# Protecting Against Potential Russian Cyber-Attacks

## Guidance for U.S. State, Local, Tribal, and Territorial (SLTT) Entities

<table>
<thead>
<tr>
<th>What You Should Do Today</th>
<th>Join the Multi-State Information Sharing &amp; Analysis Center® (MS-ISAC®) or Elections Infrastructure Information Sharing &amp; Analysis Center® (EI-ISAC®).</th>
</tr>
</thead>
<tbody>
<tr>
<td>What You Should Do Tomorrow</td>
<td>Stop malicious internet activity with a Malicious Domain Blocking and Reporting (MDBR) service provided by the MS- and EI-ISAC.</td>
</tr>
<tr>
<td>What You Should Do in the Next Week</td>
<td>Turn on multi-factor authentication (MFA) for any system that offers it. Obtain a recent vulnerability scan of externally facing IT assets and install all possible patches and updates.</td>
</tr>
<tr>
<td>What You Should Do in the Next Two Weeks</td>
<td>Enable logging on any device that is capable and configure a log collection system.</td>
</tr>
</tbody>
</table>
| What's Next | If you’ve already completed the suggestions above, here are two other important recommendations:  
  - Develop or update an incident response (IR) plan.  
  - Ensure systems are properly backed up and backups are protected from ransomware attacks. |

## Contact

The MS-ISAC Security Operations Center (SOC) is available 24×7×365 to assist via phone or email.

- **Phone:** 866-787-4722
- **Email:** soc@msisac.org

To learn more and get further details on level of effort, guidance, and cost, visit our website: [https://www.cisecurity.org/russian-cyber-attacks](https://www.cisecurity.org/russian-cyber-attacks)

## Additional Resources

For resources from our colleagues at CISA, please also see their [Shields Up](https://www.shieldsup.gov) webpage.