o visitante e, neste sentido, permitem relacionar o visitante com o registo automático do percurso de navegação interna do mesmo utilizador num determinado *site*: quando o *site* é consultado, que páginas são vistas, que documentos são descarregados, podendo assim o responsável do *site* conhecer melhor as preferências de cada utilizador.

Os dados relativos à navegação do visitante não são armazenados no *cookie*, mas sim no servidor do respectivo *site*.

O objectivo é adaptar-se da melhor maneira possível aos gostos do utilizador, disponibilizando de imediato conteúdos que, à partida, poderão ser do seu agrado.

Por outro lado, após análise do tipo de conteúdos a que um utilizador acede mais vezes num determinado *site*, o responsável por esse *site* pode dispor publicidade especialmente dirigida àquele visitante, logo que este aceder ao *site*.

Esta associação entre o reconhecimento que o *cookie* faz do visitante e os dados de navegação do visitante num *site* permite também que o visitante seja tratado de forma mais amigável, pelo nome (caso o tenha alguma vez indicado), ou que já não precisem de solicitar a morada ou outros contactos (desde que o tenham feito uma primeira vez).

Um motor de busca também pode colocar *cookies*. Neste caso, pode agregar facilmente a um mesmo utilizador todas as informações sobre as pesquisas realizadas, as áreas de maior interesse e os temas mais procurados por um determinado utilizador.

Nem todos os *sites* usam *cookies*, mas aqueles que o fazem devem informar os internautas desse facto, habitualmente através da política de privacidade, para que as pessoas possam escolher se os querem activados ou desactivados.

O nosso computador pode ser programado para aceitar ou rejeitar *cookies* e alguns navegadores de Internet alertam para a utilização de *cookies* por um determinado *site*. Uma vez que os *cookies* são armazenados no nosso computador, também é possível apagá-los.

Julho 2008

CNPD