# 10 Immediate Actions When Experiencing Cyber Attack

barricade cyber solutions

**01** Disconnect the infected devices' NICs from the network.

**02** Disconnect Network Internet connectivity (including wireless).

**03** Separate backups from the network and write protect where possible.

**04** If you have cloud backups, log in from a location other than your company systems and change the credentials.

**05** Disconnect switches to prevent continued or the beginning of lateral infections.

**06** Call us 24x7x365 from a phone not associated with your firm. We can immediately begin to guide you through the proper response.

**07** We recommend you DO NOT shut down a device that is known to be in the process of encryption. You may corrupt the OS or other applications and make recovery using the keys impossible.

**08** DO NOT communicate on the network, company related email, IP phones, Teams, Slack, etc., as they are OFTEN listening to, and/or reading your communications. You also cannot take back anything said to employees, partners, etc., in writing or verbally.

**09** You should consult a lawyer known as breach council before messaging anyone not a decision-making executive or staff/service providers critical to your recovery, as this is often as much a legal issue as it is a technical emergency.

**10** DO NOT communicate with the threat actor until you have the support you need. This can create issues and start a timer. Having the right negotiator can have a massive impact on the results, so don't rush to settle.

barricadecyber.com

**Give us a call at (843) 419-8284 for 24x7 after-hours support**