



Proteger o seu computador quando navega na internet

1. Proteção Pessoal

Nas redes sociais

As redes sociais permitem-lhe estar mais próximo de familiares, amigos e pessoas com interesses comuns. Para usufruir destas redes em segurança, tenha em atenção os seguintes pontos:

Informações pessoais e perseguições

- Cuidado com as informações pessoais que transmite online.
- Não partilhe contactos telefónicos nem locais onde está ou vai estar.

Encontros com desconhecidos

Se combinar um encontro com alguém que não conhece pessoalmente, faça-o em sítios públicos.

Utilização abusiva de informação ou roubo de identidade

- Tenha o seu perfil privado, visível apenas para a sua lista de amigos e familiares.
- Não aceite pedidos de amizade de perfis suspeitos
- Não publique fotografias que revelem os sítios que frequenta
- Não divulgue informações sobre outras pessoas
- Se receber comentários ou mensagens ofensivas, alerte os administradores da rede social.

Violação de privacidade

Leia sempre a política de privacidade da rede social que usar, para garantir que os seus dados não vão ser transmitidos ou vendidos a outras empresas.

Partilha de conteúdos

- Lembre-se que os conteúdos que publicar podem ser usados noutros contextos sem a sua autorização.
- Não publique fotografias ou vídeos que o possam prejudicar no presente ou no futuro.
- Tenha em atenção que mesmo que apague o seu perfil, registo ou conteúdos, algumas informações podem já ter sido copiadas e disponibilizadas por outros utilizadores.

Direito de autor, direito de imagem e privacidade

Os perfis que criar e as informações que publicar vão ficar disponíveis online. É da sua responsabilidade o cumprimento das leis em vigor sobre privacidade, direito de imagem e autoria.

Em conversas online

Falar online tem a vantagem de juntar pessoas que estão longe umas das outras, ou que não poderiam encontrar-se de outra forma. No entanto, há que ter alguns cuidados quando se usam os serviços de chat e de mensagens instantâneas.

Fraude

Não divulgue informações a quem não conhece pessoalmente. Podem tentar roubar o seu dinheiro ou identidade e causar-lhe danos emocionais ou físicos.

Outros crimes e ofensas

Tenha atenção aos temas explorados nas salas de chat. Utilize salas de chat com moderador e nunca divulgue informação pessoal.

Vírus e antivírus

- Não abra ficheiros nem visite sites enviados por desconhecidos, ou mesmo por amigos ou familiares, se desconfiar dos conteúdos – nestes casos, avise o familiar ou amigo que poderá ter enviado um vírus.
- Tenha a firewall do Windows ativa (também pode usar uma firewall de outra marca). A firewall funciona como uma barreira que protege o seu computador contra invasões de privacidade e garante a confidencialidade das suas informações.

No email

Ao permitir enviar mensagens pela internet, o email revolucionou a forma como comunicamos no trabalho, com amigos e familiares. Para que esta forma de comunicação não lhe traga problemas, tome algumas medidas de precaução.

Envio e receção de mensagens não solicitadas (spam)

- Mantenha o antivírus sempre atualizado e ativo para examinar os emails e anexos que lhe forem enviados.
- Assinale as mensagens indesejadas como spam. Tornará o seu filtro de email mais eficaz.
- Desconfie das mensagens que dizem que ganhou prémios.

Informações pessoais ou financeiras

Não as envie por email, pois não é um meio de comunicação totalmente seguro.

Filtros

Utilize no seu email blacklists e whitelists. As blacklists eliminam mensagens que tem determinado assunto ou que são enviadas de emails específicos. As whitelists permitem receber emails de quem definir como autorizado.

Emails ou sites com oferta de programas milagrosos

Desconfie de emails ou sites com oferta de programas milagrosos que dizem aumentar a velocidade de computador ou da internet, melhorar a performance do computador ou ter detetado um vírus no computador que prometem resolver se instalar um executável (ficheiro com terminação .exe).

Em compras e bancos online

Fazer compras ou consultar e movimentar a conta bancária na internet são hábitos cada vez mais comuns e banais. Faça-o em segurança.

Sites de compras

Use apenas páginas de venda reconhecidas. Se tem dúvidas, pesquise na internet a reputação da página em questão.

Sites de bancos

- Evite aceder à sua conta bancária em computadores públicos
- Siga todas as normas de segurança recomendadas pelo banco
- Phishing – Phishing é quando alguém se faz passar pelo seu banco ou por outra instituição para ficar com os seus dados para os utilizar e se fazer passar por si
- Cuidado com sites fraudulentos que se fazem passar por empresas credíveis – como bancos, fornecedores de telecomunicações ou governo
- Ignore emails que lhe peçam informação pessoal ou financeira. As empresas não pedem esse tipo de informação por email
- Controle os extratos do seu cartão de crédito e contas bancárias para verificar se existem movimentos que não tenham sido autorizados por si.

Com as passwords

Para sua segurança, em muitos serviços disponíveis na internet – email, banco online, sites de compras, entre outros – é preciso definir uma password de acesso.

Há que ter alguns cuidados na manutenção destes códigos pessoais.

Criação e alteração da password

1. Uma ideia simples para criar uma password segura e simples de memorizar:
2. Pense numa frase que tenha significado para si (por exemplo: “Ser ou não ser, eis a questão.”)
3. Escolha as iniciais de cada palavra e fica com “Sons,eq”
4. Substitua uma das letras por um número que seja semelhante (o S é semelhante ao 5)
5. A password final vai ser “5on5,eq”

Não escolha sequências simples ou óbvias (por exemplo, “aaaa” ou “123456”)

Não crie uma password igual ao nome de utilizador, ao email, ao seu nome, à sua data de nascimento, clube ou cor preferida

Aumente a segurança da password

- acrescentando o número de caracteres (8 caracteres é razoável)
- usando letras minúsculas, maiúsculas, números e símbolos (por exemplo, Taurus=2)

Mude a sua password, no mínimo, de 2 em 2 meses.

Confidencialidade e memorização da password

- Nunca a dê a outras pessoas
- Nunca a escreva em papéis
- Nunca a guarde em ficheiros (por exemplo, documentos Word)
- Nunca a memorize no telemóvel
- Não deixe que os sites a memorizem – só assim garante que quem acede ao computador não vê ou não usa as suas informações
- Faça sempre logout (por exemplo, no botão sair) – para impedir que quem visita o mesmo site no mesmo computador veja ou use as suas informações.

Como posso alterar a minha password de acesso à internet fixa?

1. Aceda à sua Área de cliente
2. Escolha o produto Internet no menu do lado esquerdo
3. Clique em **Serviços** na barra superior
4. Escolha **Internet Sem Fios em Casa**
5. Clique em **Alterar a Password**
6. Escreva uma nova password, confirme e clique em **Alterar**.

Em downloads

Antes de abrir um ficheiro descarregado da internet, analise-o com o antivírus.

2. Proteja o seu computador

Mantenha um programa antivírus sempre atualizado.

Para navegar na internet MEO de forma segura, proteja o seu computador dos vírus mais recentes. Opte por atualizações automáticas do seu antivírus, de forma a garantir uma proteção máxima.

Para além do antivírus, também é importante atualizar o sistema operativo, os navegadores de sites (browsers) e todos os programas que utiliza. É frequente serem descobertas falhas de segurança dos programas e as atualizações resolvem esses problemas.

Os programas anti-spyware (disponíveis na internet) ajudam a encontrar ficheiros e programas potencialmente perigosos que podem estar escondidos no seu computador.

Preste atenção a sinais estranhos

Quando o computador está a ser atacado, o sistema operativo pode comportar-se de maneira diferente (por exemplo, ficar mais lento).

Faça cópias de segurança

É importante ter uma cópia de segurança dos seus ficheiros e dados. Use um disco externo ou um serviço de dados na nuvem (serviço em que armazena os seus ficheiros numa pasta da internet, acessível a partir de qualquer ponto do mundo, desde que tenha acesso à internet) para fazer cópias de segurança. Deste modo, caso o computador tenha de ser formatado, não perde nada.

3. Proteja a sua família

A internet é uma mais-valia na educação dos jovens. No entanto, pela sua inexperiência, as crianças e os adolescentes nem sempre se apercebem de alguns perigos.

- Converse com os seus filhos. Evite o isolamento e o segredo, caso passem por algum tipo de abuso ou violência online
- Coloque os computadores com acesso à internet em salas comuns da casa. Pode limitar a privacidade dos seus filhos, mas permite-lhe estar mais atento aos conteúdos a que acedem e às atividades que fazem online
- Informe os seus filhos sobre os perigos associados à partilha de informações pessoais (localizações, rotinas diárias, fotografias da casa, datas e locais de férias, etc.). Alerta-os para os riscos de conversar com estranhos e combinar encontros
- Ative o controlo parental. O controlo parental permite-lhe bloquear o acesso a determinado tipo de informação e conteúdos. Garante aos seus filhos uma experiência segura e positiva na internet.

4. Ajuda e proteção legal

Pode utilizar diversos meios para apresentar queixa e pedir ajuda. Se for vítima em blogs, emails ou redes sociais do MEO ou do SAPO, contacte o SAPO através do email abuse@sapo.pt ou do [formulário Suporte SAPO](#).

Se for vítima em sites ou serviços online que não sejam do MEO ou do SAPO contacte a [Linha Internet Segura](#).

Se for vítima de roubo de identidade, violência pessoal ou outro tipo de abuso grave, pode fazer queixa à Polícia Judiciária, que tem autoridade para investigar crimes relacionados com utilizações abusivas de redes informáticas.

Nesses casos, contacte:

Direção Central de Investigação da Corrupção e Criminalidade Económica e Financeira
Rua Alexandre Herculano, 42-A – 1250-011 Lisboa
Telefone (geral) – 218 643 900
Telefone (piquete) – 213 574 560
Email: dciccef@pj.pt
Fax: 213 160 131

5. Proteção de direitos de autor

Para lhe podermos dar o melhor, temos de garantir que o melhor continua a existir. Sabemos que gosta de conteúdos de entretenimento – como filmes e séries – de alta qualidade e esforçamo-nos diariamente para garantir a sua total satisfação. Para que possamos continuar a prestar um serviço de excelência, trabalhamos em conjunto com empresas que criam os melhores conteúdos e tecnologias.

Ao proteger os direitos de autor, estamos a proteger os nossos clientes

Ao ajudarmos a proteger os direitos de autor, estamos a garantir que os nossos clientes podem continuar a usufruir dos melhores programas de TV, filmes e músicas. Por isso, é nosso dever ajudar a garantir, em conjunto com as autoridades, a defesa dos direitos de autor dos proprietários dos conteúdos que levamos até si.

Como ajudamos na proteção dos direitos de autor?

Nos últimos anos, muitos proprietários de conteúdos têm recorrido aos tribunais para se defenderem contra o uso ilegal das suas obras.

Quando isso acontece e o tribunal concorda que os direitos de autor estão a ser violados, o proprietário pode pedir que o fornecedor do serviço de internet (ISP) bloqueie o acesso a determinados sites de partilha ilegal de conteúdos.

Sendo um ISP, o MEO tem a obrigação legal de bloquear sites que um tribunal ordene.

6. Serviços MEO para ajudar a garantir a segurança

Oferecemos-lhe serviços para que aproveite o melhor da Internet, minimizando os perigos.

Temos, para si:

- O Antivírus Panda – antivírus para clientes de Internet fixa
- A Linha Sou Smart – ajuda para configuração de programas, remoção de vírus ou correção de erros no sistema operativo – exclusivo para clientes de Internet fixa).

7. Recomendações MEO

Para saber mais sobre segurança na internet, consulte os sites ou veja os vídeos que lhe recomendamos.

Sites recomendados

- seguranca.sapo.pt
- www.cert.pt
- www.internetsegura.pt
- antivirus.sapo.pt
- linhaalerta.internetsegura.pt

Vídeos recomendados

Sobre segurança na internet

- [Segurança na Internet](#)
- [PJ dá lição sobre cibercrime](#)

Phishing

- [Phishing](#)
- [Fraude bancária na Internet](#)

Vírus

- [Vírus informáticos](#)
- [Vírus Sobig à solta](#)
- [Vírus informático no Ministério da Justiça](#)

Spam

- ["Spam" faz 30 anos](#)
- [Falsa mensagem da PSP com convocatória judicial](#)
- [Saiba como os spammers ganham dinheiro](#)

Controlo parental

- [Sabe onde está o seu filho?](#)
- [Riscos para os mais novos](#)
- [Crianças chantageadas na internet](#)
- [Operação da PJ sobre pedofilia na Internet](#)

Violação de direitos de autor

- [Fechados sites de partilha de ficheiros](#)

8. Glossário

Se phishing e malware lhe soam estranho, ou se pensa que cookies são bolachas, o nosso glossário foi feito para si.

Atualizações de segurança / Patches – Atualizações para o software ou para o sistema operativo, desenvolvidas para corrigir falhas de segurança.

Antispam – Programa que se instala no computador para evitar a receção de spam (emails não solicitados).

Antispyware – Programa que se instala no computador para o proteger contra software de spyware.

Antivírus – Programa que se instala no computador para o proteger contra programas maliciosos, que podem provocar danos (por exemplo, perda de ficheiros). Esses programas maliciosos são conhecidos como vírus, cavalos de Tróia ou malware e afetam a segurança. Podem permitir o acesso ou a transmissão de informações pessoais que estão guardadas no computador.

Browser – Programa que permite pesquisar e ver os sites alojados em servidores na internet.

Cavalo de Tróia (Trojan horse) – Programa que aparenta ser útil, mas que permite que alguém não autorizado controle o computador, a partir do exterior.

Este programa pode ser instalado pelo dono do computador (por engano) ou pode instalar-se sozinho (a partir de um outro programa).

Apesar de comprometer a segurança, não contagia outros computadores, como acontece com um vírus.

Cookies – Pequeno ficheiro de informação que um site deixa no computador e que consulta quando se torna a visitá-lo. A sua função é memorizar as preferências do visitante ou outras informações.

As cookies não são uma invasão da privacidade, apenas ajudam a personalizar a consulta de um site.

A maior parte dos navegadores de sites (browsers) aceitam cookies automaticamente, função que pode ser desativada pelo utilizador. No entanto, sem as cookies alguns sites não funcionam corretamente.

Cyberbullying – Bullying é o termo para descrever uma perseguição ou discriminação que geralmente ocorre entre crianças mais velhas ou mais fortes contra crianças mais novas ou fracas. O cyberbullying é quando essa perseguição acontece online.

Download – Processo de descarregar um ficheiro da internet para o computador.

Encriptação – Método de codificação de dados que são transmitidos através de redes públicas (como a internet). Esta codificação faz-se através de fórmulas matemáticas (os chamados algoritmos).

Para ler os dados, é necessário ter o algoritmo de descodificação.

Extensões de ficheiros escondidas – O sistema operativo Windows tem a função de esconder a extensão de tipos de ficheiros conhecidos. Esta função vem ativada de origem, mas pode ser desligada pelos utilizadores.

Muitos dos vírus que se difundem por email tiram partido desta "função", enviando em anexo ficheiros que parecem ser de um tipo inofensivo, mas que na realidade são programas maliciosos. A verdadeira extensão fica escondida e o utilizador pensa que está a abrir um ficheiro de imagem (JPG), de vídeo (MPG) ou de texto (TXT):

- VBS/LoveLetter (nome do ficheiro: LOVE-LETTER-FORYOU.TXT.vbs);
- Downloader (nome do ficheiro: MySis.avi.exe ou QuickFlick.mpg.exe);
- VBS/Timofonica (nome do ficheiro: TIMOFONICA.TXT.vbs);
- VBS/CoolNote (nome do ficheiro: COOL_NOTEPAD_DEMO.TXT.vbs);
- VBS/OnTheFly (nome do ficheiro: AnnaKournikova.jpg.vbs)

Engenharia social – Significa um meio para obter, de forma ilegal, informações importantes e sigilosas. Acontece através de ações que enganam ou exploram a confiança dos utilizadores, que recebem mensagens falsas em nome de empresas ou organizações (por exemplo, um email falso do banco) a pedir dados confidenciais. Normalmente, estas mensagens falsas alertam para consequências negativas caso o utilizador não envie os dados.

Endereço de IP – Quando os computadores se ligam à internet, estão a comunicar com outros computadores, onde estão alojados os sites ou os ficheiros que se querem consultar.

Cada computador que está ligado à internet tem um número de identificação, chamado endereço de IP. Esses endereços são compostos por quatro grupos de números separados por pontos (por exemplo, 193.136.0.1).

Quando os computadores querem contactar entre si, através da internet, consultam o DNS (Domain Name System), um diretório onde estão identificados os números de cada computador. Isto significa que ao endereço de um site corresponde um endereço de IP (por exemplo, www.cert.pt corresponde a 193.136.2.194). No entanto, estes endereços podem mudar ao longo do tempo.

Existem dois tipos de endereços IP:

- Os públicos ou globais, para os quais a rede conhece o caminho;
- Os privados, de redes locais, para os quais a rede não dá um caminho direto.

O sistema que permite traduzir um IP privado para público, permitindo aos computadores aceder à internet, chama-se de NAT (Network Address Translation).

Firewall – Programa que se instala no computador para o proteger contra acessos não autorizados. Estes acessos a partir do exterior podem ser feitos por indivíduos (hackers) ou vírus.

Alguns sistemas operativos (como o Windows XP ou o Windows Vista) têm uma firewall incluída. Nos casos em que o sistema operativo não tem esta função integrada, aconselha-se a instalação de um programa de firewall.

Hacker – Nome que se dá a alguém que tenta entrar, de forma ilegal, num computador ou noutros sistemas informáticos. Normalmente, estes indivíduos são programadores experientes e têm conhecimentos técnicos muito avançados, o que lhes permite aproveitar pontos fracos da segurança dos sistemas informáticos.

ISP – Iniciais de Internet Service Provider; fornecedor de ligação à internet (por exemplo, o MEO). O serviço pode ser feito através de uma linha telefónica ou de outro meio (por exemplo, um equipamento de Internet Móvel) que permita ligar o computador do cliente à internet. Normalmente, são fornecidos aos clientes um software, um nome de utilizador, uma password e um número de acesso telefónico.

Malware – Termo que vem de software malicioso (malicious software). É um programa que se infiltra no computador, de forma ilícita. Pode causar danos (por exemplo, perda de ficheiros) ou transmitir informações pessoais que estão guardadas no computador.

Phishing – Ação em que alguém se faz passar por um banco, ou por outra instituição, para ficar com os dados dos clientes e depois utilizá-los de forma ilícita. Normalmente, acontece através de um email que solicita dados confidenciais em sites falsos (por exemplo, uma cópia do site do banco).

Spam – Envio em massa de emails não solicitados por quem os recebe. Pode ter como objetivo a propagação de um vírus para recolha de contactos ou de ficheiros alojados no computador.

Spyware – Programa que recolhe ilicitamente informações pessoais sobre os utilizadores ou altera as configurações do computador. Normalmente, é utilizado para fins publicitários ilegais.

Software – Programa utilizado para executar determinada tarefa (por exemplo, o Word permite editar documentos de texto).

Upload – Processo de enviar um ficheiro do computador para a internet.

Vírus – Programa que se instala no computador e que pode provocar danos (por exemplo, perda de ficheiros). Estes programas afetam a segurança, podendo permitir o acesso ou a transmissão de informações pessoais que estão guardadas no computador. Os vírus possuem a capacidade de se multiplicar, infetando computadores ligados em rede (através de uma ligação de rede privada ou através da internet). A sua propagação é feita através de ficheiros (por exemplo, enviados como anexo de um email) e podem ter rotinas específicas (por exemplo, ativar-se em determinada data ou após determinada ação do utilizador).