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

***Izspiedējvīruss ir ļaunprātīga programmatūra, kura datoru un kopā ar to arī personas datus izmanto par ķīlu.*** Parasti tas sistēmā nonāk ar pikšķerēšanas e-pasta starpniecību, sistēmas ievainojamības dēļ vai citu iemeslu dēļ. Izspiedējvīruss šifrē informāciju, un, lai upuris varētu datus atgūt, kibernoziedznieki pieprasa par to ievērojamu samaksu.  Pat tad, ja lietotājs to samaksā, tas nebūt nenozīmē, ka dati tiks atgūti.  Attēlā redzams, kas faktiski notiek šāda kiberuzbrukuma gadījumā.



**Ko šādā gadījumā var darīt lietotāji?**

No izspiedējvīrusiem sevi var pasargāt vienkāršā veidā, piemēram:

1. Veidojiet datu rezerves kopijas #BackUp
2. Neklišķiniet uz saitēm, ko esat saņēmis no nezināma avota #Phishing
3. Atjauniniet sistēmas #Patch
4. Ja kāda no sistēmām tiek inficēta, nemaksājiet pieprasīto izpirkumu! #Check www.nomoreransom.org

**Kiberdrošība ir kopīga atbildība**

EKDM ir ikgadējā ES informatīvā kampaņa, kas katru oktobri notiek visā Eiropā. Tās mērķis ir palielināt informētību par kiberdrošības apdraudējumiem, veicināt kiberdrošību iedzīvotāju un organizāciju vidū un ar izglītošanas un labās prakses izplatīšanas palīdzību piedāvāt resursus sevis aizsardzībai tiešsaistē.

#CyberSecMonth #CyberAware #eSkills #Cybersecurity