Geauga County Automatic Data Processing Board
Department of Advanced Research and Cybersecurity [DARC]
Charles E. Walder, Chief Administrator

Request to Remove Blocked Domain or Email Accounts on the Geauga County Email System

Please complete this form to request the removal of a block on a domain or email account within the Geauga County Email System. Such blocks may be implemented if one or more Geauga County users receive a phishing or other malicious email, or if our security systems, staff, or external sources identify a compromise. In these cases, Geauga County takes proactive steps to protect our network by blocking the affected email account or domain to prevent further incidents.

If the compromise has been remediated and you wish to have the block removed, please fill out the form below and send per ADP staff's instructions.

Domain or Email Address requesting to have block removed _____

Name of Organization _____

Was Internal IT or External IT used to perform the remediation? ☐ Internal ☐ External

If External, Business Name? _____

Has the Compromised Account(s) been remediated? ☐ Yes ☐ No

Has the user's password been changed? ☐ Yes ☐ No

Has the user been forcibly signed out of all active sessions to ensure re-authentication is required (e.g., using 'Sign out of all sessions' in Entra ID, or similar actions)?" ☐ Yes ☐ No

Was Multi-Factor Authentication enabled on the account prior to the security incident? ☐ Yes ☐ No

If YES, how was the attacker able to bypass? _____

If NO, has MFA been enabled now? ☐ Yes ☐ No

Has the account been properly reviewed (access logs, audit logs, etc.) to know what the attacker accessed or made changes to? (This should include areas the account would have had access such SharePoint, OneDrive, SSO applications, etc.) ☐ Yes ☐ No

If YES, have those changes been undone/cleaned up to prevent possible persistence, hosting of malicious files, or any type of continual activity by the attacker? ☐ Yes ☐ No

Has the user's email been reviewed for any forwarding or other rule changes and have any changes made by the attacker to the email account been undone/cleaned up? ☐ Yes ☐ No

Has the affected workstation or device been thoroughly scanned and remediated using security tools, reimaged with a fresh OS install, or taken out of service? If other steps were taken, please specify. ☐ Yes ☐ No

_____

Has it been confirmed no other users are currently compromised? (All accounts should be reviewed using IOCs gathered from the incident to review other possible malicious activity) ☐ Yes ☐ No

What policies, procedures, security tools, or other factors have you implemented in order to mitigate potential future incidents?_____

_____

Please explain cause of the incident, remediation performed and any other relevant details:

_____

_____

_____

_____

On the lines below, please provide Information/IOCs gathered from the security incident. ADP may use the data provided in its security configuration in order to help protect the Geauga County Network.

Phishing Email Address _____

Phishing Email IP address _____

Phishing URL(s) _____

Additional Information/IOCs

_____

_____

_____

*If possible, please attach a screenshot of the phishing email received, as well as screenshots of any attachments or sites where the Phishing URL takes you (please make sure to acquire this safely, using a sandbox or other security tool). Do not forward us the actual phishing email or actual phishing attachments or links unless otherwise directed.

**If possible, please include an attachment of any hashes gathered for malicious files with descriptions for each hash.

***ADP welcomes any additional shared information beyond what is required in this form, including details about the incident, IOCs, hashes, etc. Information Security is at is strongest when we share data that can be used to help protect others.

Please note that incomplete data or unsatisfactory remediation may result in processing delays or request denials. ADP Staff may request additional information about the incident or may require incomplete or unsatisfactory forms to be completed again.

Name_____ Position/Title_____

Signature_____ Date_____

Data Center Use Only:

Date Received: _____ Processed by: _____ INC#: _____