#NoMoreRansom
#CyberDialogues

PUBLICLY AVAILABLE INFORMATION CAN BE USED FOR A #RANSOMWARE ATTACK

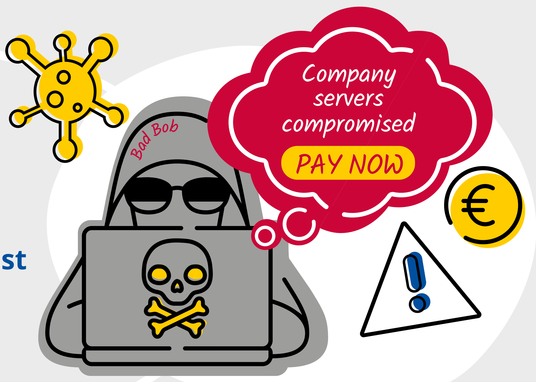
Bad Bob wants to target a specific company. He is searching open social media profiles to identify people working there.

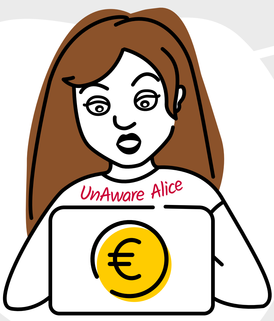
UnAware Alice receives an email asking her to validate her corporate credentials.

She is in a rush, so she does as instructed.

Thanks to Alice's account, Bad Bob gains access to her company's servers.

He locks some of their most valuable files and asks for a ransom. If they pay, he will just ask for more money.





Alice should have been more careful. If you become a victim of ransomware:

1. DON'T PAY
2. CHECK FOR DECRYPTION TOOLS: https://www.nomoreransom.org
3. REPORT IT TO THE POLICE

PROTECT YOURSELF FROM #RANSOMWARE

REMEMBER:
PROTECT YOUR DEVICES AND FILES BY FOLLOWING SIMPLE PREVENTION ADVICE.

1. KEEP YOUR PERSONAL DATA PRIVATE
2. REGULARLY CHECK YOUR PUBLICLY AVAILABLE INFORMATION (E.G. SOCIAL MEDIA)
3. DON'T CLICK ON UNEXPECTED OR SUSPICIOUS EMAILS

FOR MORE TIPS, VISIT: https://www.nomoreransom.org

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

NO MORE RANSOM

EUROPOL