SI TË MBRONI TË DHËNAT TUAJA NGA **SULMET RANSOMWARE**

Sulmet ransomware janë në rritje; ky lloj sulmi është një kërcënim serioz si për bizneset ashtu edhe për individët. Ransomware është një lloj malware që kodon skedarët tuaj dhe i mban peng derisa të jepni informacione sensitive ose t'i paguani një shpërblim sulmuesit. Informohuni me disa këshilla që mund të ndiqni për të mbajtur veten të sigurt.

1. Mbani të përditësuar sistemin tuaj operativ dhe softuerin

Kryerja e përditësimeve të rregullta për sistemin tuaj operativ dhe produktet e softuerit do t'ju ndihmojë të mbroheni nga malware. Përditësimet e sigurisë do të korrigjojnë dobësitë (vulnerabilitetet) që mund të shfrytëzohen nga një aktor keqdashës dhe do t'i parandalojnë ata të kenë akses në pajisjen tuaj.

2. Shmangni hapjen e bashkëlidhjeve në email dhe klikimin në linke të panjohura

Kriminelët kibernetikë do të përpiqen t'ju mashtrojnë për të hapur linke ose për të vizituar një faqe interneti me qëllime keqdashëse. Nëse bini pre e mashtrimit të tyre, kjo lidhje mund të fillojë shkarkimet automatike të skedarëve që përmbajnë ransomware.

3. Shkarkoni skedarë vetëm nga burime zyrtare

Një nga gjërat më të rëndësishme kur merrni skedarë nga interneti është shkarkimi nga një burim i besuar. Nëse shkoni direkt te burimi zyrtar, zvogëloni shanset për të shkarkuar malware. Për shembull, nëse dëshironi të shkarkoni Google Chrome, duhet të vizitoni faqen aktuale të Google për të shkarkuar softuerin.

4. Përdorni antivirus

Softueri antivirus është një mënyrë efektive për të parandaluar një ransomware. Softueri antivirus funksionon duke zbuluar, karantinuar dhe bllokuar malware nga ekzekutimi në një pajisje. Është e rëndësishme që programi antivirus të mbahet i përditësuar pasi kriminelët kibernetikë po lançojnë vazhdimisht viruse dhe malware të rinj.

5. Mos lidhni me kompjuterin tuaj pajisje USB nga një burim i panjohur

Një metodë e zakonshme sulmi e përdorur nga aktorët keqdashës është instalimi i malware në një pajisje USB dhe lënia e tij në një zonë publike. Kur dikush gjen pajisjen USB, ai do ta lidh USB-në në kompjuterin e tij për të zbuluar se kujt i përket. Kjo do të ekzekutojë kodin keqdashës dhe do të infektojë pajisjen e tyre me ransomware.

6. Krijoni një kopje rezervë të sigurt të të dhënave

Rezervat e të dhënave janë një mënyrë efektive për t'u rikuperuar nga një sulm ransomware. Nëse pajisja juaj është infektuar me ransomware dhe nuk mund ta deshifroni pajisjen, do të keni përsëri një kopje të të gjithë skedarëve tuaj të rëndësishëm. Për të siguruar që rezervimi i të dhënave është i aksesueshëm pas një sulmi ransomware, rekomandohet të ruhet skedari rezervë në një hard disk të jashtëm.