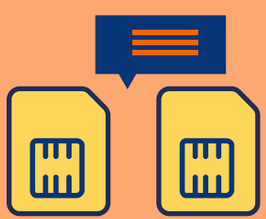
SIM SWAPPING – FRAUDE POR TELEMÓVEL

A fraude por Troca de SIMS (“SIM Swapping”) acontece quando o pirata informático, usando técnicas de engenharia social, assume o controlo do cartão SIM do seu telemóvel usando os seus dados pessoais roubados.

COMO FUNCIONA?

O pirata obtém dados pessoais da vítima através de phishing, comprometimento de dados, pesquisas na internet, apps falsas, sites falsos, malware, entre outros.

Com esta informação, o pirata engana o operador móvel, de modo a que este associe o número de telemóvel da vítima a um novo SIM na sua posse.



A partir deste momento, o pirata consegue receber chamadas e mensagens de texto, incluindo as necessárias para o acesso ao banco online.

A vítima perceberá que já não tem serviço de telemóvel e, eventualmente, deixará de ter acesso à sua conta online.

O QUE PODE FAZER?

- **Mantenha o seu software actualizado, incluindo o navegador da internet, antivirus e o sistema operativo.**
- **Não forneça dados pessoais e tenha cuidado na utilização de redes sociais.**
- **Nunca abra ou toque em links e anexos suspeitos recebidos por email ou SMS.**
- **Não responda a emails suspeitos nem fale ao telefone com pessoas desconhecidas que lhe peçam dados pessoais.**
- **Altere as suas passwords com frequência.**
- **Instale apps apenas de lojas oficiais e leia atentamente as permissões que lhe são pedidas.**
- **Sempre que possível, não associe o seu número de telemóvel a contas online sensíveis.**
- **Escolha um PIN apenas conhecido por si, para restringir o acesso ao seu cartão SIM. Não o partilhe nunca.**
- **Verifique com frequência os seus extratos bancários.**

FOI ALVO DESTE ATAQUE?

- Se o seu telemóvel perder acesso à rede sem razão, reporte o facto imediatamente ao seu operador.
- Se o seu operador lhe confirmar que o seu SIM foi “trocado”, reporte-o de imediato às autoridades policiais.

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

#CyberScams