NO MORE RANSOM!

Potrebujete pomôcť s odomknutím Vášho digitálneho života?

No More Ransom

Rady pre obete

Ako môžete predísť infekcii ransomwarom?

- Pravidelne zálohujte dáta uložené na Vašom počítači. Udržujte najmenej jednu kópiu na médiu, ktoré nebude pripojené k počítaču.
- Neklikajte na odkazy v nevyžiadaných alebo podozrivých e-mailoch.
- Vyhľadávajte a sťahujte len oficiálne verzie softwaru a vždy z dôveryhodných stránok.
- Na ochranu Vašich systémov pred hrozbami (vrátane ransomware) používajte odolné bezpečnostné produkty.
- Uistite sa, že Váš bezpečnostný software a operačný systém sú aktualizované.
- Na internete buďte ostražití a neklikajte na podozrivé odkazy, pop-up okná alebo dialógové boxy.
- Nepoužívajte vysoko privilegované kontá (kontá s administrátorskými oprávneniami) pre každodennú činnosť.

Boli ste infikovaní? Čo robiť ďalej...

- Vždy navštívte www.nomoreransom.org, aby ste zistili, či ste boli infikovaní variantami ransomwarov, pre ktoré sú tu zadarmo dostupné dešifovacie nástroje .
- Neplaťte výkupné. Budete financovať kriminálnikov a povzbudzovať ich v tom, aby pokračovali v ich nelegálnych aktivitách.
- Nahláste to Vašej národnej polícii. Čím viac informácií poskytnete, tým viac môžu byť orgány presadzovania práva efektívnejšie pri rozkladaní kriminálnych aktivít.
- Odpojte Vaše zariadenie od internetu alebo iného sieťového pripojenia (napr. domáca WiFi sieť) ihneď ako je to možné, aby ste zamedzili šíreniu infekcie.
- Preformátujte pevný disk infikovaného zariadenia, nainštalujte operačný systém, aplikácie, aktualizácie a obnovte uzamknuté súbory z Vášho záložného média (ak nejaké máte).

EUROPOL | EC3 European Cybercrime Centre

europol.europa.eu
nomoreransom.org