Zastavení útoku

- Odpojte napadený počítač/e od sítě.
  - Vytažením datového kabelu
  - Vypnutím wifi, pokud má počítač hardwarový vypínač.
  - Nespoléhejte se na odpojení od sítě (vypnutí wifi) v operačním systému!

Minimalizace škod

- Vypněte počítač a v žádném případě nezapínejte (při bootování se může spustit škodlivý software (např. ransomware, který zašifruje data).
- Z jiného zařízení (např. telefonu) na jiné síti (ideálně mobilní data) nejprve změňte heslo k vašemu hlavnímu emailovému účtu, poté k dalším účtům, ke kterým jste byli na daném počítači přihlášeni a také všude, kde máte stejná hesla.
- Pokud se k vašemu online účtu nemůžete přihlásit, zkuste obnovu hesla, příp. kontaktujte zákaznickou podporu
- Pokud byly v napadeném zařízení privátní klíče ke kryptoměnám, převeďte vše na jiné adresy
- Informujte správce sítě - nechte váš účet dočasně odstranit z firemních systémů, administrace internetových stránek (Facebook, LinkedIn apod.) a komunikačních kanálů (Slack, skupiny na Signalu, Telegramu apod.)
- Zablokujte platební karty pro platby na internetu
- Zkontrolujte odeslanou poštu (přes webové rozhraní, stále z jiného zařízení) zda vašim jménem neodešly škodlivé emaily
- Zkontrolujte ostatní zařízení v síti
- Informujte kolegy, přátele, zákazníky a obchodní partnery
- Pokud byly v počítači zneužitelné dokumenty (např. naskenované doklady), informujte PČR

Obnovení

- Pevný disk z napadeného zařízení připojte k jinému počítači (např. přes USB):
  - Pokud nemáte zálohu:
    - zkopírujte dokumenty a/nebo konfigurační soubory k programům a logy (mohou sloužit k zjištění způsobu útoku).
- Vymažte disk specializovaným softwarem (nespoléhejte se jen na formátování).
- Nainstalujte operační systém z důvěryhodného zdroje (např. originální nosič) a veškeré dostupné aktualizace.
- Nepoužívejte k obnovení kompletní zálohu disku, může obsahovat škodlivý software!