|  |  |
| --- | --- |
|  |  |

***Izsiljevalsko programje je zlonamerna programska oprema, ki se polasti računalnika in skupaj z njim osebnih podatkov.*** Običajno v sistem vstopi z lažnim elektronskim sporočilom, zaradi ranljivosti sistema itd. Izsiljevalsko programje podatke zašifrira in kibernetski zločinci zahtevajo zajetne zneske, da bi žrtev do njih ponovno pridobila dostop. Čeprav uporabnik plača zahtevani znesek, to ne pomeni nujno, da bo ponovno pridobil dostop do podatkov. Oglejte si diagram, kaj se dejansko zgodi ob takem napadu.



**Kako lahko uporabniki ravnajo v takem primeru?**

Pred izsiljevalskim programjem se lahko obvarujete preprosto:

1. svoje podatke varnostno kopirajte #BackUp,
2. ne klikajte na povezave iz neznanih virov #Phishing,
3. redno posodabljajte svoje sisteme #Patch,
4. če vaše naprave podležejo, ne plačajte zahtevanega zneska! #Check www.nomoreransom.org

**Kibernetska varnost je naša skupna odgovornost**

Evropski mesec kibernetske varnosti je kampanja EU za ozaveščanje, ki poteka oktobra vsako leto po vsej Evropi. Pri državljanih in organizacijah želi spodbujati kibernetsko varnost, jih ozaveščati o grožnjah kibernetski varnosti ter z izobraževanjem in širjenjem dobrih praks poskrbeti za vire, da se lahko na spletu obvarujejo pred njimi.

#CyberSecMonth #CyberAware #eSkills #Cybersecurity