

IT bezpečnosť kancelárie



Prečo sú firmy obľúbeným terčom útokov?

- ✓ Na účtoch majú viac financií ako bežní ľudia.
- ✓ Disponujú veľmi zaujímavými a citlivými údajmi, ktoré môžu byť zneužitú na ďalšie vydieranie či predaj na čiernom trhu.
- ✓ Útoky môžu slúžiť ako forma konkurenčného boja.

Na čo si dávať pozor pri práci s počítačom?

- ✓ Phishingový útok a sociálne inžinierstvo
- ✓ Cielené útoky
- ✓ Malvér

Ako chrániť vašu domácu kanceláriu pred ransomvérom?

- ✓ Pravidelne aktualizujte operačný systém a všetky softvéry. Ak je to možné, povoľte automatické aktualizácie.
- ✓ Siahnite po viacvrstvovom bezpečnostnom balíku, akým je napríklad ESET Internet Security alebo ESET Internet Smart Security Premium, ktorý vašej domácej kancelárii poskytne komplexnú ochranu.
- ✓ Jedným z najlepších opatrení, ktoré môžete urobiť, aby ste zabránili negatívnym dôsledkom útoku ransomvérom, je pravidelné zálohovanie súborov. Môžete na to využiť externú jednotku, cloudovú zálohovaciu službu alebo oba spôsoby.

Ako zabezpečiť domácu kanceláriu bez pomoci IT experta?

Začnite vašim domácim routrom

Zmeňte výrobné heslo. Pri inštalácii routra nezabudnite skontrolovať firmvér. Uistite sa, že je vždy aktualizovaný.

Držte sa základov bezpečnosti

Používajte bezpečnostný softvér, ktorý obsahuje viac vrstiev ochrany.

Určte si doma bezpečnú pracovnú zónu

Uistite sa, že máte vyhradenú bezpečnú pracovnú zónu, ktorú využívate na prácu. Chráňte všetky firemné zariadenia pomocou silného hesla alebo prístupovej frázy.

Zostaňte ostražití bez ohľadu na to, odkiaľ pracujete

Je jedno, či pracujete z kancelárie, z domu alebo z vašej obľúbenej kaviarne. Mali by ste byť naďalej ostražití pred kybernetickými hrozbami. Neklikajte na odkazy alebo prílohy, najmä v nevyžiadaných e-mailoch.

Vzdelávajte sa

Hrozby sa neustále menia a vyvíjajú. Je preto dôležité sa neustále vzdelávať.