How to Use Malwarebytes Breach Remediation

Malwarebytes Breach Remediation does not prevent malware from being installed on a computer. Following safe computing practices continues to be the best way to safeguard computers and data from malicious attacks. Regularly running Malwarebytes Breach Remediation to scan for malware is a safe computing practice. If you notice that your computer’s performance is sluggish or you suspect that your computer’s security has been compromised by malware, Client Services recommends that you use Malwarebytes Breach Remediation to scan your computer immediately.

To scan your computer for malware do the following.

1. Print these instructions
2. Close all open programs
3. Select the Windows start button
4. Navigate to All Programs > Malwarebytes Breach Remediation
5. Select one of the scan options:

   **Malwarebytes Anti-Rootkit** – A quick scan that includes anti-rootkit scanner functionality during the scan. Any rootkits or other identified threats will be quarantined.

   **Malwarebytes Full Scan** – A thorough, lengthier scan of the entire computer that includes anti-rootkit scanner functionality. Any rootkits or other identified threats will be quarantined.

   **Malwarebytes Quick Scan** – A quicker, shorter scan that examines computer hotspots for malware without analyzing the entire computer. Any threats found will be quarantined.
6. Please wait as scanning commences through the following stages:

Stage One: Product key registration

![Product key registration screenshot]

*Product key registered successfully*
Stage Two: Product update

Stage Three: Scanning
Stage Four: Output is generated

7. Once the scan completes, press any key to continue
8. Restart your computer