

Credential Security Best Practices for Your MSP

<https://campus.barracuda.com/doc/86545695/>

This section provides the best practices for credential security.

In today's environment, end-customers are being targeted and infected with ransomware through their MSPs. As MSPs often hold the keys to their customers' environment, MSPs have an enormous responsibility to be vigilant about securing their credentials to ensure attackers cannot exploit customers through this type of access.

To help you strengthen your credential security, Barracuda MSP encourage you to adhere to the following best practices:

- [Review access to MSP tools](#)
- [Enforce a strong password policy](#)
- [Use two-factor authentication](#)
- [Store passwords securely](#)
- [Review user roles](#)

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.