

Campanha #AlertaRansomware

Mensagens-chave para divulgação em comunicações institucionais, redes sociais e outros canais

Mensagem 1:

O ransomware é um tipo de software malicioso que os cibercriminosos utilizam para bloquear o acesso, destruir ou publicar dados ou ficheiros encontrados nos dispositivos infectados, a menos que seja pago um resgate.

Tudo começa com um clique de um e-mail ou mensagem aparentemente inofensiva, contendo um link ou anexo malicioso. A interação com este conteúdo permite a instalação do software no dispositivo, dando aos atacantes acesso ao sistema.

A partir daí, identificam e encriptam os dados sensíveis, tornando-os inacessíveis, e é nesse momento que exigem um resgate para restaurar o acesso.

Saiba como se proteger do ransomware e como responder a um ataque em: <https://ncsirt.mz/alerta-ransomware/>

#AlertaRansomware

Mensagem 2:

Imagine perder o acesso a todos os seus ficheiros: fotografias, documentos, dados bancários. Tudo porque clicou num link ou abrir um anexo de um e-mail. É isso que o ransomware faz.

O risco de um ataque de ransomware pode ser reduzido com medidas fáceis e práticas:

- ◆ Nunca clique em links, e-mails ou ficheiros de origem duvidosa
- ◆ Tenha cuidado ao partilhar informações pessoais online
- ◆ Crie palavras-passe fortes alfanuméricas, com pelo menos 12 caracteres
- ◆ Não use informações pessoais nas palavras-passe
- ◆ Utilize palavras-passe diferentes para cada conta, bem como um gestor de palavras-passe
- ◆ Active a autenticação multifactor em todos os sites e redes sociais
- ◆ Utilize uma firewall e um antivírus fiável
- ◆ Não instale software “pirata” ou duvidoso

- ◆ Mantenha o software actualizado
- ◆ Faça cópias dos seus dados regularmente em discos externos e em serviços de nuvem protegidos

#AlertaRansomware <https://ncsirt.mz/alerta-ransomware/>

Mensagem 3:

Os primeiros minutos após um ataque podem fazer toda a diferença para limitar os danos.

Se for vítima de ransomware, actue imediatamente:

- ◆ 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
- ◆ Não apague ficheiros, não formate o dispositivo e não reinicie sistemas sem orientação técnica, porque pode destruir evidências importantes para a investigação.
- ◆ Registe mensagens, capturas de ecrã e outras evidências que possam apoiar a investigação e a resposta ao incidente
- ◆ Não pague o resgate: Pagar o resgate não assegura que os dados serão recuperados. Além disso, o pagamento financia actividades criminosas e pode incentivar novos ataques
- ◆ Recupere os dados a partir de cópias de segurança
- ◆ Procure apoio de especialistas e aceda a *No More Ransom.org* para verificar se existe alguma ferramenta de apoio de descriptação disponível
- ◆ Denuncie o caso à Polícia da República de Moçambique e à Procuradoria-Geral da República, e notifique a Equipa Nacional de Resposta a Incidentes de Segurança Cibernética – CSIRT.mz: <https://ncsirt.mz/reportar-incidente/>

#AlertaRansomware <https://ncsirt.mz/alerta-ransomware/>