

Segurança Online

A Segurança Online é um dos temas com os quais todos nos deveremos preocupar diariamente. Não se trata apenas de uma questão de proteção a nível financeiro, mas também de salvaguarda dos dados e privacidade. O Banco Montepio possui plataformas que garantem a proteção do património dos seus Clientes e que asseguram a confidencialidade dos seus dados.

No entanto, as precauções também deverão ser asseguradas do lado dos Clientes através da adoção de alguns cuidados, para evitar facilitar a vida a quem procura aceder aos seus dados bancários.

No vídeo difundido pela Associação Portuguesa de Bancos poderá compreender um pouco mais sobre o tema: [Segurança Online - Saber mais para se proteger melhor](#)

Como poderão aceder aos meus dados e como posso proteger-me?

Os ataques informáticos efetuados diretamente sobre os Clientes baseiam-se em táticas cada vez mais sofisticadas e difíceis de detetar. Saber identificar os tipos de fraude que existem online é, por isso, um passo fundamental para estar mais protegido. Conheça os #Cyberscams mais comuns, numa iniciativa promovida pela Europol e pela Federação Bancária Europeia (EBF), que conta com o apoio da Associação Portuguesa de Bancos.

Clique sobre as imagens para aceder com maior detalhe à informação:



Consulte também o guia '[Banca e Internet - Prevenção](#)', elaborado pela Associação Portuguesa de Bancos (APB), e fique a conhecer algumas das regras para uma utilização segura da Internet.

Para além das dicas acima, conheça as nossas dicas de segurança online, para um serviço de homebanking mais seguro:

- Nunca facultar a terceiros dados pessoais e identificativos, como os seus códigos ou outra informação que permita o acesso às suas contas bancárias online;
- Ter sempre instalado no seu computador um programa de antivírus devidamente atualizado;
- Ter uma firewall instalada também no seu computador, permitindo-lhe filtrar o tráfego de entrada e saída;

Montepio Investimento, S.A.

Sede Social: Avenida de Berna, 10, 1050 – 040 Lisboa | Capital Social: €180.000.000,00

Matrícula e NIPC 505 087 286 | CRC Porto

- Atualizar com frequência o software instalado no seu computador como, por exemplo, sistema operativo e browser de acesso à Internet;
- Ter sempre presente que os Bancos NUNCA solicitam informações pessoais e/ou confidenciais através de mensagens de correio eletrónico ou SMS, pelo que perante qualquer solicitação neste âmbito, contacte os nossos serviços. Estamos sempre disponíveis!
- Verificar se o ambiente seguro no acesso ao site está sempre associado a um endereço que começa por <https://>, com certificado válido e seguro "Caixa Económica Montepio Geral, Caixa Económica Bancária, S.A. [PT]" e se a página possui um cadeado na barra inferior ou superior do seu browser;
- Alertas adicionais:
 - Não introduzir Número de Telemóvel, Código PIN e as coordenadas do Cartão Matriz de forma conjunta;
 - Não introduzir as coordenadas na sua totalidade;
 - Não introduzir os relacionados com o seu Cartão de Crédito (N^o de Cartão, CVV, Nome do Titular);
 - Em situações de revogação dos Códigos de Acesso, a reativação do Serviço deverá ser sempre efetuada através do Phone24 (707 20 20 24 / +351 217 241 624);
 - O BEM nunca envia mensagens automáticas (por contacto telefónico, emails ou SMSs) aos seus clientes solicitando dados de segurança ou informações confidenciais.

Reveja ainda as situações de risco e quais as principais regras de segurança que deve adotar na utilização do seu computador, telemóvel, tablet, no acesso à internet e canais de Homebanking.

Cuidados com mensagens de correio electrónico, SMSs e outras formas de contacto:

- Suspeite de qualquer e-mail, chamada telefónica ou SMS, que peça uma "ação imediata" ou crie um sentido de urgência ou risco grave. Em caso de dúvida contacte o seu banco;
- Suspeite de e-mails supostamente do seu Banco mas que inicia o seu texto com cumprimentos como "Querido Cliente" ou qualquer outra saudação diferente das que o seu banco habitualmente utiliza nas suas comunicações;
- Suspeite dos erros gramaticais ou de escrita nas mensagens que recebe através de qualquer canal habitual de comunicação;
- Posicione o cursor do rato sobre links de mensagens de email suspeitas. Isso mostrará o verdadeiro endereço para onde será direcionado se o selecionar. Se o destino do link for diferente do escrito na mensagem ou contenha um nome ou código de país diferente da entidade emissora, pode ser uma indicação de fraude;
- Não clique nos links de mensagens ou SMSs suspeitos. Em caso de dúvida, poderá copiar o endereço do link (URL) da mensagem recebida e faça uma pesquisa num motor de pesquisa. O endereço do link pode já ter sido identificado como sendo fraudulento/malicioso;

- Suspeite de anexos em mensagens de mail de suspeita ou desconhecida. Abra apenas anexos que estiver à espera de receber;
- Suspeite de páginas ou formulários onde são solicitados em conjunto, o número de telemóvel, códigos de acesso (utilizador/password) e todas as coordenadas do cartão matriz;
- Caso haja captação dos dados pessoais, nomeadamente os códigos de acesso (utilizador/password) e telemóvel, tenha em atenção se é contactado por alguém que alega ser funcionário de uma operadora de telecomunicações (ou usurpando qualquer outra entidade) para que consiga ter acesso a algum código recebido por SMS ou que contacta a operadora de telecomunicações, usurpando a entidade do cliente, para que consiga obter a 2ª via do cartão SIM, para que consiga obter os novos códigos por SMS;
- O facto de ter recebido um e-mail de um amigo não significa que tenha sido ele mesmo a enviar. O computador do seu amigo pode ter sido comprometido por um malware (software malicioso), cujo comportamento é enviar e-mails para todos os seus contatos. Se receber um e-mail suspeito de um amigo ou colega, confirme, ligando-lhe para o número de telefone que tem e nunca para o número que seja identificado na mensagem;
- Esteja alerta para mensagens de correio eletrónico com promessas de dinheiro fácil ou negócios que parecem demasiado aliciantes, estas ofertas podem ter o objetivo de utilizar a sua conta para fins ilícitos;
- Os Bancos nunca solicitam informações pessoais e/ou confidenciais por contacto telefónico, mensagens de correio eletrónico ou por SMS. Se receber uma mensagem/contacto nesse sentido, não forneça qualquer informação e entre de imediato em contacto com o seu banco, através da respectiva linha de apoio telefónico;
- Evite clicar em mensagens, imagens ou conteúdos publicitários de aspecto ou origem duvidosa.

Cuidados com acesso a sites e navegação na internet:

- Nunca aceda a sites, através de links, com informação pessoal, confidencial ou sensível, ou que permita realizar operações bancárias. Digite sempre o endereço completo do site a que pretende aceder na respetiva barra;
- Os Códigos de Acesso/Passwords são Pessoais e Intransmissíveis, pelo que nunca deverão ser fornecidos/disponibilizados a terceiros, nem mesmo, a outro(s) titular(es) da(s) conta(s);
- Sempre que aceder a sites bancários, verifique se o endereço se inicia por https://, com certificado válido e seguro "Caixa Económica Montepio Geral, Caixa Económica Bancária, S.A. [PT]" e que, no final do endereço ou barra inferior da janela, se encontra um cadeado;
- Contacte o seu banco caso verifique que os dados solicitados na página de acesso ao serviço homebanking foram alterados, sem comunicação prévia;
- Estabeleça limites e crie regras de utilização da Internet. Por exemplo, implemente restrições de acesso para impedir os mais novos de instalar ou de executar programas que não sejam do seu conhecimento;
- Evite clicar em links ou fazer download de aplicativos de fontes desconhecidas.

Cuidados com o seu equipamento (PC, telemóvel ou tablet):

- Instale um antivírus e mantenha-o permanentemente atualizado. Não atualizar o antivírus é quase o mesmo que o não ter;
- Utilize também uma "firewall" no seu computador. Trata-se de um programa que lhe possibilita filtrar o tráfego da Internet que entra e sai do seu computador, tornando mais difícil o contágio por software malicioso;
- Esteja atento às atualizações de segurança que os fornecedores credíveis de software disponibilizam e aplique-as de acordo com as instruções que são fornecidas. Este aspecto é particularmente relevante para actualizações do navegador que usa para aceder à Internet (Google Chrome, Safari, Firefox, Internet Explorer, Opera, etc) e do sistema operativo do seu computador (Windows, iOS, Google Chrome OS, etc);
- Dificulte o acesso indevido ao seu smartphone e proteja-o com uma password de acesso. Estes equipamentos podem ser facilmente perdidos ou roubados;
- Instale apenas as aplicações disponibilizadas pelos fornecedores confiáveis (Apple AppStore/iTunes, Google Play™, Windows® PhoneStore, BlackBerry® World, Nokia Store). Confirme sempre quais são os níveis de permissão que são pedidos;
- Aceda apenas a Redes Wi-Fi conhecidas;
- Sugerimos ainda que ensine os mais novos que nem tudo deve ser partilhado na internet e nas redes sociais e que a utilização dos computadores/smartphones deve ser efetuada de forma responsável.

Como posso reportar ao Banco de Empresas Montepio uma situação em que seja alvo de fraude?

Entre imediatamente em contacto connosco através do telefone 210.416.200 ou email info@bancobem.pt