Dia Internacional
da Internet mais Segura!

07 FEV

Região Autónoma da Madeira
Governo Regional

Secretaria Regional
de Inclusão Social e Cidadania
Direção Regional da Cidadania e dos Assuntos Sociais

Introdução

O *DIA DA INTERNET MAIS SEGURA* é assinalado, todos os anos, em vários países, no início de fevereiro, com o objetivo de promover a utilização segura e consciente da internet, por parte de toda a população, nela se incluindo crianças e idosos: grupos mais expostos aos riscos desta rede de comunicação global.

A Direção Regional da Cidadania e dos Assuntos Sociais, através da Direção de Serviços do Consumidor, associa-se a esta comemoração, com o lançamento de um COMPÊNDIO INFORMATIVO, em formato digital, com DICAS DE SEGURANÇA nos diversos âmbitos, nomeadamente, segurança na internet em geral, *e-mail*, *operações* bancárias, compras *online* e redes sociais.

Com estas dicas pretende-se alertar os Consumidores para os riscos a que poderão estar expostos aquando da navegação na Internet, dando-lhes algumas ferramentas que contribuem para mitigar esses riscos, permitindo que naveguem na internet de modo mais seguro.

Em complemento, foi elaborado um QUESTIONÁRIO que visa avaliar o grau de conhecimentos do Consumidor, nesta matéria, bem como, reforçar o conhecimento sobre o tema, ao permitir a consulta dos resultados corretos às questões apresentadas.

Em cada tema, serão dadas ferramentas transversais à utilização de todo o tipo de equipamentos ligados à Internet.

Dicas

Segurança na internet em geral

1. Assegure-se que o seu dispositivo (*smartphone*, computador, tablet ou outro equipamento similar) possui o *firmware* atualizado;

2. Efetue sempre as atualizações de *software* recomendadas pelo fabricante ou por quem desenvolveu as aplicações;

3. Não descarregue software não credenciado, como sejam, por exemplo, programas que se encontrem fora das lojas de aplicações, *Play Store*, etc.;

4. Crie uma senha ou padrão de segurança para aceder ao seu dispositivo;

5. Não se esqueça do antivírus! É uma ferramenta importante!;

6. Utilize senhas diferentes em cada sítio na Internet e altere-as, com regularidade (preferencialmente, de 6 em 6 meses);

7 Utilize conexões seguras! Deve evitar acessos públicos, como redes de centros comerciais, cafés e computadores partilhados, privilegiando o uso de redes privadas, nomeadamente, a sua internet fixa e móvel:

7.1 Se utilizar equipamentos públicos, não aceda a informações bancárias e evite entrar nas suas redes sociais. Se o fizer, não guarde as senhas no computador, devendo terminar a sessão, eliminar histórico e o cache do browser;

7.2 Na sua rede doméstica (privada), utilize o protocolo de segurança WPA2 ou superior, devendo mudar o nome e senha da sua rede (router);

7.3 Caso o seu router não disponha do protocolo WPA2 ou superior, deve solicitar um equipamento mais recente ao seu operador de comunicações eletrónicas;

7.4 Ao partilhar a sua internet doméstica com outra pessoa, utilize a opção guest do seu router com uma senha diferente da sua rede privada;

7.5 Deve adquirir uma VPN (Virtual Private Network) se utiliza frequentemente equipamentos públicos e/ou redes públicas;

8 Não clique em links ou forneça quaisquer dados, em caso de dúvida sobre a origem, veracidade e/ou identidade do remetente.

E-mail

1 Proteja a sua caixa postal digital com uma senha robusta, de preferência com mais de 12 caracteres, incluindo símbolos, números, utilização do alfabeto entre letras maiúsculas e minúsculas;

2 A senha do e-mail deverá ser exclusiva, ou seja, diferente de todas as que utiliza noutros sítios na internet;

3 Caso pretenda uma segurança de "nível militar", pode usar chaves de segurança num equipamento de hardware;

4 Nunca partilhe a senha do seu e-mail;

5 Analise frequentemente o registo de atividade do seu e-mail;

6 Remova as aplicações que já não utiliza do registo de atividade.

Operações bancárias

1 No acesso à sua entidade bancária, através do browser, certifique-se de que o endereço digitado na barra de pesquisa corresponde ao sítio oficial do banco. Há registo de casos de clonagens de sítios da internet de instituições bancárias!

2 Salve no seu browser como marcador, o sítio oficial da sua instituição bancária;

3 Em caso algum, forneça os seus dados de homebanking a terceiros;

4 A instituição bancária não solicita dados de acesso ao *homebanking* (n.º de utilizador / código multicanal / código da matriz) por telefone ou por e-mail aos seus clientes! Apenas solicita informações pessoais (nome, morada, data de nascimento) ou dados avulsos do código multicanal ou da matriz, mas nunca os números todos! Se isso acontecer, poderá a estar a ser alvo de tentativa de fraude!

5 A utilização das aplicações de homebanking das diversas instituições bancárias, devem estar sempre atualizadas;

6 Deve configurar um parâmetro adicional de segurança, no caso das aplicações bancárias, dificultando o seu acesso a quem se possa apropriar indevidamente do seu dispositivo móvel;

7 Sempre que possível, opte pela configuração dos seus dados biométricos, evitando o acesso através de FACE ID;

8 Confirme todas as operações que realiza antes de proceder à sua concretização, pois muitas delas são irreversíveis;

9 Sempre que possível, evite colocar o número dos seus cartões físicos, aquando das compras online;

10 Opte pela criação de cartões virtuais, temporários e com limite de utilização, mitigando o risco de serem utilizados sem o seu consentimento, em caso de ciberataque. Estes cartões são criados a partir da existência de um cartão físico, sendo únicos e seguros.

Compras online

1. Opte por aceder a sites de empresas de confiança e marcas conhecidas;
2. Pesquise e compare preços;
3. Obtenha informações prévias sobre o produto, antes da compra;
4. Recolha informações completas sobre a identificação da empresa ou do vendedor, nomeadamente, o nome ou denominação social, o seu endereço geográfico e eletrónico, o registo comercial e o número de identificação fiscal;
5. Certifique-se de que está a comprar numa loja fidedigna, tendo em atenção o endereço do website, por ex. https://www.(nomedaloja) e do domínio, sendo os mais comuns ".com" e ".pt";
6. Pesquise em fóruns na internet e visualize eventuais reclamações de outros consumidores, certificando-se da identidade e credibilidade do vendedor,
7. Leia as informações da loja online, os termos e condições da venda e as políticas de privacidade (Ex: condições de devolução e reembolso; prazos e custos de entrega; assim como, o valor real dos produtos em caso de saldos, promoções; ...);

8 Verifique se o sítio da internet tem os certificado SSL, se o endereço que figura da barra tem a sigla “https” ou o símbolo de um cadeado;

9 Não forneça dados pessoais ou confidenciais que não sejam absolutamente necessários para realizar o pagamento;

10 Opte sempre por cartões virtuais e temporários, limitando o seu montante ao valor da compra;

11 Utilize outros meios de pagamento que forneçam segurança adicional, como o Paypal, entre outros;

12 Escolha uma modalidade de pagamento segura, tendo em vista o produto que vai comprar;

13 Saiba que, após fazer uma compra online, o vendedor deve enviar imediatamente a fatura em formato digital;

14 Guarde os comprovativos de pagamento;

15 Em caso de fraude, participe às entidades competentes, nomeadamente, à Polícia de Segurança Pública, Polícia Judiciária e a Autoridade Regional das Atividades Económicas.

Redes sociais

1 As senhas das redes sociais devem ser diferentes da senha do seu e-mail, devendo privilegiar o uso de uma senha diferente em cada rede social;

2 Não partilhe a sua senha com terceiros;

3 Não clique em links enviados por utilizadores que não conhece;

4 Antes de aceitar qualquer pedido que lhe seja dirigido, informe-se acerca da identidade do remetente;

5 Opte pela "segurança a dois passos", que consiste na introdução de uma senha principal e do código enviado para se autenticar, maioritariamente, através de token que receberá via SMS ou através de aplicação de autenticação;

6 Tenha atenção à informação que disponibiliza nas redes sociais, pois a mesma pode indicar o local onde se encontra, onde vive ou frequenta;

7 Não ligue as suas contas de redes sociais entre si;

8 Atribua às aplicações as permissões essenciais para funcionarem, devendo desabilitar aquelas que o identificam geograficamente (localização);

9 Preste atenção aos redireccionamentos para páginas externas às redes sociais;

10 Caso opte por efetuar alguma compra, através de uma rede social, avalie o risco da operação, procurando feedback de outros utilizadores;

11 Não se encontre pessoalmente com desconhecidos.

Dia Internacional
da Internet mais Segura!

O Mundo Digital está em constante mudança, razão pela qual as recomendações de segurança aqui indicadas não são estanques. Mantenha-se atualizado e devidamente informado sobre as novas realidades e consciente da importância de adotar comportamentos responsáveis e seguros ao navegar na Internet.

Navegue em Segurança!

Link de acesso ao questionário - ***AQUI***

Região Autónoma da Madeira
Governo Regional

Secretaria Regional
de Inclusão Social e Cidadania
Direção Regional da Cidadania e dos Assuntos Sociais