GSD. - Reported scam attempt

Article ID: KB0039863
Created: 2024-12-19 14:03:42
Updated: 2024-12-19 14:03:42
Author: {'link': 'https://fmcnadev.service-now.com/api/now/table/sys_user/acaf843397d74958f7e3bb8fe153afe3', 'value': 'acaf843397d74958f7e3bb8fe153afe3'}
Category: {'link': 'https://fmcnadev.service-now.com/api/now/table/kb_category/b513d404c3ca1a100acd3300150131fb', 'value': 'b513d404c3ca1a100acd3300150131fb'}

General Information:

Possible symptoms/errors:

User calls to report a potentially successful scam attempt via phone

Alternative names of the system:

N/A

IMPORTANT NOTICE:

Priority of incidents related to scams can be no lower than P3Always begin handling scam attempts by resetting user's Active Directory password.

Solution:

1. Reset the user's Active Directory password. Follow GSD. Windows - AD User Account Password Reset (KB0016151)

2. Create an incident containing all available information regarding the scam attempt:

What were the details of the attempt? What was the user told/presented with?Has the user provided any data/downloaded or installed any software/clicked on any links?Any related e-mails or phone numbersContact information of the userTime of the attempt

Assign the incident to Int_WW_CyberThreatDetection_SecaaS_SLS_FDT and send an email to CERT@Fresenius.com containing the ticket number and all relevant information.

Assignment Group:

Int_WW_CyberThreatDetection_SecaaS_SLS_FDTCERT@Fresenius.com

Ticket Creation:

Template: N/ACategorization:

Configuration Item: N/ACategory: N/ASubcategory: N/A

Important Links:

N/A