No MEO SPGS, SA, preocupamo-nos em garantir a segurança das transações online e a proteger os dados pessoais dos nossos clientes. Para salvaguardar essa segurança, é também importante que adote regras básicas enquanto comunica, partilha e explora a internet.

Clique numa das opções e veja as nossas recomendações.

Proteja-se e ao seu computador

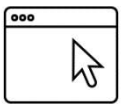
Garanta a segurança das suas contas, transações online e dados pessoais. Conheça as melhores de práticas de segurança pessoal.

Saiba mais »

E-mails e telemóvel

Saiba identificar comportamentos estranhos no seu telemóvel e mantenha-se atento a mensagens de email de desconhecidos ou com anexos.

Saiba mais »



Navegue em segurança

Sabe quais os cuidados a ter quando acede a um site na internet ?

Saiba mais »

O que é o phishing?

É uma tentativa de fraude que leva o utilizador a crer que está a interagir com um site fiável, enquanto lhe roubam dados sensíveis.

Saiba mais »

Proteja-se e ao seu computador

Proteja-se

O MEO SPGS, SA preocupa-se em garantir a segurança das transações online e proteger os dados pessoais dos seus clientes. Para salvaguardar essa segurança é também importante que cada cliente do MEO respeite, permanentemente, **práticas de segurança pessoal**:

- Mantenha sempre os seus códigos de acesso reservados, não os divulgue a terceiros;
- Evite aceder a um computador público ou partilhado com pessoas desconhecidas quando tiver que utilizar os seus dados pessoais, de forma a minimizar a possibilidade;
- Se tiver de realizar operações a partir de um computador partilhado por vários utilizadores, ou no qual não tenha plena confiança, recomendamos que antecipadamente ative a “Segurança Adicional - Acesso Controlado”, para que as operações necessitem de validação, através de códigos de ativação recebidos por SMS;
- Se utiliza Certificados Digitais, certifique-se de que o seu computador não é utilizado por terceiros ou pessoas nas quais não tenha plena confiança;
- Verifique as transações nas suas contas regularmente;
- Sempre que entrar numa nova sessão na Internet (“login”) memorize ou guarde a data/hora de início da mesma. Na sessão seguinte, verifique se a data/hora do último login coincide com a informação de que dispõe;
- Evite utilizar login automático. Para sua segurança, é preferível inserir os dados de acesso em cada autenticação;
- Memorize os seus dados de acesso e nunca os anote em papéis. Se desconfiar que alguém descobriu o seu código de acesso, substitua-o imediatamente;
- Escolha códigos de acesso fáceis de decorar mas difíceis de adivinhar. Evite usar os mesmos códigos de acesso para diferentes situações;
- Certifique-se de que, cada vez que termina a sessão na Internet (“logout”), clica no botão 'Sair';
- Altere periodicamente o seu código de acesso. Não utilize códigos que possam ser fáceis de descobrir (ex: datas de aniversário, telefones, nomes da família, etc.). Nem devem seguir padrões de teclado (ex: “qwerty…”, “123456…”);
- Não faculte, em caso algum, por telefone, correio eletrónico ou por outro meio de comunicação à distância, qualquer informação reservada;

- Guarde em local seguro os cartões com os códigos de segurança, o envelope com a password de acesso ao serviço de acesso à Internet, as faturas e outros documentos que contenham informação confidencial, uma vez que com base nessa informação terceiros não autorizados podem aceder aos seus dados pessoais e demais informação confidencial;
- Para se certificar de que está nos sites oficiais do MEO, confirme se, na barra de endereço de IP, surgem as letras do endereço do MEO.

Proteja o seu PC

Entre os principais inimigos de segurança na Internet, encontram-se os vírus de computador. Os vírus são programas que se instalam no disco e podem causar vários problemas. Por exemplo pode perder toda a informação do disco rígido ou ser espiado sem se aperceber, as suas informações confidenciais podem ser capturadas, armazenadas ou enviadas para o exterior.

Deixamos aqui **algumas recomendações de segurança**, para prevenir ataques inesperados:

- Utilize um antivírus para prevenir acessos indesejados ao seu computador e mantenha-o atualizado contra os últimos vírus. Recomendamos que visite regularmente os sites das empresas que são responsáveis pelo licenciamento do seu antivírus com o objetivo de instalar todas as atualizações disponíveis regularmente;
- Mantenha o seu sistema operativo (ex: Windows) e o browser (ex: Internet Explorer) com a versão mais recente. Por vezes são descobertas algumas vulnerabilidades nestes produtos e são disponibilizadas atualizações para corrigir essas lacunas. Recomendamos que visite regularmente os sites das empresas que são responsáveis pelo licenciamento do software/programa associado ao seu sistema operativo e o browser com o objetivo de instalar todas as atualizações disponíveis regularmente;
- Se desconfia que o seu computador possa estar com um vírus ou se quer saber se um software/programa ou arquivo que recebeu anexado a um e-mail não tem vírus, deve fazer um scan ao local/ ficheiro em questão.

Esteja atento ao seu e-mail e telemóvel

Quando aceder ao seu e-mail ou utilizar o seu telemóvel, deve considerar as seguintes recomendações:

- Evite abrir arquivos ou programas anexados em mensagens de e-mail sem primeiro os verificar com um antivírus atualizado, mesmo que a mensagem seja de uma pessoa da sua confiança. Essas mensagens são muitas vezes utilizadas para propagar vírus;
- Evite abrir e-mails de origem desconhecida e adote uma postura conservadora mesmo com e-mails que pareçam escritos e enviados por conhecidos;
- Se tiver dúvidas relativamente a um pedido recebido por e-mail, SMS, MMS ou mensagem instantânea, contacte a entidade originária dessa mensagem;
- Se receber um e-mail, SMS ou MMS, com a informação de que ganhou um prémio, deverá questionar a credibilidade do mesmo;
- Deve desconfiar dos e-mails redigidos noutros idiomas, com erros de digitação ou de ortografia, de remetentes desconhecidos ou forjados no campo “De:”, ou em que no subject/assunto contenham assuntos que não são habituais;
- Deve também desconfiar das mensagens repetidas;
- Desative a opção "Painel de Pré-visualização" (ou "Preview Pane") do seu correio eletrónico para evitar que uma mensagem com vírus (geralmente em HTML) seja processada automaticamente. Se desejar manter essa opção ativada, aconselhamos a que, no correio eletrónico, defina a receção de todas as mensagens em formato de texto;
- Antes de subscrever um serviço de valor acrescentado (SVA), leia atentamente as condições de subscrição do mesmo. Por vezes a adesão a estes serviços apresentase mascarada através de e-mails de inquéritos, aparentemente inofensivos;
- Desconfie sempre que tiver chamadas não atendidas de números desconhecidos ou que considere suspeitos, nomeadamente internacionais. Se tiver dúvidas, não ligue de volta.

Se receber um e-mail / SMS / MMS do MEO ou de outra entidade a solicitar a introdução dos seus dados de acesso à Área de Cliente ou dados pessoais (ou mesmo se receber um e-mail com um link para uma página onde depois deve inserir os seus dados pessoais), **não** se trata de um e-mail do MEO. **O MEO nunca lhe solicitará que introduza os seus dados por e-mail - estes e-mails são concebidos e enviados por criminosos para tentar obter os seus dados pessoais**. Se tiver dúvidas sobre a autenticidade de algum e-mail que receba de um remetente do MEO, **contactenos imediatamente**.

Esteja atento ao seu telemóvel

O que devo fazer para reduzir o risco de o meu telemóvel ser infetado por vírus?

- Evite instalar aplicações no seu telemóvel, a menos que confie na origem das mesmas;
- Não ignore ou cancele os alertas de segurança indicados pelo seu telemóvel;
- Se estiver particularmente receoso, existem disponíveis no mercado programas de antivírus que podem ser descarregados pela Internet para um computador (e depois transferidos para o telemóvel) ou diretamente para o telemóvel, e que permitem fazer a "limpeza" do vírus do equipamento. A utilização destas soluções é da responsabilidade das empresas que as disponibilizam, não existindo nenhuma relação de parceria entre estas empresas e o MEO.

Como posso remover um vírus do meu telemóvel?

- No caso de o seu equipamento estar infetado com um vírus, a solução pode passar por colocar o telemóvel em reparação (onde será feita uma atualização do software);
- Os sintomas mais comuns são: a bateria descarrega muito depressa, a sincronização de dados não funciona, desliga-se frequentemente, faz chamadas ou envia mensagens não desejadas.

Que cuidados devo tomar em relação ao Bluetooth?

O Bluetooth é uma tecnologia de conexão sem fios que funciona por ondas de rádio de curto alcance. Exemplos do uso do Bluetooth são a ligação a auriculares, Carkits, sincronização com computadores ou PDA. Desta forma, aconselhamos as seguintes medidas de prevenção na utilização do Bluetooth:

- Ligue o Bluetooth apenas quando necessário;
- Escolha o modo "hidden" ou "oculto" por defeito, nas configurações Bluetooth e utilize o modo "show to all" ou "visível" apenas quando necessário;
- Não devem ser aceites mensagens/conteúdos desconhecidos ou inesperados, mesmo que origem seja conhecida, pois poderá tratar-se de um envio provocado por um vírus que reside no telemóvel originador;
- Verifique sempre que o envio é intencional, antes de aceitar o conteúdo. Não instale aplicações desconhecidas ou de fontes não conhecidas, a menos que tenha conhecimento claro da aplicação em causa e conheça a sua proveniência.

Navegue em segurança

Existem certos cuidados a ter quando acede a um site na internet. Aqui, registamos alguns pontos-chave que deve ter em atenção:

- Certifique-se da autenticidade dos sites visitados na internet. Endereços falsos podem capturar os dados inseridos/registados;
- Evite aceder a sites que requerem dados sensíveis (como lojas online, sites bancários, etc.) através de links e opte por digitar o endereço dos mesmos (http://www.exemplo.pt) diretamente na barra de endereços do seu browser;
- Quando o computador não estiver a ser usado, feche o browser ou faça “shut down”;
- Evite usar computadores públicos para realizar qualquer tipo de operação/transação. Podem ter os programas antivírus desatualizados e assim permitir a captura de informações confidenciais suas ou dos seus dados pessoais;
- Sempre que estiver a fazer transações num site seguro, deverão aparecer as letras “https” antes do endereço. Desconfie dos sites que não apresentam o “s” a seguir ao “http”;
- Instale uma firewall para obter um nível adicional de segurança entre a internet e o seu computador. Este software protegerá o computador contra acessos remotos não autorizados.

Phishing: saiba do que se trata

Phishing é um fenómeno de fraude eletrónica. Consiste essencialmente numa tentativa de imitar o conteúdo de um site (pode chegar até si na simples forma de um pop-up ou e-mail) levando o destinatário a acreditar estar a interagir com uma determinada entidade de confiança. Estas ações têm como objetivo obter alguma mais-valia (dados pessoais, números de conta, códigos de acesso, etc.) ou denegrir a imagem dessa entidade. Com os dados assim obtidos podem ser realizadas transferências ou outras operações em nome dos utilizadores que não se apercebem que estão a fornecer os dados a criminosos.

Para sua própria proteção, deve seguir os seguintes procedimentos:

- Valide as fontes e conteúdos: por muito autêntica que a mensagem pareça ser (pode ter símbolos oficiais, ter boa apresentação, dizer que vem de um endereço legítimo, etc…) desconfie sempre e confirme a autenticidade dos conteúdos por outra via que não a internet;

  Saiba detetar mensagens de phishing: os seguintes critérios podem ajudar a identificar possíveis mensagens de fraude (mas não é certo que identifiquem todos):

- Pede informação pessoal (como passwords, números de identidade, telefones, etc…);
- Pedem urgência na resposta ao e-mail para pressionar a sua resposta. Um utilizador sob pressão responde mais facilmente a este tipo de comunicações. São usadas frases como “Urgente”, “A usa conta será cancelada”, “Última oportunidade até hoje às xx:xx horas”, etc…;
- Alguns têm erros de escrita e normalmente é quase certo ser um e-mail falsificado por não nativos de Portugal
- Cumprimentos genéricos como “Caro cliente” no início da comunicação.
- Evite seguir links desconhecidos em e-mails suspeitos: Não prima links como 'Veja Aqui' ou qualquer email;
- Suspeito lhe sugira clicar num link, evitando assim entrar em sites suspeitos;
- Denuncie situações de phishing: colabore com o CSIRT MEO, criando uma nova mensagem de e-mail para csirt@meo.pt e dentro da mensagem anexar o e-mail de phishing original. Envie sempre para este endereço os conteúdos que considere fraudulentos para posterior análise;
- Apague a mensagem: após denunciar situações de fraude, apague a mensagem de phishing da sua mailbox;
- Escreva manualmente no browser o endereço que pretende visitar.

Ao reportar estes casos pode ajudar a reduzir o número de fraudes online.
Para mais informações consulte: http://www.antiphishing.org/.