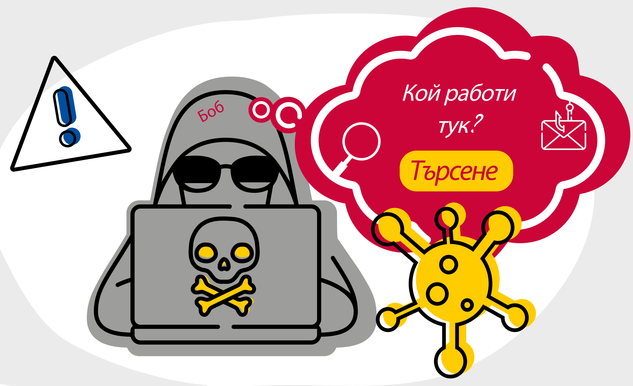
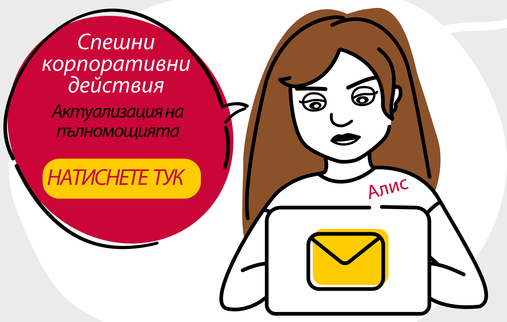
#NoMoreRansom
#CyberDialogues

ОБЩЕСТВЕНО ДОСТЪПНАТА ИНФОРМАЦИЯ МОЖЕ ДА СТАНЕ ОБЕКТ НА #RANSOMWARE АТАКА

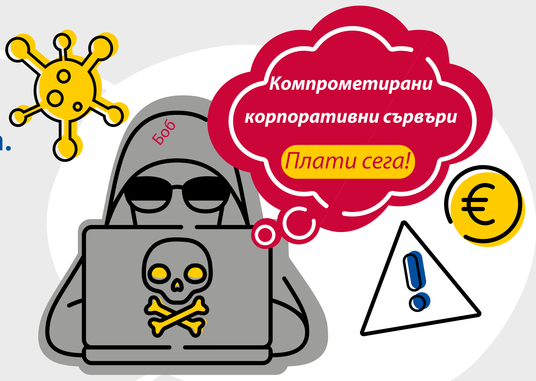
Хакерът Боб иска да се насочи към определена компания.
Той претърсва отворени профили в социалните мрежи, за да идентифицира работещите там.

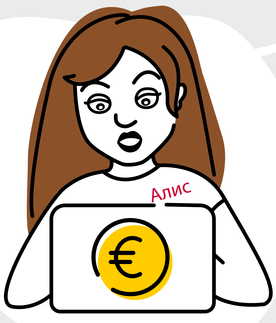




Алис изненадващо получава имейл, в който я молят да потвърди корпоративните си пълномощия.
Тя бърза, затова изпълнява указанията.

Благодарение на акаунта на Алис, Боб получава достъп до сървърите на компанията.
Той заключва някои от най-ценните им файлове и иска откуп.
Ако те платят, той просто ще поиска още пари.





Алис е трябвало да бъде по-внимателна. Ако станете жертва на ransomware:

1. НЕ ПЛАЩАЙТЕ!
2. ПРОВЕРЕТЕ ЗА ИНСТРУМЕНТИ ЗА ДЕКРИПТИРАНЕ: https://www.nomoreransom.org
3. ОБАДЕТЕ СЕ В ПОЛИЦИЯТА

ЗАЩИТЕТЕ СЕБЕ СИ ОТ #RANSOMWARE

ЗАПОМНЕТЕ: ЗАЩИТЕТЕ УСТРОЙСТВАТА И ФАЙЛОВЕТЕ СИ, КАТО СЛЕДВАТЕ ЛЕСНИ СЪВЕТИ ЗА ПРЕВЕНЦИЯ.

1. ПАЗЕТЕ ЛИЧНИТЕ СИ ДАННИ ПОВЕРИТЕЛНИ.
2. РЕДОВНО ПРОВЕРЯВАЙТЕ ПУБЛИЧНО ДОСТЪПНАТА СИ ИНФОРМАЦИЯ.
3. НЕ КЛИКАЙТЕ ВЪРХУ ПОДОЗРИТЕЛНИ ИМЕЙЛИ.

ЗА ОЩЕ СЪВЕТИ, ПОСЕТЕТЕ: https://www.nomoreransom.org

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

ИНСТИТУТ ПО ПУБЛИЧНА АДМИНИСТРАЦИЯ

NO MORE RANSOM

EUROPOL