Webinar Questions and Answers

Reportable Unclassified Cyber Events

Webinar guests submitted several questions before and during the December 13 *Reportable Unclassified Cyber Events* session. The following responses are provided by the Defense Security Service (DSS) Counterintelligence (CI) directorate.

Question: Are requests to join social networking sites, like LinkedIn, from unknown requesters reportable as Suspicious Contract Reports (SCRs)?

Answer: In cases where an individual receives an invitation from a Social Networking Site (SNS) from an unknown sender, or even from a known sender, it may be reportable. If there is anything that causes suspicion regarding a SNS invitation, please report that to your local supporting security or CI representative. From SNS or from any other source, DSS wants reported as SCRs any attempt to establish a relationship, where that request may come from a foreigner, or from anyone who indicates they are interested in pursuing a relationship, particularly when the requester demonstrates that their interest is based on a cleared employee's access to classified information or based on the employee's position within a cleared contracting firm. Some SNS "friending" requests will be from random contacts and may not represent a cause for CI concern. In other cases, people do receive requests to link up over an SNS with individuals, perhaps foreign individuals, with whom a cleared employee may have been associated with before, perhaps on an international project. In those cases, or in any cases where there is a concern that you are being targeted based on your position or access, please report these. And, keep in mind, anything you put on a SNS for public view is there for our adversaries to see and they may use that information to target you.

Question: You mentioned that some phishing emails, like the bank scam, are technically spam and need not be reported. Are there any cases where a phishing email should be reported as a SCR?

Answer: Yes. In this case, you should apply the principles I discussed to determine if this is something that was sent in bulk to a wide audience or if this could possibly be something that is targeted to your firm. A phishing email that is apparently targeted to your firm, that asks for specific information about your firm, or that claims to have been approved or requested by your firm (when in fact has not been approved) should be reported. A phishing email that is generic in nature and appears to be an attempt to potentially commit financial fraud should not be reported to DSS.

Question: The instructions for uploading potentially malicious files are fairly complicated. Is there any way I can receive more information on this process.

Answer: Yes, they are complicated, but after inputting a few files into the system, it should become easier. If you need any further instruction on these procedures, please contact your supporting security or CI representative and he or she will be happy to walk you through this process to ensure that malicious files are properly put into the Safe Access File Exchange (SAFE) system. Further details for uploading the header/footer information are provided in the webinar attachment.

Question: Do you have any tips for recognizing and/or dealing with spoofed email addresses or domain names in an email address?

Answer: Some companies are able to block all external email that is (illicitly) using their domain address. If this can be done, it should cut down on spoofed emails you may receive. DSS is interested in reports of spear phishing emails that use this technique, so if those emails are blocked, it would deny the ability to collect, categorize, and respond to those threats.

If you receive spoofed emails in which the sender is using your email domain and the ability is there to look at that email and make an assessment as to whether the email is part of a spear phishing effort, that would be encouraged. However, spammers sometimes use the tactic of spoofing domain names to make the item appear to have come from within your domain. In cases such as these, it is recommended that you use the techniques discussed in today's webinar to determine if the item looks like it has been sent in bulk or if it is generic in nature. If either of those two criteria are met, the item is likely to be spam. If it looks like they are trying to get specific information or ask you to open an attachment when appearing to specifically target you or your firm, it should be reported as a possible CI concern.

Question: Does the National Industrial Security Operating Manual (NISPOM) require emails set aside as spam from company filtering software to be reviewed for possible CI interest?

Answer: This is a very good question. DSS appreciates industry's vigilance to educate its workforce to be alert to and report suspicious emails. However, some suspicious emails may be redirected, perhaps by corporate IT security procedures, do not actually arrive in someone's inbox, and may go unreported.

Some of the best Suspicious Contact Reports (SCRs) come from savvy IT or other industry professionals who scan emails that are set aside as spam, and occasionally find items of concern sent to the spam folder. The NISPOM does require cleared industry to report suspicious items, however, it is often difficult to address each item that is automatically sent to a junk or spam folder.

As emphasized in today's webinar, DSS wants to make it easier for industry to satisfy NISPOM reporting requirements by making it clear that if an item can be positively identified as spam, it

need not be reported. It is always best to err on the side of caution and report items if you cannot positively determine that they are spam. If through minimal review it is obvious that your email is spam, then your efforts can stop there. One suggestion on how to spot check would be to scan the emails set aside as spam for any indication of spoofing or spear phishing email. Such a scan, done on a periodic basis, should go relatively quickly. And, if there is the ability to review emails set aside for any indication that these emails contain direct requests for information or your products or services, and they otherwise meet the email SCR reporting criteria discussed today, those would be reportable as SCRs.

Question: Are requests through personal accounts reportable, or must they be through work email?

Answer: If you ever receive any cyber-related item to one of your personal accounts (be it email, social networking, dating sites, professional forums, etc.) that gives you any cause for concern, definitely report those. Some of the most concerning cyber events occur over personal links to the Internet. Our adversaries have been known to look for individuals who may have access to proprietary or classified information and target them through their personal accounts. DSS is concerned with what you may receive over your company systems, as well as with those suspicious items that come over your personal accounts.

Today's presentation focused on the most common types of SCRs reported to DSS. We could probably fill another session entirely with threats that you may see over social networking sites. If you ever have indication that you are potentially being targeted by a cyber entity for your knowledge or based on your position of trust within your company, these are tipoffs that need to be reported. Remember, our adversaries are adept at finding out information on you that they can then use to exploit you online. Don't get sucked in by individuals who contact you online and make false claims about their identity; they may be adversaries who can use your available information to attempt to establish a relationship with you. Be particularly wary of such contacts that may come from overseas, and definitely report those.