Sugestões e conselhos

Fomente bons hábitos de segurança em linha com as sugestões e os conselhos que se seguem. Esta secção foi desenvolvida em coordenação com a iniciativa Get Safe Online (Reino Unido) e o Departamento de Segurança Interna dos EUA

- Proteger o computador pessoal (PC) e dispositivos portáteis
- Proteger os dados pessoais e a identidade
- Proteger informações comerciais fora da organização
- Ligações com segurança
- Precauções na Web

Proteger o computador pessoal (PC) e dispositivos portáteis

PC

- Use uma barreira de segurança (*firewall*): as barreiras de segurança protegem a rede de alguns vírus e piratas informáticos.
- Instale *software* antivírus: o *software* antivírus evita que o seu computador seja infetado por vírus.
- Obtenha as atualizações de segurança mais recentes: mantenha as suas aplicações e o sistema operativo em boas condições e devidamente atualizados.
- Trave os programas espiões (*spyware*): não abra mensagens de correio eletrónico e anexos suspeitos para evitar que o seu computador seja invadido por estranhos.
- Faça cópias de segurança regulares: proteja-se de perdas de dados.

Computadores portáteis

- Desligue as ligações sem fios quando não estiverem em uso ou não forem necessárias.
- Ligue regularmente o computador portátil a uma rede fidedigna para atualizar os mecanismos de segurança.
- Faça cópias de segurança da informação armazenada no computador portátil.
- Não deixe o seu computador portátil num local sem vigilância.

Unidades USB

- Use uma unidade USB codificada.
- Coloque a unidade *flash* USB no modo só de leitura através do interruptor para evitar a transmissão de vírus: algumas unidades *flash* USB têm um interruptor que permite colocar a unidade num modo só de leitura, para evitar que o computador anfitrião escreva dados na unidade ou modifique os dados nela existentes.

- Analise a unidade *flash* USB com um programa antivírus depois de copiar ficheiros de um computador não fidedigno ou não autorizado, para evitar a transmissão de vírus.
- Antes de inserir a unidade USB no computador de outra pessoa, apague todos os ficheiros que não sejam pertinentes para esse uso.
- Faça cópias de segurança dos dados existentes na unidade USB, para poder recuperá-los em caso de desastre.
- Use uma corrente ou uma fita para prender a unidade USB e, assim, evitar a perda do suporte de dados: devido às suas dimensões reduzidas, as unidades *flash* USB são fáceis de perder e tornam-se alvos privilegiados de roubo. Além disso, à medida que aumenta a capacidade de armazenamento, também aumenta o volume potencial de dados em risco de acesso não autorizado. As unidades *flash* USB são normalmente transportadas em malas, mochilas, malas de computadores portáteis, casacos, bolsos de calças ou são deixadas em computadores sem vigilância. Tem-se verificado recentemente um aumento do número de incidentes devido à perda, esquecimento, empréstimo não autorizado ou roubo de unidades USB.

Telemóveis, *smartphones* e agendas digitais

Os *smartphones* e agendas digitais, como os dispositivos Windows Mobile, Palm, iPhone, Android e Blackberry, dispõem de ligação à Internet e suportam o armazenamento de grandes volumes de informação. É precisamente por serem ultraportáteis que devem ser tratados com cuidados redobrados.

- Desligue as ligações sem fios (ou seja, Bluetooth e WLAN) quando não estiverem a ser usadas. A tecnologia Bluetooth permite a comunicação entre dispositivos eletrónicos através de uma ligação via rádio de curto alcance.
- Não deixe o seu telemóvel, smartphone ou agenda digital num local sem vigilância. Caso contrário, poderá perder dados.
- Use a função de palavra-passe para evitar intrusões remotas no seu smartphone

Proteger os dados pessoais e a identidade

- **Use uma palavra-passe forte**: a palavra-passe é o equivalente à chave e à fechadura da sua casa na Internet. As palavras-passe são uma grande defesa e boas práticas neste domínio ajudam a garantir a segurança de dados pessoais sensíveis e da sua identidade. A palavra-passe do computador é a chave de acesso a toda a informação — empresarial e pessoal — que está armazenada no computador e nas suas contas em linha. Use uma palavra-passe forte para proteger os seus dados: use um conjunto complexo de carateres, combinando letras (maiúsculas e minúsculas), números e símbolos. Quanto mais variados forem os carateres na palavra-passe, mais difícil se torna adivinhá-la. Não use dados pessoais — nome, nome dos filhos, datas de aniversário, etc. — que outras pessoas possam já conhecer ou obter com facilidade, e tente evitar palavras comuns: alguns piratas

informáticos utilizam programas que experimentam todas as palavras existentes no dicionário.

- **Altere a palavra-passe com regularidade**: caso suspeite de violação da integridade do seu sistema, altere imediatamente as palavras-passe.
- **Mantenha a palavra-passe secreta**: a sua palavra-passe é exclusiva e não deve ser partilhada com ninguém. Sempre que possível, tente memorizar as palavras-passe. Desenvolva uma estratégia para as memorizar. Se anotar as palavras-passe, guarde as anotações num local seguro. Não deixe as anotações com as palavras-passe num local onde não deixasse também os dados que as palavras-passe se destinam a proteger.
- **Uma conta, uma palavra-passe**: use palavras-passe diferentes para cada uma das suas contas em serviços na Internet (ou, pelo menos, use várias palavras-passe diferentes). Se usar as mesmas palavras-passe em várias contas, um pirata que tenha acesso a uma conta poderá também aceder a todas as outras.
- **Proteja as suas contas**: muitos fornecedores de contas disponibilizam meios suplementares de verificação da identidade antes de permitirem operações nos respetivos sítios Web.
- **Controle a sua presença em linha**: sempre que estiverem disponíveis, programe as definições de privacidade e segurança nos sítios Web para um nível de partilha de informação com que se sinta confortável. É preferível limitar as pessoas com quem partilha informação.
- **Use as redes sociais com cuidado**: tenha em atenção que as redes sociais podem agregar muitos dos riscos associados à presença em linha, nomeadamente assédio moral através da Internet, divulgação de informação privada, ciberperseguição, acesso a conteúdos inadequados para a idade dos utilizadores e, em casos mais extremos, aliciamento e abuso de menores em linha.

Proteger informações comerciais fora da organização

- **Proteja a segurança das informações sensíveis**: quando não estiver nas instalações da sua organização, mantenha as informações sensíveis e os equipamentos em segurança para evitar a sua perda ou roubo. Seja especialmente cauteloso em locais públicos, onde deve tratar a informação com cuidado.
- **Mantenha a confidencialidade das informações comerciais**: tenha presente que outras pessoas podem escutar as suas conversas. Não divulgue a qualquer pessoa informações confidenciais da sua organização.
- **Cuidado com terceiros à espreita**: quando viajar ou quando estiver a trabalhar a partir de uma localização remota, tenha cuidado com terceiros à espreita.
- **Use o acesso ao correio eletrónico através da Web com cuidado**: usar um navegador da Internet para ler o correio exige a aplicação das mesmas cautelas que a utilização de um programa de correio eletrónico e tem mesmo alguns riscos específicos.

Ligações com segurança

- **Desligue as ligações sem fios quando não estiverem em uso ou não forem necessárias.**
- **Use os pontos de acesso Wi-Fi com inteligência**: quando usar pontos de acesso Wi-Fi, restrinja o tipo de operações que efetua e ajuste as definições de segurança do seu dispositivo, para limitar quem pode ter acesso ao seu equipamento.
- **Proteja o seu dinheiro**: quando efetuar compras ou operações bancárias em linha, confirme que os sítios Web são seguros. Procure endereços Web começados por «https://» ou «shttp://», que são sinónimo de medidas adicionais de segurança no sítio Web para proteger os seus dados pessoais. Os endereços começados por http:// não são seguros.
- **Ponha um travão ao correio eletrónico indesejado**: o correio eletrónico indesejado é uma ameaça de segurança. Não abra mensagens de correio eletrónico e anexos de remetentes desconhecidos.
- **Em caso de dúvida, apague**: quando as hiperligações nas mensagens de correio eletrónico, nos *tweets*, nas publicações ou na publicidade em linha tiverem um ar suspeito, mesmo que conheça a origem, é melhor apagá-los ou, se for o caso, marcá-los como correio eletrónico indesejado.
- **Reencaminhar apenas o conteúdo necessário das mensagens de correio eletrónico**: antes de reencaminhar uma mensagem, verifique se é necessário apagar o histórico da mensagem.
- **Navegue na Internet com cautela.**
- **Não descarregue documentos nem materiais de fontes que não sejam fidedignas.**
- **Use computadores públicos com cuidado:** só deve usar um computador público para ligações à Internet, se este permitir ligações codificadas (indicadas por um cadeado no canto inferior direito da janela do navegador e pelas letras «https://» no início do endereço do sítio Web).
- **Use serviços de acesso ao correio eletrónico através da Web fornecidos por empresas conhecidas e fidedignas.**

Precauções na Web

- **Mantenha-se atualizado:** mantenha-se informado das novas formas de garantir a sua segurança em linha. Consulte as informações mais recentes em sítios Web fidedignos e partilhe-as com a família, amigos e colegas: incentive-os a aplicar precauções na Web. Reforce a segurança do seu navegador.
- **Pense antes de passar à ação**: tenha cuidado com as comunicações que sugerem uma ação imediata, que fazem ofertas demasiado boas para serem verdade ou que solicitam dados pessoais.
- **Faça cópias de segurança**: faça cópias eletrónicas para proteger o seu trabalho, música, fotografias e outras informações em formato digital, e guarde as cópias num local seguro.