RCC-E Defensive Cyber Operations Division
REPORTING PHISHING ATTEMPTS

If you receive a suspicious e-mail:

- **DO NOT** reply to the message
- **DO NOT** follow its instructions
- **DO NOT** forward to another recipient
- **DO NOT** access any embedded links or attachments (clicking on or copying links from e-mail to browser)

***If you did not interact with the suspicious e-mail, follow the instructions in the BLUE section.**

Please report any suspected Phishing e-mails to RCC-E DCOD for analysis via the following method:

1. Single click to highlight the Phishing E-mail within the Messages List in Outlook
2. Go to 'File' – 'Save As' – 'Outlook Message Format' – 'Unicode (*.msg)' and Save **(See NOTE Below)**
3. Create a new e-mail
   a. Attach a copy of the saved phishing e-mail
   b. Add the <Subject Line> "Phishing E-mail Submission"
   c. Send the e-mail to usarmy.wiesbaden.rcc-e.mbx.phishing-reporting-dcod@army.mil
4. Permanently delete the phishing e-mail by highlighting it and pressing Shift+Delete

NOTE: OWA users must right-click suspicious e-mail and select 'Forward as Attachment' to create .eml file

No further action is required on your part. When in doubt, please submit the e-mail!

***If you interacted with the suspicious e-mail, please follow the instructions in the RED section.**

If you mistakenly interact with the suspicious e-mail by ***taking any actions such as: replying, forwarding, following its instructions, opening attachments, accessing links, etc.*** OR ***receive a specifically addressed phishing e-mail*** (e.g. one directly targeting you or your organization, aka Spear Phishing), submit the e-mail message for analysis by taking the following actions:

1. Immediately contact unit (local) Information Security System Manager (ISSM) to report possible incident
2. Ensure ISSM contacts 119/AESD to create an ITSM trouble ticket
3. AESD personnel will assist you in creating the ticket and properly preserving the suspicious e-mail message
4. After completion of the above steps, **DISCONNECT** the system from the network

RCC-E DCOD needs your assistance when combating phishing attacks. The sooner information related to the occurrence is shared, the more efficient the cybersecurity community can mitigate potential vulnerabilities or exploits. Feel free to contact RCC-E DCOD at any time with questions or concerns regarding phishing attempts:

DSN: 314.565.6333 **Comm**: +49(0)611.143.565.6333 **NIPR:** usarmy.wiesbaden.rcc-e.mbx.dco-d@army.mil