AMEAÇAS DA WEB

OLHE DUAS VEZES ANTES DE CLICAR

Pode perder o seu dinheiro, a sua informação pessoal e até os dados armazenados, se o dispositivo parar de funcionar. Não se deixe apanhar!

COMO PODE ACONTECER?

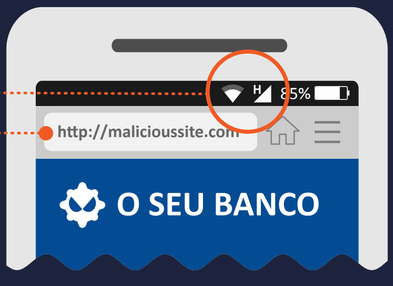
ATAQUES DE PHISHING: Enganam os utilizadores e levam-nos a fornecer informação pessoal fazendo-se passar por uma entidade credível. Propagam-se através do e-mail, mensagens de texto ou das redes sociais.

NAVEGAÇÃO EM SITES WEB: O seu dispositivo móvel pode ser infetado através de uma simples visita a um site Web não seguro.

TRANSFERÊNCIA DE FICHEIROS: As hiperligações e os anexos nocivos podem ser integrados diretamente num e-mail.

PORQUE É EFICAZ?

Os dispositivos móveis estão CONSTANTEMENTE LIGADOS à Internet.



O TAMANHO REDUZIDO DO ECRÃ DO DISPOSITIVO é uma condicionante geral. Os browsers dos dispositivos móveis mostram as URL num espaço de ecrã limitado, o que dificulta a confirmação da legitimidade do domínio.

A CONFIANÇA IMPLÍCITA DO UTILIZADOR na natureza pessoal de um dispositivo móvel.

O QUE PODE FAZER?

Desconfie de qualquer SMS ou chamada telefónica de uma empresa que solicite informação pessoal. Pode verificar se a mensagem/chamada é legítima ligando diretamente para o número oficial da empresa.

Ao navegar na Web através do seu dispositivo móvel, certifique-se de que a sua ligação é garantida através de HTTPS. Pode sempre confirmar olhando para o início da URL.

Nunca clique numa hiperligação/num anexo de um e-mail ou SMS não solicitado. Elimine-o imediatamente.

Tenha cuidado se este o conduzir para uma página com erros gramaticais, erros ortográficos ou de baixa resolução.

Se disponível, instale uma aplicação de segurança móvel que o alerte para qualquer atividade suspeita.

EUROPOL EC3 European Cybercrime Centre

POLÍCIA JUDICIÁRIA

#MobileMalware