

O que é o **RANSOMWARE?**

O ransomware é um **software malicioso** que bloqueia ou encripta os ficheiros de um utilizador ou organização e exige o pagamento de um resgate para restaurar o acesso aos dados

A **PREVENÇÃO** começa consigo



NÃO CLIQUE EM LINKS OU ANEXOS SUSPEITOS

Não clique em links, e-mails ou ficheiros de origem duvidosa. Esta é uma das formas mais comuns de ataques de ransomware



PROTEJA OS SEUS DADOS PESSOAIS

Tenha cuidado ao partilhar informações pessoais online, como nome, número de identificação, fotografias ou dados bancários



REFORCE A SUA SEGURANÇA

Active a autenticação de dois factores em todos os sites e contas de redes sociais, use palavras-passe diferentes para cada conta, com recurso a um gestor de palavras-passe, utilize uma firewall, instale um antivírus confiável e não use software “pirata” e duvidoso



USE PALAVRAS-PASSE FORTES

Uma palavra-passe deve ter pelo menos 12 caracteres e incluir letras maiúsculas, minúsculas, números e símbolos. Não inclua informação pessoal (data de nascimento, nomes, local de trabalho ou residência)



FAÇA CÓPIAS DE SEGURANÇA REGULARMENTE

Criar cópias de segurança (backup) dos seus dados num disco externo ou na nuvem para garantir que não os perde em caso de ataque



MANTENHA O SOFTWARE ACTUALIZADO

Actualize regularmente o sistema operativo e os programas. As actualizações ajudam a proteger o seu dispositivo contra novas ameaças



O que fazer em caso de ataque de **RANSOMWARE?**

Os **primeiros minutos** após um ataque podem
fazer toda a diferença para limitar os danos
Actue de imediato

Se for vítima, **AJA** imediatamente

1. ISOLE

Isole imediatamente o dispositivo afectado, desligando-o da rede, removendo o cabo de rede ou desactivando o Wi-Fi, para evitar a propagação do ataque

2. PRESERVE

Não apague ficheiros, não formate o dispositivo e não reinicie sistemas sem orientação técnica, pois isso pode destruir evidências importantes para a investigação

3. GUARDE PROVAS

Guarde mensagens, capturas de ecrã e outras provas que possam apoiar a investigação e a resposta ao incidente

4. NÃO PAGUE

Pagar o resgate não assegura que os dados serão recuperados. Além disso, o pagamento financia actividades criminosas e pode incentivar novos ataques

5. RECUPERE

Procure apoio de especialistas e consulte a página www.nomoreransom.org/ para verificar se existe alguma ferramenta de apoio disponível de descriptação de dados

6. DENUNCIE

Denuncie o caso à Polícia da República de Moçambique e à Procuradoria-Geral da República

7. NOTIFIQUE

Notifique a Equipa Nacional de Resposta a Incidentes de Segurança Cibernética – CSIRT.mz

www.ncsirt.mz/reportar-incidente/

