FINANFARMA
Especialistas em Saúde Financeira

myFINANFARMA

Boas práticas de Segurança myFinanfarma

1. Utilização do computador

Deve garantir que utiliza software licenciado e com as últimas atualizações instaladas, dado que é através destas que são corrigidas as vulnerabilidades de segurança detetadas, com antivírus atualizado, para garantir auxílio na proteção contra malware (vírus, trojans, worms, spyware), e firewall ativa para impedir acessos remotos não autorizados aos dados.

O antivírus deve ser instalado de uma fonte fidedigna, mantido atualizado automaticamente e executado regularmente a procura de vírus no seu dispositivo, em ficheiros que lhe são enviados antes de abrir e em novo software antes de instalar.

2. Utilização da Internet

A. Não utilizar computadores públicos nem redes públicas para aceder ao myFinanfarma

O acesso através de computadores públicos aumenta a probabilidade de revelação de dados a terceiros uma vez que pode estar a ser observado, os dados podem estar a ser armazenados no computador que está a utilizar ou captados na rede pública a que acedeu, pelo que deve ser evitado.

B. Não comunicar os seus dados pessoais

Para aceder ao myFinanfarma necessita de introduzir o nome de utilizador e palavra-chave. Estes dados devem ser memorizados – não devendo ser guardados no browser utilizado, nem escritos, nem enviados para si mesmo ou comunicados a alguém.

A palavra-chave deve ser alterada regularmente (e.g. 60 dias) e deve ter em conta as seguintes recomendações:

a. Deve conter pelo menos 12 caracteres, letras maiúsculas, letras minúsculas, números e caracteres especiais;

b. Não deve utilizar uma palavra-chave com padrões fáceis de reconhecer nem com dados que sejam facilmente associados a si (por exemplo data de nascimento, data de casamento, número de documento de identificação, telefone);

Através de um ataque de bruteforce, um atacante levará tanto mais tempo a descobrir a sua palavra-chave quanto maior a sua complexidade.

Exemplo: *pense numa frase fácil de decorar para si e utilize as primeiras letras para a password: Esta frase pode ser um bom exemplo para criar uma palavra passe robusta. (Efpsubepcuppr.) Pode robustecer ainda mais com a utilização de algarismos (Efps1bepc1ppr).*

C. Consultar sites seguros

Deve consultar sites seguros, o url começa com https:// e tem um cadeado na barra de endereço, uma vez que nestes a informação transmitida não é acessível

a terceiros, devido à encriptação dos dados e verificação da autenticidade do servidor através de certificados digitais. Pode verificar um certificado digital de um site clicando no cadeado da barra de endereço.

D. Não abrir mensagens de remetentes desconhecidos/não confiáveis

As mensagens de email com anexos são frequentemente utilizadas para difundir vírus, não devendo por isso abrir os anexos sem se certificar junto do remetente da mensagem que esta foi de facto enviada por ele e sem executar o antivírus sobre os mesmos.

E. Conferir os dados do pedido antes da inserção de um sms token

Todos os pedidos realizados através do myFinanfarma requerem um segundo fator de autenticação, a colocação de um sms token, que é enviado para o número de telemóvel do utilizador. O utilizador não o deve comunicar a ninguém e antes de inserir o sms token deve verificar que os dados do pedido que realizou são os que lhe estão a ser comunicados no sms.

F. Terminar sempre a sessão myFinanfarma

Clique sempre em "Sair" antes de fechar a janela do browser. Embora o myFinanfarma esteja configurado para garantir o logout automático ao fim de algum tempo, desta forma assegura que terceiros não poderão aceder ao seu myFinanfarma no seu computador.

G. Limpar a cache e cookies do computador regularmente

Embora o myFinanfarma esteja configurado para não guardar cache, tal pode acontecer devido a configurações dos browsers, pelo que deve limpar a cache e cookies após cada utilização, para que não haja risco de terceiros terem acesso aos seus dados.

Para proceder à limpeza de cache e cookies deve aceder às configurações do browser e no menu de histórico escolher a opção "Limpar dados de navegação".

Falhas de Segurança

O cumprimento das boas práticas acima referidas aumentará o nível de segurança, evitando que seja alvo e vítima de ataques, como o phishing e o spyware.

Phishing

Se receber emails com links ou ficheiros anexos que requeiram uma ação, nomeadamente de um remetente desconhecido ou não confiável, não deve abrir, responder ou reencaminhar o email, os ficheiros não devem ser abertos e/ou descarregados para o computador e os links não devem ser acedidos, uma vez que podem conter vírus que irão infetar o seu computador.

A. Se receber um email a indicar que se não efetuar imediatamente uma dada ação, nomeadamente partilha de dados confidenciais, os seus contratos serão inibidos, não o faça.

A Finanfarma não requere aos clientes a partilha de quaisquer dados pessoais, pelo que em caso de dúvida contacte-nos - utilizando o contacto que está no nosso website e não um que possa constar no email ou página web acedida através de link e/ou email fraudulento que recebeu.

B. Se receber um email cuja proveniência pareça ser a Finanfarma, mas não é, e em que lhe é pedido que através de um link aceda ao myFinanfarma, não o faça, dado que o link pode dirigi-lo para uma página web que parece legítima (por vezes muito semelhante à real), e ao introduzir as suas credenciais estas são guardadas para fins fraudulentos.

Nunca deve aceder ao seu myFinanfarma por links - deve digitar sempre o url da página à qual pretende aceder.

Existem alguns denominadores comuns em emails com propósito fraudulento:

a. Requerem uma ação, nomeadamente clicar num link ou partilhar dados pessoais, como por exemplo a sua palavra-chave, indicando que se não o fizer poderá levar à suspensão de um serviço;

b. A linguagem da mensagem não é por vezes a adequada, contendo erros de escrita;

c. Ao clicar num link é dirigido para uma página não segura (mesmo que o url fraudulento seja muito semelhante ao original deve verificar sempre o endereço).

Em caso de ter sido alvo de tentativa de phishing ou de ter sido vítima do mesmo, reporte para o cso@anf.pt.

Spyware

Os ataques de spyware são efetuados através da instalação, sem o conhecimento do utilizador, de software que permite recolher informações confidenciais das ações realizadas. Para reduzir a probabilidade de ser alvo deste tipo de ataque, deve assegurar que tem um antivírus instalado e atualizado, que tem módulo anti-spyware ativo e corretamente configurado e evitar instalar software de fontes não confiáveis.

Mecanismos de segurança da Finanfarma

No acesso ao myFinanfarma estão implementados mecanismos de segurança para evitar que seja alvo e vítima dos ataques acima referidos.

A. Autenticação e identificação

Para fazer login no myFinanfarma, o cliente deve introduzir o seu nome de utilizador e palavra-chave.

No primeiro acesso é ainda requerido um sms token. Após este primeiro acesso, o utilizador deve alterar a palavra-chave que lhe foi enviada após adesão, seguindo as boas práticas de definição de palavras-chave referidas anteriormente.

Para alterar as credenciais de acesso deve proceder da seguinte forma:

a. Para alterar a palavra-chave deve inserir a palavra-chave atual e a nova que pretende, confirmando-a;

b. Para alterar o telemóvel para onde é enviado o sms token, terá sempre de receber um token no telemóvel definido inicialmente para confirmar a alteração.

B. Segundo fator de autenticação - SMS token

O sms token é uma credencial de segurança adicional para autenticação e confirmação de pedidos no myFinanfarma.

É requerido sms token para as seguintes ações:

a. No primeiro acesso – após colocação da palavra-chave o utilizador tem de inserir um código enviado para o seu telemóvel;

b. A cada 90 dias, ao realizar login no myFinanfarma;

c. Para confirmação da realização de pedidos e confirmação das autorizações pendentes.

Nos casos acima é enviado para o telemóvel do utilizador um código de utilização única e que tem validade de 120 segundos, sendo que ao fim deste tempo deve solicitar um novo token.

C. Consulta da data e hora do último acesso

Ao aceder ao myFinanfarma, o cliente é informado no canto superior direito da data e hora do seu último acesso. Desta forma poderá detetar eventuais acessos indevidos.

D. Logout automático

Ao fim de algum tempo de inatividade o myFinanfarma está configurado para proceder ao logout automático, de forma a assegurar que a sessão não fique aberta por esquecimento. Para novo login deve voltar a introduzir nome de utilizador e palavra-chave.

E. Certificado digital

O certificado digital é emitido por uma autoridade certificadora independente que permite validar que o site é legítimo, e garante que as comunicações são encriptadas e seguras.

Abaixo segue um print do certificado digital da página myFinanfarma:

FINANFARMA
Especialistas em Saúde Financeira

my FINANFARMA

my.finanfarma.pt