

# CIRT Playbook Battle Card: GSPBC-1008 - Money Mule Scams - CEO Fraud

(P) Preparation	(I) Identification	(C) Containment
<ol style="list-style-type: none"> <li>1. Perform routine inspections of controls/weapons</li> <li>2. Perform routine phishing education</li> <li>3. Conduct phishing simulations</li> <li>4. Establish procedures for verifying requested financial transactions out of band</li> <li>5. Log incoming and outgoing emails</li> <li>6. Establish a method for users to report suspicious emails</li> </ol>	<ol style="list-style-type: none"> <li>1. Monitor for:               <ol style="list-style-type: none"> <li>a. Emails with suspicious attachments</li> <li>b. Multiple identical emails sent from unknown sources</li> <li>c. Emails sent from typo domains</li> <li>d. Emails that fail SPF and/or DKIM</li> </ol> </li> <li>2. Investigate and clear ALL alerts associated with the impacted assets</li> </ol>	<ol style="list-style-type: none"> <li>1. Inventory (enumerate &amp; assess)</li> <li>2. Detect   Deny   Disrupt   Degrade   Deceive   Destroy</li> <li>3. Observe -&gt; Orient -&gt; Decide -&gt; Act</li> <li>4. Issue perimeter enforcement for known threat actor locations</li> <li>5. Review email logs to identify other affected users</li> <li>6. Review relevant financial transactions</li> </ol>
(E) Eradication	(R) Recovery	(L) Lessons/Opportunities
<ol style="list-style-type: none"> <li>1. Contact financial institutions to halt/reverse transactions</li> </ol>	<ol style="list-style-type: none"> <li>1. Blacklist sources of phishing emails               <ol style="list-style-type: none"> <li>a. Individual sending email addresses</li> <li>b. Entire sending domain, if appropriate</li> </ol> </li> <li>2. Report the incident to the appropriate law enforcement agency</li> </ol>	<ol style="list-style-type: none"> <li>1. Perform routine cyber hygiene due diligence</li> <li>2. Engage external cybersecurity-as-a-service providers and response professionals</li> </ol> <div data-bbox="1392 954 2043 1079"> <p>Notes:</p> <ol style="list-style-type: none"> <li>1. Report cybercrime:  <a href="https://www.ic3.gov/default.aspx">https://www.ic3.gov/default.aspx</a> </li> </ol> </div>