PLANO NACIONAL
DE FORMAÇÃO FINANCEIRA

TODOS CONTAM

FINANÇAS DIGITAIS
PROTEGER EQUIPAMENTOS E ACESSOS À INTERNET

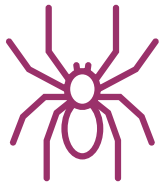
01 RISCOS A QUE ESTÃO EXPOSTOS OS EQUIPAMENTOS

02 CUIDADOS A TER

RISCOS A QUE ESTÃO EXPOSTOS OS EQUIPAMENTOS

PLANO NACIONAL
DE FORMAÇÃO FINANCEIRA
TODOS CONTAM

Um simples *download* pode instalar vírus que redirecionam o utilizador para páginas falsas



Pharming – Vírus que a vítima instala no seu equipamento (computador, tablet ou telemóvel), ao fazer o *download* de um ficheiro, que altera endereços pré-fixados pela vítima (nos seus favoritos por exemplo) e redireciona-a para uma página falsa

Spyware – Programa malicioso que é instalado no equipamento da vítima (computador, tablet ou telemóvel) para espiar e recolher os seus dados pessoais, como a palavra-passe ou código de acesso à conta bancária

CUIDADOS A TER

PLANO NACIONAL
DE FORMAÇÃO FINANCEIRA
TODOS CONTAM

Cuidados a ter para reduzir o risco de ocorrência de fraudes e proteger o acesso ao equipamento, evitando o acesso fácil por terceiros:

- Definir de palavras-passe fortes
  - Pouco óbvias
  - Não associadas a informação pessoal fácil de obter (datas de aniversário, nome dos filhos, etc.)
  - Com combinação de maiúsculas, minúsculas, números e símbolos, por exemplo

Deve evitar-se guardar palavras-passe e outras informações confidenciais em papel, em mensagens de *e-mail* ou no telemóvel. Existem gestores de palavras-passe *offline*, como o *Keepass*, que têm essa função

CUIDADOS A TER

Cuidados a ter para reduzir o risco de ocorrência de fraudes e proteger o acesso ao equipamento, evitando o acesso fácil por terceiros:

- Criar sequências de bloqueio de ecrã
- Manter atualizados o sistema operativo do equipamento, os *browsers* de acesso à internet e os programas antivírus e anti *spyware*
- Atualizar aplicações e programas instalados nos equipamentos, pois permitem corrigir problemas de segurança que o fabricante vai detetando

CUIDADOS A TER

PLANO NACIONAL
DE FORMAÇÃO FINANCEIRA
TODOS CONTAM

Cuidados a ter para reduzir o risco de ocorrência de fraudes e proteger o acesso ao equipamento, evitando o acesso fácil por terceiros:

- Apagar aplicações que já não são utilizadas
- Não clicar em *links*, nem fazer *downloads* cuja origem se desconhece
- Evitar a utilização de *wi-fi* públicos ou desconhecidos

Os movimentos da conta bancária devem ser consultados regularmente, para atuar atempadamente e evitar ou mitigar prejuízos financeiros resultantes de possíveis ataques fraudulentos