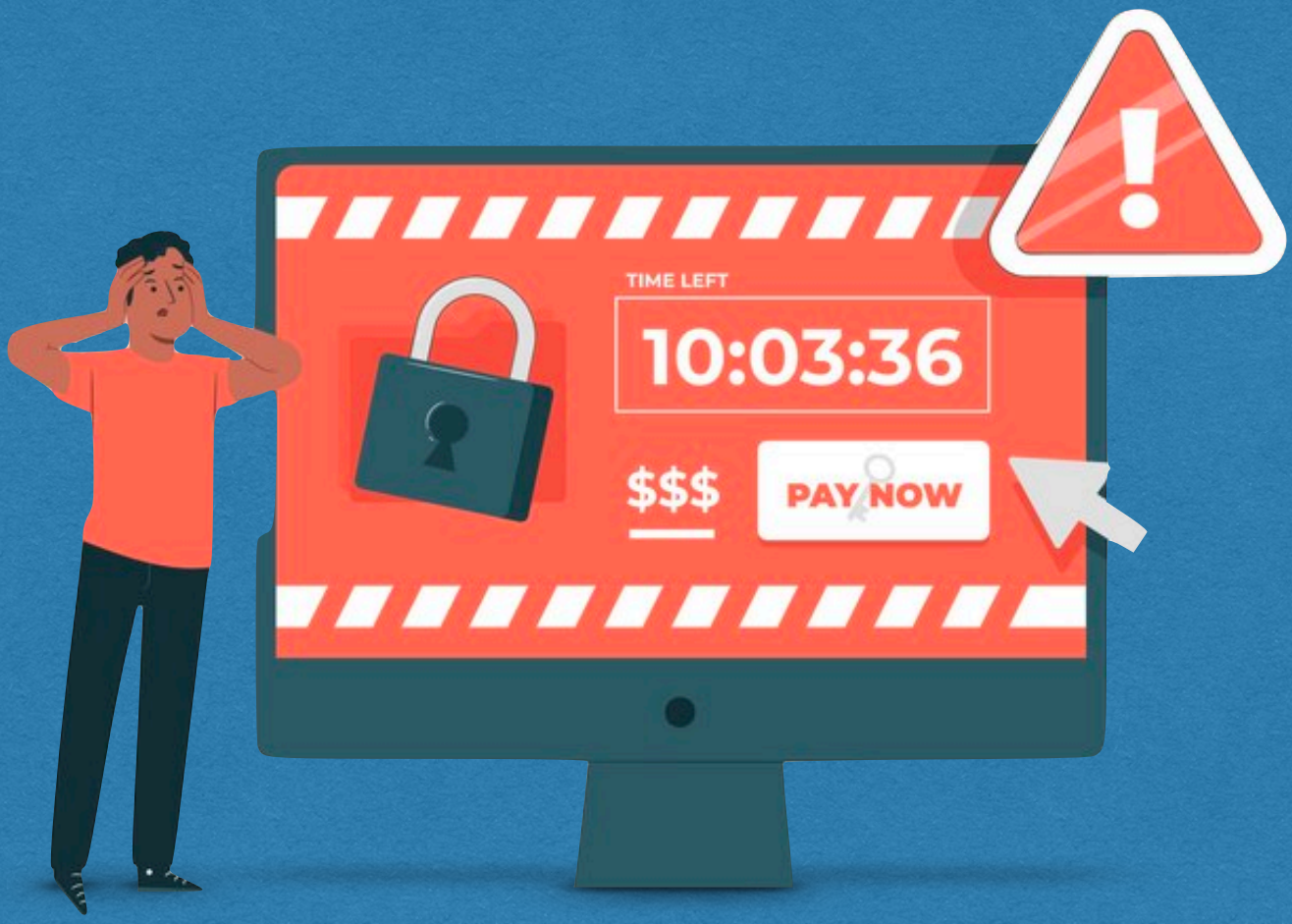
CIBERSEGURANÇA



#02 - O que é o Ransomware e como prevenir este tipo de ataque?

AHRESP®
ASSOCIAÇÃO DA HOTELARIA, RESTAURAÇÃO E SIMILARES DE PORTUGAL
Instituição de Utilidade Pública

highdome
closing the cyber gap

CIBERSEGURANÇA

Em parceria com a highdome,
especialista em segurança cibernética
para pequenas e médias empresas,
vamos disponibilizar-lhe todos os meses
conteúdos exclusivos para o sensibilizar,
a si e aos seus colaboradores,
a adotarem uma postura de prevenção
constante que permita fortalecer a
resiliência cibernética na sua empresa.

highdome
closing the cyber gap

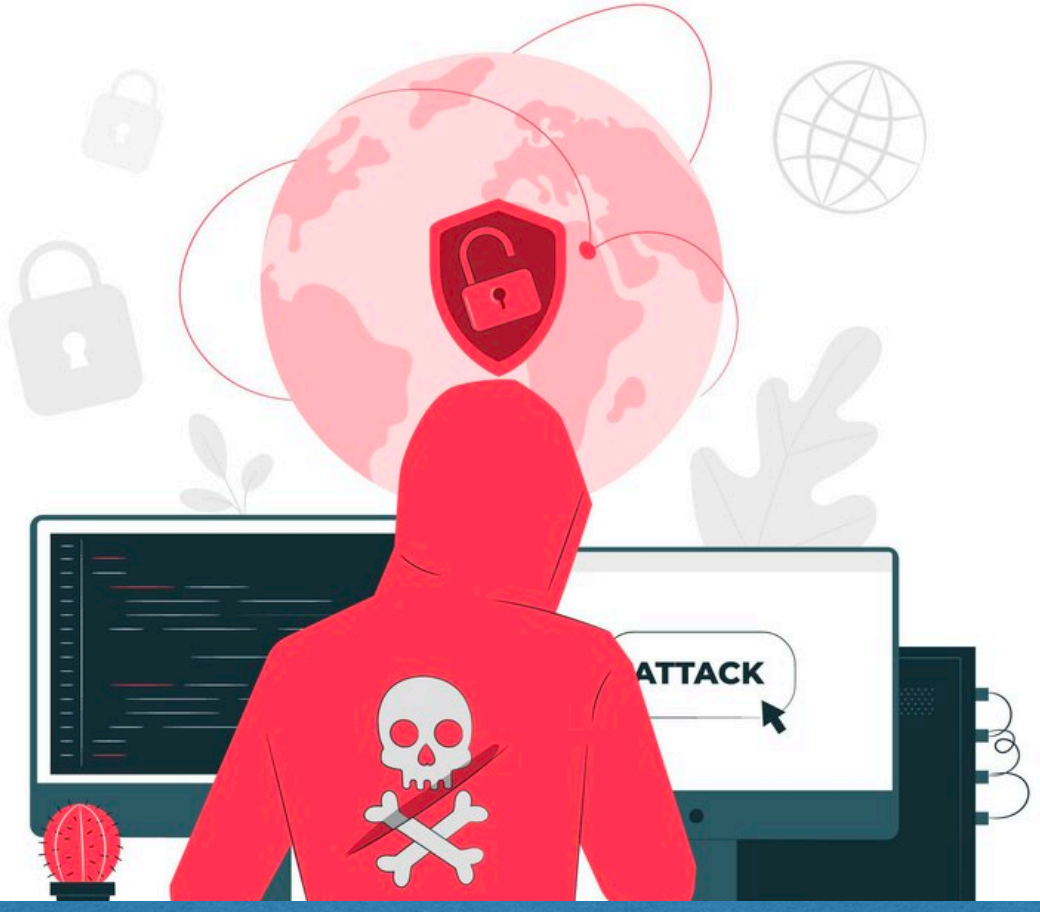
AHRESP®
ASSOCIAÇÃO DA HOTELARIA, RESTAURAÇÃO E SIMILARES DE PORTUGAL
Instituição de Utilidade Pública

#02
O que é o Ransomware

Ransomware é um tipo de malware que criptografa os arquivos da vítima.

Os invasores exigem um resgate da vítima para restaurar o acesso aos arquivos; por isto o nome ransomware.

Os ataques de ransomware estão a tornar-se cada vez mais comuns e podem causar transtornos e perdas financeiras significativas para indivíduos e organizações, além de uma exposição negativa da marca da empresa atacada.



#02
O que é o Ransomware

Existem várias formas de o ransomware chegar ao dispositivo da vítima. Alguns métodos comuns incluem:

Anexos de e-mail:
os invasores podem enviar software malicioso num anexo de e-mail, disfarçado como um arquivo legítimo.
Quando a vítima abre o anexo, o ransomware é instalado no seu dispositivo.

Links maliciosos:
Os invasores podem enviar um e-mail ou uma mensagem instantânea com um link que, se for clicado, transfere e instala o ransomware no dispositivo da vítima.

Downloads através de sites comprometidos:
o dispositivo da vítima pode ser infectado com ransomware simplesmente por visitar um site comprometido.
O malware é automaticamente transferido e instalado no dispositivo.

Explorações de vulnerabilidades de software:
O ransomware pode chegar ao dispositivo da vítima através de uma exploração de vulnerabilidades de software que ainda não foram corrigidas.
Isso pode acontecer se a vítima estiver a usar software desatualizado, por isso é importante manter todos os softwares actualizados.

#02
O que é o Ransomware

É muito importante seguir as melhores práticas de como prevenir ataques de ransomware:

- Atualizar e corrigir regularmente o seu sistema operativo e outros softwares.
- Usar um programa antivírus credível e mantê-lo atualizado.
- Fazer backup de arquivos importantes regularmente num local separado e seguro.
- Evitar abrir anexos de e-mail ou links de fontes desconhecidas.
- Desativar macros em documentos do Office, de fontes não confiáveis.

Se for vítima de um ataque de ransomware, é importante não pagar o resgate.

Isso pode encorajar os invasores e torná-lo um alvo de ataques futuros.
Em vez disso, tente restaurar os seus arquivos de um backup recente.
Se não tiver um backup, pode ser necessário procurar ajuda de um serviço profissional na área de dados.

Divulgue estes conselhos e partilhe-os na sua rede de contactos!

Caso queira aprofundar os seus conhecimentos e dos seus colaboradores consulte as informações sobre o Programa de Prevenção Cibernética da Highdome:

learn.highdome.io/prevencaocibernetica

CYBERSEGURANÇA

AHRESP®
ASSOCIAÇÃO DA HOTELARIA, RESTAURAÇÃO E SIMILARES DE PORTUGAL
Instituição de Utilidade Pública

highdome
closing the cyber gap