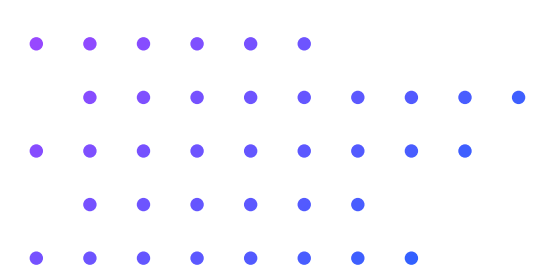


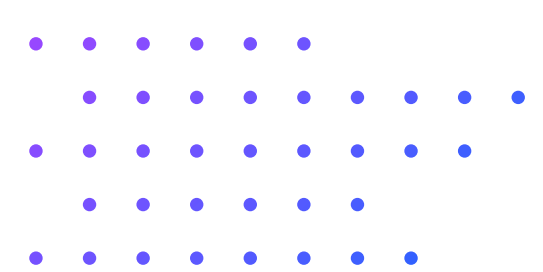
6 pravidel kybernetické bezpečnosti



1

Používejte silná, unikátní hesla a vícefaktorové ověření

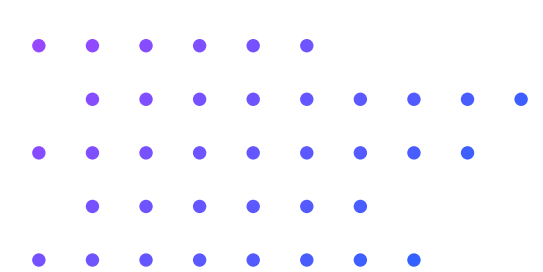
Minimálně 14 znaků, kombinace písmen, číslic a symbolů. Nepoužívejte osobní údaje ani známá slova. Zapněte vícefaktorové ověření tam, kde je to možné.



2

Pozor na přílohy a odkazy v e-mailech

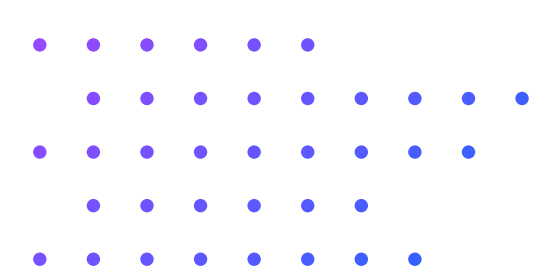
Podezřelé e-maily hlase IT oddělení. Neotvírejte podezřelé přílohy těchto e-mailů a neklikejte v nich na odkazy.



3

Chraňte bezpečnost svého zařízení

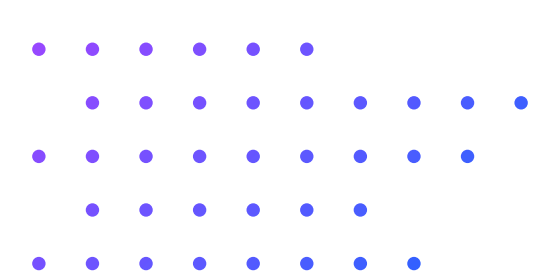
Při odchodu od zařízení ho vždy zamkněte, i když odcházíte jen na chvíli. Případné odcizení zařízení ihned hlase.



4

Nepoužívejte veřejnou Wi-Fi pro práci bez firemní VPN

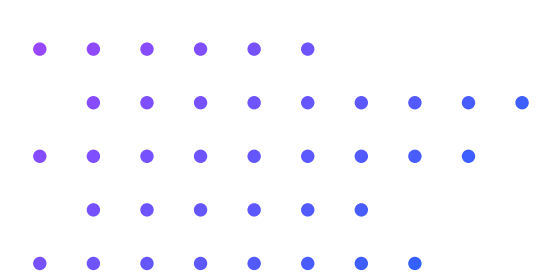
VPN šifruje komunikaci. Bez ní může být vaše připojení odposloucháváno a útočníci mohou získat přístup k firemním datům.



5

Používejte jen schválené nástroje

Používejte jen schválené firemní nástroje např. pro ukládání a sdílení souborů. Vyhněte se tzv. „shadow IT“.



6

Nevkládejte citlivé údaje do AI nástrojů

Firemní data a osobní údaje do AI nepatří. Formulujte dotazy obecně, informace před vložením anonymizujte a v nástroji vypněte funkci pamatování historie.



+420 515 919 805 | info@master.cz
www.master.cz

MasterDC