Manter o computador seguro

A Internet oferece aos hackers, a oportunidade de acesso ao seu computador. De facto, apesar de a Internet ser um excelente meio de encontrar informação, efetuar downloads ou encontrar música, é nesse acesso que o seu computador se encontra mais exposto a eventuais ataques. Para minimizar esse risco, existem algumas medidas que poderá tomar:

Mantenha o Sistema Operativo e o browser do seu computador atualizados

Esporadicamente vão sendo descobertas vulnerabilidades de segurança nos Sistemas Operativos e browsers de acesso à Internet, razão pela qual as empresas produtoras do software vão lançando patches (atualizações) de segurança para correção desses problemas. As vulnerabilidades de segurança podem ser aproveitadas por vírus ou hackers para conseguirem um acesso não autorizado aos computadores desatualizados.

Para obviar estas fraquezas deverá visitar regularmente os websites das empresas de software para obter os patches de segurança e atualizações disponíveis.

Se utilizar uma das versões do sistema operativo Windows poderá aceder ao site http://windowsupdate.microsoft.com, para efetuar o download das últimas correções de segurança da sua versão do Windows e do browser Microsoft Internet Explorer.

Adicionalmente, poderá selecionar a opção Proteja o seu PC em 3 Passos, para aceder a um tutorial da Microsoft que o poderá ajudar a aumentar o nível de segurança do seu computador.

Utilize e mantenha atualizado um software Anti-Vírus

Os softwares de Anti-Vírus, desde que constantemente atualizados, constituem uma forte barreira à infeção por parte dos inúmeros vírus informáticos que circulam diariamente na rede e que podem implicar a perda de dados ou informação vital presente no seu computador ou permitir o acesso a este gerando uma falha de segurança. Poderá encontrar informação adicional sobre software de antivírus nos seguintes endereços:

Avira AntiVir: http://www.avira.com

Symantec Norton AntiVírus: http://symantec.com

Kapersky Anti-Vírus: http://www.kapersky.com

ESET NOD32 Anti-Vírus: http://www.eset.com

BitDefender Anti-Vírus: http://www.bitdefender.com

McAfee VirusScan: http://www.mcafee.com

Trend Micro AntiVirus plus AntiSpyware: http://www.trendmicro.com

ZoneAlarm AntiVirus: http://www.zonealarm.com

AVG Anti - Vírus: http://www.grisoft.com (versão gratuita)

Avast! Home edition: http://www.avast.com (versão gratuita)

Utilize software de Firewall

Uma firewall é um program que auxilia à proteção do seu computador e da informação nele contida, ao bloquear tentativas de intrusão e tráfego não autorizado de e para o seu PC. Poderá encontrar informação adicional sobre software de firewall nos seguintes endereços:

Norton Personal Firewall: http://www.symantec.com

Mcafee Personal Firewall: http://mcafee.com

CA Personal Firewall: http://ca.com

TrendMicro PC-Cillin Internet Security: http://www.trendmicro.com

Kapersky Internet Security: http://www.kapersky.com

Normal Personal Firewall: http://www.norman.com

Outpost Firewall: http://www.agnitum.com

Kerio Personal Firewall: http://www.sunbelt-software.com (versão gratuita)

Webroot desktop Firewall: http://www.webroot.com (versão gratuita)

Zone Alarm Firewall: http://www.zonelabs.com (versão gratuita)

Comodo Personal Firewall: http://www.personalfirewall.comodo.com (versão gratuita)

Utilize software Anti-Spyware

Spyware é todo o software com capacidade de captar informação teclada ou existente num computador e reenviá-la para outrém sem conhecimento do utilizador. Este software é muitas vezes dissimulado em mensagens de E-mail, auto instalando-se no computador do utilizador. Pelo facto de este tipo de software poder quebrar a privacidade na utilização da Internet é altamente recomendável a utilização e atualização constante de software Anti-Spyware.

Poderá encontrar informação adicional sobre software Anti-Spyware e Anti-Trojan nos seguintes endereços:

PestPatrol: http://www.pestpatrol.com

SuperAntiSpyWare: http://www.siperantispyware.com

Webroot Spy Sweeper: http://www.webroot.com

Ad- Aware SE Personal Edition: http://www.lavasoft.com (versão gratuita)

Spybot Search&Destroy: http://www.safer-networking.org (versão gratuita)

Spyware Terminator: http://www.crawler.com (versão gratuita)

a2 Free Anti-Trojan: http://www.emsisoft.com (versão gratuita)

Spyware Doctor: http://www.pctools.com

CounterSpy V2: http://www.sunbelt-software.com

Conservar o E-mail seguro

Como um meio de comunicação cada vez mais generalizado, algumas precauções se impõem na utilização do E-mail:

Nunca envie informação sensível por E-mail

Dado que a generalidade das mensagens de E-mail recebidas ou enviadas não possuem o seu conteúdo encriptado, qualquer informação pessoal incluída na mensagem está sujeita ao risco de interceção da informação, pelo que, em caso algum, deverá ser enviada informação sensível (como por exemplo a Identificação e o Código PIN do Montepio24 ou o número do Cartão de Crédito).

Assim, nunca deverá responder a qualquer E-mail inesperado solicitando informação pessoal, ou preencher quaisquer dados confidenciais numa página de Internet a que tenha acedido por intermédio de link disponibilizado numa mensagem de E-mail, mesmo que a mensagem pareça ser proveniente de um remetente credível.

O Montepio não envia mensagens automáticas aos seus Clientes solicitando Dados de Segurança ou informação confidencial, bem como deixou de incluir nos E-mails, quaisquer links para páginas do endereço www.montepio.pt.

Um tipo de fraude existente, consiste na criação de Web Sites falsos com imagens semelhantes às utilizadas nas páginas das Instituições Financeiras, com o objetivo de enganar os utilizadores, levando-os a inserirem informação pessoal (dados pessoais, códigos de acesso ou números de Cartões de Crédito). A captação destes dados, permitiria a utilização ilegítima para acesso a páginas privadas.

Os links para estas páginas falsas está, cada vez mais, a ser difundida por E-mail, anunciando a necessidade de alteração de códigos de acesso ou a alterações do nível de segurança de serviços de Internet Banking. Caso receba algum E-mail deste tipo, trate-o com desconfiança, mesmo que a página indicada aparente ser fidedigna e não insira nenhuma informação sensível que permita o acesso às suas contas.

Atenção aos E-mails inesperados com ficheiros anexos

Atualmente, as mensagens de E-mail são um dos meios mais comuns para o alastramento de vírus. Alguns vírus possuem a capacidade de se reenviarem para os endereços de E-mail da lista de contactos do PC infetado, o que implica que possa receber mensagens infetadas provenientes de um remetente conhecido.

Assim, não é aconselhável abrir ficheiros anexos a mensagens de E-mail com extensões: .exe, .pif, .vbs, dado estas poderem estar associadas a vírus. Com uma maior probabilidade de conterem vírus, ficheiros com duplas extensões (.jpg.pif, .doc.vbs, etc) nunca deverão ser abertos.

Preservar os Dados de Identificação

O «roubo de identidade» é o ato de apropriação ilegítima dos dados pessoais de um indivíduo sem o seu conhecimento, para, por exemplo, efetuar pedidos de crédito, compras ou obter acesso a fundos. Como, na generalidade dos casos, os extratos ou faturas geradas por contas fraudulentas são enviadas para moradas diferentes, a vítima pode não se aperceber atempadamente da fraude.

Reduza os riscos e proteja a sua informação pessoal aplicando as seguintes sugestões:

Utilização da Internet em locais públicos

Evite a utilização da Internet em Ciber Cafés, Livrarias e outros locais públicos, por forma a evitar o risco de captação da informação.

Previna-se da fraude online

Tenha em atenção que existem páginas de Internet desenhadas especificamente para captar informação pessoal. Por vezes, os links para essas páginas são transmitidos por E-mail, fazendo-se passar por entidades bancárias ou outras entidades credíveis. Sempre que possível, escreva o endereço da página a que pretende aceder na barra de endereços do browser ou utilize a lista de Favoritos para aceder a páginas de Instituições Financeiras.

O Montepio não envia mensagens automáticas de E-mail aos seus Clientes, onde constem links para páginas do endereço www.montepio.pt.

Desative a opção Auto Complete do browser

Tal ajudará a prevenir a visualização da sua informação por outras pessoas que utilizem o seu computador. Para alterar esta definição no browser Internet Explorer:

Aceda ao menu Tools;

Selecione a opção Internet Options;

Escolha a pasta Content;

Carregue no botão AutoComplete;

Retire as opções selecionadas da área Use AutoComplete For;

Selecione os botões Clear Forms e Clear Passwords para apagar a informação armazenada relativa ao preenchimento de formulários e passwords.

Mantenha os seus códigos seguros

Os códigos (tal como o Código PIN Montepio24 e o Cartão Matriz) são a chave para acesso a informação confidencial, pelo que deverão ser extremamente bem protegidas:

garanta a confidencialidade dos códigos memorizando-os;

os códigos são pessoais e intransmissíveis, não devendo ser divulgados a ninguém;

deverá proceder à alteração dos códigos regularmente;

ao introduzir códigos, certifique-se de que ninguém o estará a visualizar;

tente criar códigos que não sejam facilmente descobertos por terceiros, ao não incluírem informação pessoal (nomes, datas de nascimento, números de telefone, etc);

utilize códigos diferenciados para aceder a serviços distintos;

Garantir a segurança da sessão de utilização do Net24

Na sessão de utilização do Net24 deverá ter cuidados adicionais:

no acesso à Internet deverá, sempre que possível, evitar locais públicos (Ciber Cafés, Aeroportos, Hotéis, etc.);

para aceder a www.montepio.pt, opte por introduzir diretamente o URL na barra de endereços ou utilize a opção dos Favoritos ao invés de aceder através de um link disponibilizado num E-mail ou noutra página de Internet;

No acesso (login) - certifique-se que introduz a combinação Identificação/Código PIN correta e que ninguém observa esses dados;

Na saída (logoff) - selecione sempre a opção Sair do menú do Net24 e feche a janela de browser para garantir que nenhuma informação fica residente na memória do PC.

Nota: alguns dos links mencionados referem-se a páginas Web controladas e geridas por terceiras entidades (não afiliadas do Montepio). Deste modo, o Montepio, não será responsável pelos conteúdos, políticas de privacidade ou segurança dessas páginas.