predica.

Phishing Incident Response Plan

SOC Team

- Locate all malicious mails and enforce deletion of them.
- Block end-user from sending mails.
- Send mail to IT Security Contact requesting to perform trigger remediation actions as follows:

Service Desk

- Block end user's sign-in for the time of the investigation.
- Perform a password reset and pass the password to either IT Security Contact or end user's manager.

- Remove suspicious inbox rules/forms/forwarding addresses using PowerShell.
- Enforce MFA on end-user on all devices and platforms.
- Remove assigned administrative roles for a grace period.

Service Desk

Unblock the sign-in.

IT Team

Scan end-user's PC.

- Unblock users from sending mails.
- Consult with IT Security Contact the IP list and block all suspicious addresses.

IT Security

- Request mandatory security training for end-user to raise awareness.

Follow us