Phishing Website Allowlisting - Introduction

GrintOps invests significant effort into ensuring our phishing websites work without issue. However, depending on the security tools in use, specific issues may arise when attempting to use our phishing websites for simulated phishing purposes.

In the list below, we outline some of the security solutions that may be in-use and whether any allowlisting is needed:

- Google Safe Browsing: **No action required**
- Microsoft Smart Screen: **No action required**
- Microsoft Defender for Endpoint (Web Protection): **Allowlisting required**
- McAfee/Trellix Web Control: **No action required**
- Palo Alto Networks PAN-OS And Prisma Access: **Allowlisting required**
- Sophos Web Protection: **Allowlisting required**
- Cisco Umbrella: **Allowlisting required**
- Fortinet FortiGate: **Allowlisting required**
- VIPRE Endpoint Security: **Allowlisting recommended**

If you're using a web filtering solution outside those listed above, and you're experiencing issues, please **contact the GrintOps team**.

Revision #3
Created 29 July 2025 14:55:36 by Admin
Updated 29 July 2025 16:29:24 by Admin