ZABEZPEČENIE V OBDOBÍ KRÍZY

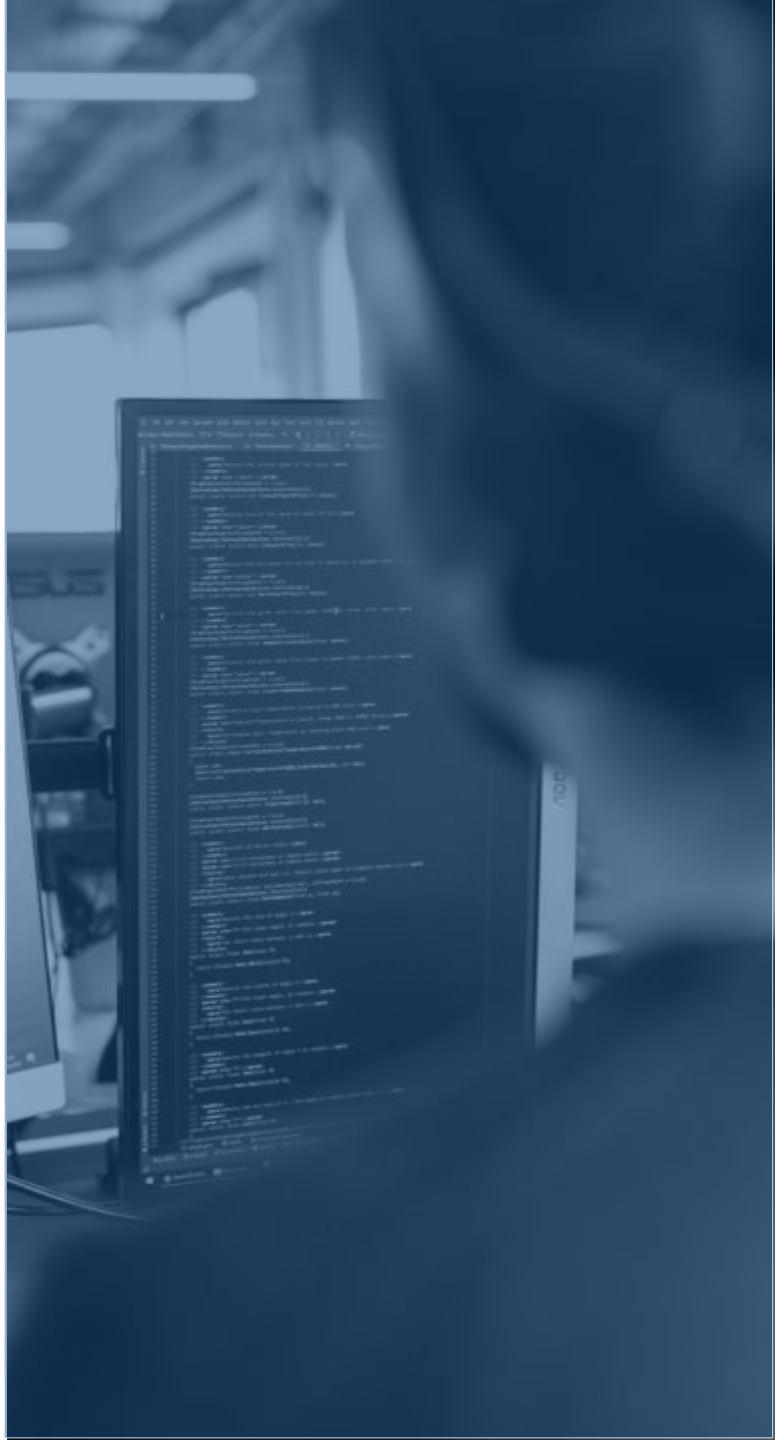
Marec, 2022

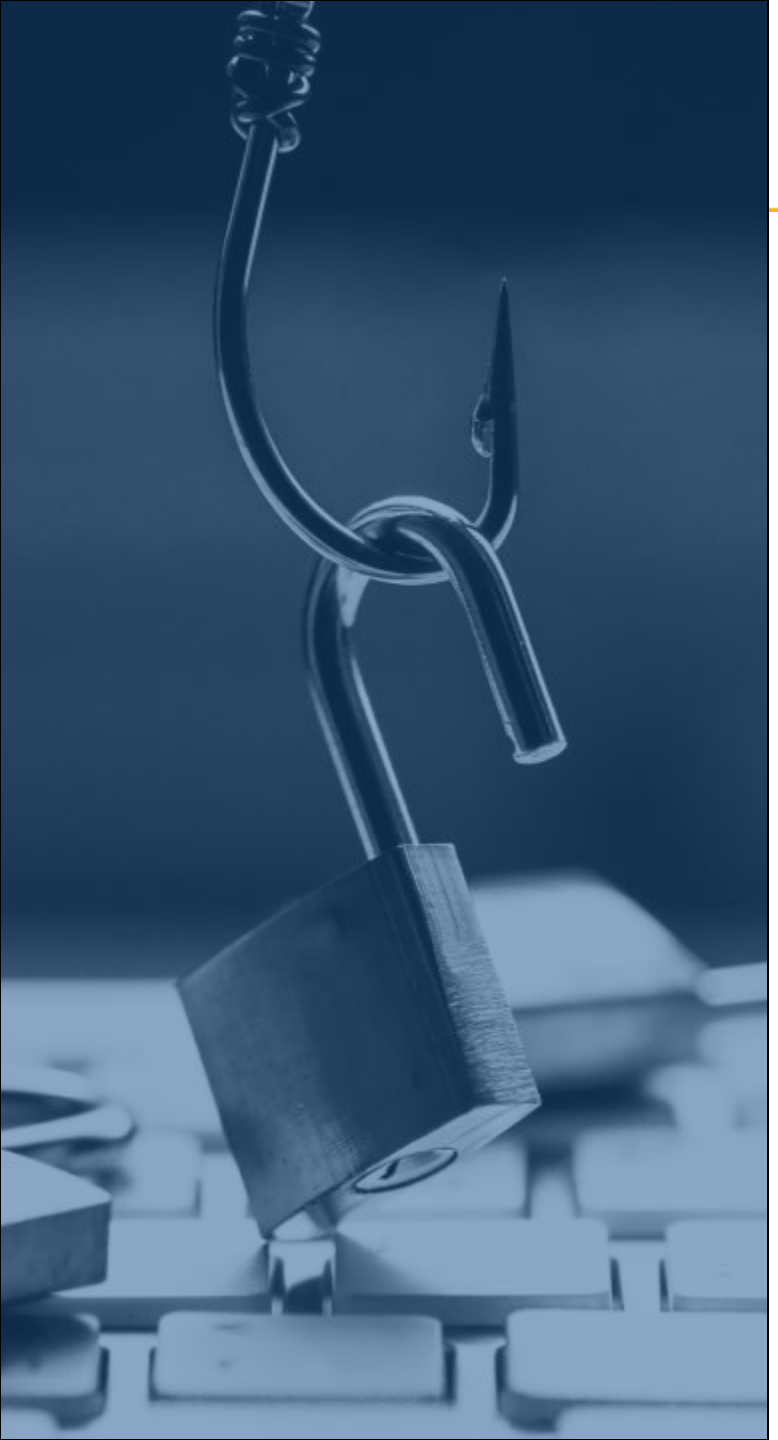
Technológiu poskytuje

Prečo na tom záleží

Kybernetická činnosť, ktorá súvisí s rusko-ukrajinským konfliktom sa prudko zvyšuje a aj keď nie sme do konfliktu priamo zapojení, zasahuje aj nás.

Každá svetová kríza má v sebe kybernetickú dimenziu a prudký nárast škodlivých e-mailov s phishingom naznačuje, že táto kríza nie je iná.





O čo ide

1. Obidve strany spustili vzájomné kybernetické útoky, ktoré zahŕňajú malvér, ktorý maže údaje, a prepínanie webových stránok offline, aby sa predišlo ich zneužitiu.

2. Tieto útoky sa nie vždy podarí zastaviť a často infikujú zariadenia a webové stránky, ktoré do konfliktu nie sú zapojené. Patria sem aj vaše podnikové alebo osobné zariadenia.

3. Vaše súkromné účty na sociálnych sieťach sú tiež ohrozené rizikom heknutia na účely šírenia falošných informácií alebo malvéru.

Čo môžete urobiť na ochranu svojej domácej siete

Nainštalujte si aktualizáciu operačného systému a zabezpečenia. Ak sú dostupné, malo by sa vám v počítači či telefóne zobraziť upzoornenie.

Pridajte dvojfaktorové overenie k svojim účtom na sociálnych sieťach (Facebook, Linkedin, Twitter atď.) a svojim e-mailovým účtom. Ak je to možné, pridajte aj záložný e-mailový účet.

Povedzte svojim priateľom a rodine, čo sa deje, a naliehajte na nich, aby postupovali rovnako.

Čo môžete urobiť na ochranu našej siete

Staráme sa o bezpečnosť internej siete, takže neexistujú žiadne technické kroky, ktoré musíte prijať.

Počas tohto obdobia môžete byť terčom vyššieho počtu phishingových útokov. Dávajte pozor na e-maily, v ktorých vás niekto žiada o pomoc s technickými alebo finančnými problémami.

Vždy skontrolujte adresu odosielateľa a nezabudnite, že toto je najdôležitejší krok pri identifikácii phishingu.