

Student Guide

Short: Suspicious Emails

Objective	Determine whether an email is suspicious based on warning signs and determine the correct action to take if the email is suspicious.
POC	counterintelligence.Training@dss.mil
Estimated completion time	15 minutes

Introduction

Our nation's economic stability and national security are under attack. More and more, industrial spies are turning away from conventional methods and using a less risky and more successful approach.

Security professionals call them direct request emails. By sending email directly to employees, spies attempt to purchase sensitive technology legitimately. Once in possession of sensitive components, they can reverse engineer the technology in order to sell it for less than U.S. companies due to the fact that they save money by not spending on research and development. Defense contractors are often the targets of these attempts and when foreign countries use this approach, they may not only reverse engineer the technology to sell, they may also utilize the component itself, further endangering national security. As a cleared employee or a facility security officer of a defense contractor, you too could be the target of a direct request email.

If you received a suspicious email, would you know what to do?

Types of Suspicious Emails

In order to identify suspicious emails it will help to know about their origins. Suspicious emails may come from anywhere in the world. They may come directly from the foreign country that intends to use the requested item, or they may come from a third party foreign country. Suspicious emails may even come from a front company located in the United States.

Direct Request

Direct request emails come directly from the foreign country that intends to use the item but are often altered in order to disguise the actual end use or end user. Senders hope that the email will appear legitimate and the U.S. company will overlook any discrepancies.

Third Party Request

Third party request emails use purchasers located outside of the requesting country. Senders hope that the third party will complete a transaction with the U.S. company and then illegally ship the items to the end using country.

Domestic Front Company Request

Domestic front company request emails use or co-opt established purchasing entities in the United States. By purchasing within the U.S. and then shipping the items illegally, senders hope to avoid export controls.

Suspicious Email Elements

Regardless of where the email originates, there are several red flags that can help you tell the difference between a suspicious email and a non-suspicious email. First, remember that in order to be considered suspicious an email must mention an export controlled or classified item. If export controlled or classified items are included then there are several questions you should ask yourself:

- Does the email discuss export controls?
- Is there anything suspicious about the requestor?
- Is there anything suspicious about the specified end use?

Does the email discuss export controls?

All suspicious emails discuss export controlled or classified items, but some emails may also acknowledge the export control policies themselves. By acknowledging export controls, or indicating expertise in dealing with them, senders hope to create an impression of legitimacy. In addition, suspicious emails may also ask for an unusual means of delivery or a rapid decision time.

Sample:

From: John Smith [johnsmith@aerosolutions.net]

Subject: Business Venture

To whom it may concern:

We want to buy **an export controlled military communications system** {Discussion of export controlled or classified items}, both Model 123 and Model 124. **I know you have export control for some sensitive technology products** {Acknowledgement of export controls}, so can we **submit an end-user-statement for the export permit** {Knowledge of export requirements}? **Please respond immediately – we need the technology right away** {Requests for unusual or rapid delivery}.

John Smith

AeroSolutions Inc

- Discussion of export controlled or classified items
Remember, in order to be considered suspicious, the email must request an export controlled or classified item.
- Acknowledgement of export controls
WHAT: For direct requests and third party requests, it is common for the requestor to state they know the requested item is export controlled.

WHY: Requestors do this to create the impression that they are knowledgeable and legitimate.

- Knowledge of export requirements

WHAT: Suspicious requestors often include a statement expressing their knowledge of export requirements.

WHY: Requestors do this to create the impression that they are knowledgeable and legitimate.

- Requests for unusual or rapid delivery

WHAT: The suspicious requestor will often suggest an unusual means of delivery or will request a rapid decision concerning the sale.

WHY: Business transactions typically follow a standard process and require time to make decisions. If a potential customer suggests that you vary from your standard process, beware.

Is there anything suspicious about the requestor?

Sometimes information about the requestor may raise a concern. Suspicious requests often come from previously unknown companies. Requestors may use a generic email address or indicate that they are a parts procurer located in a foreign country. In addition, poor grammar and other language errors may also raise a red flag. Alone, each of these elements might not warrant attention, but when considered along with the other suspicious elements, there's cause for concern.

Sample:

From: John Smith [**johnsmith@gmail.com**] {A generic email address}

Subject: Export Controlled Ultrasonic Emitter

Hello,

I am John Smith and manager of an **agency to purchase military communications items and accessories in COUNTRY X** {A foreign country}.

We are interested in purchasing an export controlled ultrasonic emitter from you company.

Hope to receive you answers {Grammatical errors}.

Good Day!

John Smith

New Customer Co.,LTD {An unknown company or new customer}

- An unknown customer or new customer
WHAT: The suspicious requestor is often a previously unknown company or one that has not previously completed a sale.

WHY: First time requestors might not always raise a red flag, but it's best to be on alert, especially if you've already noted other suspicious elements.
- A generic email address
WHAT: The individual requestor does not have an email address with the requesting company's name.

WHY: While there are legitimate reasons for this, it also provides a level of anonymity to the requestor and this should raise concerns.
- A foreign country
WHAT: Most frequently, suspicious emails come from a parts procurer located in a foreign country which claims to represent a country on the National Security Threat List.

WHY: Remember that direct request and third party request emails are sent from foreign countries. You should always be wary of unfamiliar foreign parts procurers.

- Grammatical errors

WHAT: Often times a suspicious email is full of bad grammar and misspellings.

WHY: Because they often come from foreign countries, English is not the requestor's primary language. While an error or two is understandable, anything more should raise concerns.

Is there anything suspicious about the specified end use?

Some warning signs relate to the end use of items specified in a suspicious email. Requestors may specify a non-specific or benign end user, and they may also deny any military application. Requestors make these claims in order to ease concerns over the potential use of the requested item.

Sample:

From: John Smith [johnsmith@globestandard.net]

Subject: Product Info Request

Sales Representative,

I am John Smith and my company wishes to buy an export controlled laser technology **for use in university experiments** {Non-specific or benign end user}. I'm sure this is **not for army or official use** {Denial of military application}

Please respond.

Sincerely,

John Smith

Global Standards

- Non-specific or Benign End User

WHAT: Requestors often avoid identifying the end user by name. Instead, they use vague terms (i.e. university, institute, lab, etc).

WHY: Requestors do this to ease any concerns the defense contractor might have. It is easy for the requestor to identify a specific institution once interest has been expressed in making a sale.

- Denial of Military Application

WHAT: Requestors often specify that the end user has no military connections.

WHY: Requestors do this to increase legitimacy by creating the appearance of a benign end user.

Consequences of Actions

So what should you do if you think you've received a suspicious email? As with any email, there are a number of actions you could take. You could respond to it. You could also delete it. However, there is really only one correct action to take, and that is to report it. The action you take has repercussions for the economy and national security.

Reply

When you reply to a suspicious email, your organization begins a journey that may eventually lead to monetary loss or a compromise of national security. If an email seems suspicious to you, don't reply to it.

Delete

When you delete a suspicious email, you're not eliminating the problem. Instead you're failing to provide DSS with information that could help them piece together the big picture and determine who is targeting U.S. companies. If you received a suspicious email, the odds are high that several other companies were also targeted. If an email seems suspicious to you, don't just delete it.

Report

When you report a suspicious email, you're taking an active role in stopping those responsible. You do this by providing DSS with information that can help them piece together the big picture, which in turn helps them provide adequate information to the intelligence community, the FBI, and Homeland Security. As a general rule of thumb, if you're in doubt about an email, report it to your Industrial Security Representative.

Practice Activity

You work at Overlook Enterprises, a defense contractor that produces several export-controlled items. Because you have just learned how to recognize suspicious direct-request emails, you will help three coworkers, who have received emails that may or may not be suspicious, decide what to do with their email.

Use the following resource about Overlook Enterprises to assist you in making your determinations:

Customers:

- Blume-Fischer-Cross
- Bradshaw Mitchell Avionics
- Gray Matter, LLC
- Kanuk Industries

Export Controlled Items:

- KII-0444-17 Global Positioning Satellite System Simulator
- KII-0444-26 Unmanned Airship Gimbal
- KII-0444-44 Infrared Sensor
- KII-0521-51 Ultrasonic Range Finder
- KII-0543-08 Bias Controller
- KII-0593-21 Radiation Hardened Programmable Read Only Memory

Countries on the National Security Threat List:

- Country X
- Country Y
- Country Z
- Country Purple
- Country Orange

Email 1

From: Susan Smith [mailto:susansmith@brightpath.com]

Subject: Quote Request KII-0444-44

Hi,

Thanks for the information. The technical supported information is not mentioned in case we have questions about the controller and the evaluation kit.

We are thinking of buying the KII-0444-44 infrared sensor. It is very likely that Brightpath ships products to a foreign country but we have the required export permits. Please confirm if this is ok or do you have agency or distributors in the country already.

Regard
Susan Smith
Brightpath Technology LLC
Newport News, VA 23602
Tel - 757.555.1234

What should you do with this email? Select an action.

- Reply
- Delete
- Report

Email 2

From: Thomas Edwards [mailto:thomas.edwards@bradshawmitchell.com]

Subject: Quote Request KII-0421-49

Greetings,

This year is shaping up to be a good one for Bradshaw-Mitchell. In conjunction with a contract we are hoping to win, we need an estimate for part KII-0421-49. If you would, please send us a preliminary estimate for 25 of these items so that we may include it in our proposal.

I look forward to hearing from you.

Regards,
Tom Edwards
Contracts Officer
Bradshaw-Mitchell Avionics
San Diego, CA 92101

What should you do with this email? Select an action.

- Reply
- Delete
- Report

Email 3

From: Peter centricspace

Subject: Re: buy this product-Program Read Only Memory – 5V

Good Morning!

First of all, pls let me introduce myself and our company, this is peter from Centricspace International Group Ltd, Head Office in Country Z, Branch Office in Country Purple. Now we have a client who want to buy ur product, in other words, 32K*8 Radiation Hardened Programmable Read Only Memory. We know of export control and are able to get the needed permits for the transaction.

I wander if your company have stock for them,and could u tell me how many do I buy for them?

ur sincerely,peter
www.centricspace.com
Tel: 86-10-67726085
Email: sales@centricspace.com
MSN:peter_chang0426@hotmail.com

What should you do with this email? Select an action.

- Reply
- Delete
- Report

Summary

The next time you get an email that seems suspicious, remember, the decisions you and your colleagues make have a real impact on the economy and on national security.

When you reply to a suspicious email, you open the door to potential revenue loss as a result of industrial espionage. On a larger scale, it could result in the compromise of national security. Suspicious email should be reported.

When you choose to delete a suspicious email, it does not ensure that the emails will stop. In order to stop the potential threat, you must report suspicious emails to DSS so that DSS can piece together the bigger picture.

When you choose to report suspicious emails, you're doing your part to prevent industrial espionage and protect national security.

Answer Key

Email 1

From: Susan Smith [mailto:susansmith@brightpath.com]

Subject: Quote Request KII-0444-44

Hi,

Thanks for the information. The technical supported information is not mentioned in case we have questions about the controller and the evaluation kit.

We are thinking of buying the **KII-0444-44 infrared sensor** {Export controlled or classified item}.

It is very likely that Brightpath ships products to a **foreign country** {Foreign country} but we have the **required export permits** {Knowledge of export requirements}. Please confirm if this is ok or do you have agency or distributors in the country already.

Regard

Susan Smith

Brightpath Technology LLC {An unknown or first time customer}

Newport News, VA 23602

Tel - 757.555.1234

You should have REPORTED the email. Remember, when you choose to report suspicious emails, you're doing your part to prevent industrial espionage and protect national security.

Email 2

From: Thomas Edwards [mailto: thomas.edwards@bradshawmitchell.com]

Subject: Quote Request KII-0421-49

Greetings,

This year is shaping up to be a good one for Bradshaw-Mitchell. In conjunction with a contract we are hoping to win, we need an estimate for part KII-0421-49. If you would, please send us a preliminary estimate for 25 of these items so that we may include it in our proposal.

I look forward to hearing from you.

Regards,
Tom Edwards
Contracts Officer
Bradshaw-Mitchell Avionics
San Diego, CA 92101

Because the sender is an established customer and the email does not reference an export controlled item, it is not suspicious. Therefore, you could have selected to Delete or Reply to the email. Although it is not a suspicious email, you could have also selected Report, because when in doubt about an email, report it to DSS.

Email 3

From: Peter centricspace

Subject: Re: buy this product-Program Read Only Memory – 5V

Good Morning!

First of all, pls let me introduce myself and our company, this is peter from Centricspace International Group Ltd, Head Office in **Country Z** {Foreign country}, Branch Office in **Country Purple** {Foreign country}. Now we have a client who want to buy ur product, in other words, 32K*8 **Radiation Hardened Programmable Read Only Memory**. We **know of export control** {Export controlled or classified item} and are able to get the needed **permits** {Knowledge of export requirements} for the transaction.

I wander if your company have stock for them,and could u tell me how many do I buy for them?

ur sincerely,peter

www.centricspace.com

Tel: 86-10-67726085

Email: sales@centricspace.com

MSN:peter_chang0426@hotmail.com {A generic email address}

You should have REPORTED the email. Remember, when you choose to report suspicious emails, you're doing your part to prevent industrial espionage and protect national security.