Suspicious Emails Short
Student Guide

February 2024

Center for Development of Security Excellence

Contents

Welcome

The Colonial Pipeline is one of the largest oil pipelines in the U.S. It spans 5,500 miles and transports oil along the East Coast. In May 2021, it was the target of one of the largest cyberattacks on critical infrastructure. The attack caused gas shortages, raised gas prices at the pump, and caused some states to declare an emergency. The attackers gained access to the pipeline's information systems in part using suspicious emails.

The incident highlighted how cyber threats can have far-reaching consequences, disrupting essential services and causing significant financial losses. If you received a suspicious email, would you know what to do?

Welcome to the Suspicious Emails Short. This Short will familiarize you with warning signs that an email is suspicious and provide guidance on what to do if you suspect that something is not right.

Learning Outcome—

- Given an email, determine whether the email is suspicious based on warning signs and determine the correct action to take if the email is suspicious.

Where Do They Come From?

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.

Term	Definition
Front Company	A company or business entity that is established, used, or co-opted for an illicit purpose; wherein the management, control, influence, or criminal activities are being directed by a hidden or disguised individual or group.

Direct Request

Direct request emails come directly from a foreign country but are often altered 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

A front company is a business entity that is established, used, or co-opted for an illicit purpose. The management, control, influence, or criminal activities are directed by a hidden or disguised

individual or group. By purchasing within the U.S. and then shipping the items illegally, senders hope to avoid export controls.

What Are They Targeting?

Being aware of what adversaries want helps you protect you and your organization's information. Adversaries' targets include:

- International Traffic in Arms (ITAR), export controlled and critical technology, and controlled unclassified information (CUI)
- Information related to research and development
- Company unclassified networks, portals, commonly accessed websites, and search history
- Proprietary information, such as business strategy, financial information, human resources, and product data
- Administrative end user credentials including usernames, passwords, tokens, Virtual Private Network (VPN) data
- Patch update sequences and patterns to determine if the company uses a set date to update its systems

Term	Definition
ITAR	The International Traffic in Arms Regulations (ITAR) implements the provisions of the Arms Export Control Act (AECA) and controls the export and import of defense-related articles and services on the U.S. Munitions List.

Methods of Operation

Adversaries often follow distinct patterns or methods of operations to gain access to personnel, information, and technology. Being aware of these methods can help you protect against being a target. Methods include the attempted acquisition of technology – this includes attempts to acquire the equipment itself or diagrams, schematics, plans, and spec sheets; requests for information, also known as RFIs – that is, collecting protected information by directly or indirectly eliciting personnel for protected information and technology; and attempts to exploit commercial and business activities. This may be through existing relationships or by establishing new relationships through joint ventures, partnerships, mergers and acquisitions, or foreign military sales.

Another method is the exploitation of the supply chain. The supply chain may be compromised by the introduction of counterfeit or malicious products or materials with the intent to gain unauthorized access to protected data, alter data, disrupt operations, or interrupt communication.

Foreign intelligence entities or other adversaries may exploit cyber operations by compromising the confidentiality, integrity, or availability of targeted networks, applications, credentials, or data so they can access, manipulate, or exfiltrate personnel information or protected information and technology.

Finally, adversaries attempt to gain information through the exploitation of experts. This may be under the guise of peer or scientific board review of academic papers or presentations; requesting a consult with faculty members or subject matter experts; or attempting to invite or otherwise entice subject matter experts to travel abroad or consult for foreign entities. Cleared academia must be especially vigilant against this method.

Regardless of the specific method used by our adversaries, their goal is to gain and maintain access to our personnel, information, equipment, facilities, activities, operations, and networked systems.

Elements of Suspicious Emails

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, does the email mention an export controlled or classified item? Is there anything suspicious about the specified end use? *Alone*, each of these elements might not warrant attention – yet when considered along with *other* suspicious elements, there is cause for concern.

Let's take a closer look.

Mentions Export Controls or Classified Items

Suspicious emails may 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.

This sample email contains several warning signs.

From: Jane Doe [janedoe@aerosolutions.net]
Subject: Business Venture

To whom it may concern:

We want to buy a military communications system, both Model 123 and Model 124. I know you have export control for some sensitive technology products, so can we submit an end-user-statement for the export permit?

Please respond immediately – we need the techology right away.

Jane Doe
AeroSolutions Inc

Warning Sign	Explanation
"I know you have export control for some sensitive technology products…"	Acknowledgement of Export Controls For direct requests and third-party requests, it is common for the requestor to state they know the requested item is export controlled. Requestors do this to seem knowledgeable and legitimate.
"…submit an end-user statement for the export permit…"	Knowledge of Export Requirements Suspicious requestors often include a statement expressing their knowledge of export requirements. Requestors do this to create the impression that they are knowledgeable and legitimate.
"Please respond immediately – we need the techology right away."	Unusual Delivery Means or Request for Rapid Decision The suspicious requestor will often suggest an unusual means of delivery or will request a rapid decision concerning the sale. 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.

Suspicious 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.

This sample email contains several warning signs.

From: Jane Doe [janedoe@gmail.com]
Subject: Export Controlled Ultrasonic Emitter

Hello,

I am Jane Doe and manager of an agency to purchase military communications items and accessories in COUNTRY X.

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

Hope to receive you answers.

Good Day!

Jane Doe
New Customer Co.,LTD

Warning Sign	Explanation
[janedoe@gmail.com]	Generic Email Address The individual requestor does not have an email address with the requesting company's name. While there are legitimate reasons for this, it also provides some anonymity to the requestor and should raise concerns.
"…agency to purchase military communications items and accessories in COUNTRY X."	Foreign-Based Parts Procurer 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. Direct request and third-party request emails are sent from foreign countries. You should always be wary of unfamiliar foreign parts procurers.
"Hope to receive you answers."	Bad Grammar Often times a suspicious email is full of bad grammar and misspellings. 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.
New Customer Co.,LTD	First Time Requestor/New Customer The suspicious requestor is often a previously unknown company or one that has not previously completed a sale. First time requestors might not always raise a red flag, but it's best to be on alert, especially if there are other suspicious elements.

Suspicious 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.

This sample email contains several warning signs.

From: Jane Doe [janedoe@globestandard.net]
Subject: Product Info Request

Sales Representative,

I am Jane Doe and my company wishes to buy an export controlled laser technology for use in university experiments. I'm sure this is not for army or official use.

Please respond.

Sincerely,
Jane Doe
Global Standards

Warning Sign	Explanation
"…for use in university experiments…"	Non-specific or Benign End User Requestors often avoid identifying the end user by name. Instead, they use vague terms (i.e., university, institute, lab, etc.). Requestors do this to ease any concerns the cleared contractor might have. It is easy for the requestor to identify a specific institution once interest has been expressed in making a sale.
"…not for army or official use…"	Denial of Military Application Requestors often specify that the end user has no military connections. Requestors do this to increase legitimacy by creating the appearance of a benign end user.

Phishing

Phishing is a type of suspicious email we have all received at some point. Phishing emails contain many of the same elements of other suspicious emails, such as generic greetings and spelling errors, with the added element of embedded malicious content, links, or attachments.

Phishing uses email to deceive you. This deception may try to elicit personal information from you that can be used to steal your identity, or it may prompt you to click a link or download an attachment that can be used to gain access to your computer or network. The email usually claims to be from a business or organization that you deal with, exploiting the credibility of a legitimate entity. For example, phishers may pose as your internet service provider, credit card company, or bank. The message often says that you need to update or validate your account information. It might threaten some dire consequence if you don't respond, or it might promise you some type of reward, such as money, a trip, or electronics. The message directs you to a website that looks just like a legitimate organization's website but is not affiliated with the organization in any way.

Phishing Approaches

Hackers use several common approaches. For example, they may say they've noticed suspicious activity or login attempts or claim you have an account or payment issue. They may ask you to confirm personal or financial information or include an invoice that you don't recognize. Phishing emails will often request you to click on a link to make a payment or say you're eligible to register for a government refund. They may offer a coupon for free goods or services or claim information is needed for you to receive a payment. All of these things are common signs of a scam that you should not fall for.

In addition, hackers also use more targeted approaches. For example, they may target you using spear phishing. Spear phishing is a specialized attack against specific targets used to collect information or gain system access. Hackers learn the target's legitimate contacts – for example, your coworkers and associates, family members, organizations you belong to, and schools your children attend. They then send messages that appear to be from those contacts.

Hackers also use whaling to target high-value or senior personnel. The higher up you are in an organization, the more likely you are to be a target of spear phishing or whaling.

Protection Measures

There are several measures you can take to avoid being a victim of suspicious emails.

- Use security software to protect your computer.
- Use multi-factor authentication to protect your accounts.
- Protect your data by backing it up.
- Beware of links in email. Check to see if the link's address matches the link typed into the email by resting your mouse on the link *without* clicking on the link.
- Call before you click. Do not trust an official-looking communication. Assume it is malware until proven otherwise.
- Finally, consider using specialized email accounts. For example, use one account for work, one for friends, and one for online purchases. Having multiple accounts makes it more difficult for a hacker to gain access to your information.

Consequences of Actions

So, what should you *do* if you think you've received a suspicious email? There are a number of actions you could take. You could respond to it or open the link or attachment, if there is one. 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.

Open Link/Attachment

Opening a link or attachment in a suspicious email can have severe consequences. From identity theft to installing malware on your system, the consequences can be far reaching. Never open links or attachments in a message unless you are absolutely certain that the email is legitimate.

Delete

When you delete a suspicious email, you're not eliminating the problem. Instead, you're failing to provide information that could help piece together the bigger 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. The National Industrial Security Program Operating Manual (NISPOM) requires the reporting of suspicious contacts. If you suspect you or your company has been targeted with a suspicious email, whether it be via phishing or solicitation, report it immediately. Reporting allows the Defense Counterintelligence and Security Agency (DCSA) to share and address risks with other government and commercial sector partners.

Review Activity Introduction

Now that you know the types of suspicious emails, warning signs to look out for, and the consequences of your actions, it's time to apply that information.

You work at Overlook Enterprises, a cleared contractor that produces several exportcontrolled items. Because you have just learned how to recognize suspicious direct-request emails, you will help five coworkers who have received emails that may or may not be suspicious decide what to do. Review the email, and determine the appropriate action to take.

Several tools are available to assist you in making your determination. Use the provided list of your company's customers, a list of your company's export-controlled items, and the countries on the National Security Threat List. This list includes fictional countries for this training purpose.

Resource	List	
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	

Review Activity 1

Elaine Durham, Senior Engineer: Can you take a look at this email and help me determine if it's suspicious?

From: Petra cyberwatch

Subject: Re: Counter-UAV system

Good morning!

Pls let me introduce myself and our company, this is petra from CyberWatch Ltd, Head Office in Country Z, Branch Office in Country Purple. We are a cyber and IT company offering solutions for terrorism and security challenge. Now we have a client who want to buy ur counterUAV product. We knowof export control and are able to get the needed permits for the transaction.

I wander if your company have stock for them?

have a nice day!

best wishes to u and ur family!

ur sincerely,petra

www.cyberwatch.com

Tel: 86-10-67726085

Email: sales@centricspace.com

MSN:petra_song04@hotmail.com

Suspicious Element	Explanation
"Country Z" or "Country Purple"	Foreign Parts Procurer
"anti-UAV product"	Export Controlled Item
"know of export control"	Acknowledgement of Export Controls
"permits"	Knowledge of Export Controls
"MSN:petra_song04@hotmail.com"	Generic Email Address

Select the correct response.

- ○ Reply
- ○ Delete
- ○ Report

Review Activity 2

Dahlia Caine, Engineer and Associate Professor: I just received an email and I'm not sure whether to report it or not.

From: Carlos Moreno [mailto: cmoreno@learnalot.com]

Subject: Technical Review Request

Greetings,

We met last summer at the tech conference in Richmond. I very much enjoyed hearing about your research at the University. The following might be of interested to your research. Please take a look as soon as you are able. You can view it on this secure website: Technical Load Data Peer Review.

Respectfully

Carlos Moreno

LearnALot Technologies

Alexandria, VA 22304

Tel – 703.555.1234

Suspicious Element	Explanation
Technical Review Request	Academic solicitation
Technical Load Data Peer Review	Suspicious link
LearnALot Technologies	Unknown Sender

Select the correct response.

- ○ Reply
- ○ Open Link/Attachment
- ○ Delete
- ○ Report

Review Activity 3

David Surbrook, Project Manager: I just received an email and I'm not sure whether to report it or not.

From: Sarita Smith [mailto: sarita@brightpath.com]

Subject: Quote Request KII-0444-44

Hi,

Thanks for the information.

We are thinking of buying your radar surveillance system. 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

Sarita Smith

Brightpath Technology LLC

Newport News, VA 23602

Tel – 757.555.1234

Suspicious Element	Explanation
"radar surveillance system"	Export Controlled Item
"foreign country"	Non-specific End User
"required export permits"	Knowledge of Export Controls
"Brightpath Technology LLC"	First Time Customer

Select the correct response.

- ○ Reply
- ○ Delete
- ○ Report

Review Activity 4

Donald Joseph, Business Analyst: I'm not certain about this email. Can you take a look?

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

Select the correct response.

- ○ Reply
- ○ Delete
- ○ Report

Review Activity 5

Jack Jones, Project Manager: I just received an email and I'm not sure whether to report it or not.

From: May Chung [mailto: mchung@YourBank.com]

Subject: Account Compromise

Greetings

We detected suspicious activity on your checking account. Please verify your account activity immediately.

Review Account Activity

May Chung

Your Bank

Linthicum, MD 21601

Tel – 410.555.1234

Suspicious Element	Explanation
"Account Compromise"	Common phishing approach
"Review Account Activity"	Suspicious link
"Your Bank"	Phishing attempt spoofing the recipient's bank

Select the correct response.

- ○ Reply
- ○ Open Link/Attachment
- ○ Delete
- ○ Report

Conclusion

Congratulations on completing the Suspicious Emails Short! 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. You should now be able to determine whether the email is suspicious based on warning signs and determine the correct action to take if the email is suspicious.

Appendix A: Answer Key

Review Activity 1

Elaine Durham, Senior Engineer: Can you take a look at this email and help me determine if it's suspicious?

From: Petra cyberwatch

Subject: Re: Counter-UAV system

Good morning!

Pls let me introduce myself and our company, this is petra from CyberWatch Ltd, Head Office in Country Z, Branch Office in Country Purple. We are a cyber and IT company offering solutions for terrorism and security challenge. Now we have a client who want to buy ur counterUAV product. We knowof export control and are able to get the needed permits for the transaction.

I wander if your company have stock for them?

have a nice day!

best wishes to u and ur family!

ur sincerely,petra

www.cyberwatch.com

Tel: 86-10-67726085

Email: sales@centricspace.com

MSN:petra_song04@hotmail.com

- ○ Reply
- ○ Delete
- ◉ Report (correct response)

Feedback: *When you choose to report suspicious emails, you're doing your part to prevent industrial espionage and protect national security. Deleting a suspicious email does not ensure that the emails will stop. In order to stop a potential threat, you must report suspicious emails to DCSA so that they can piece together the bigger picture. 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.*

Review Activity 2

Dahlia Caine, Engineer and Associate Professor: I just received an email and I'm not sure whether to report it or not.

From: Carlos Moreno [mailto: cmoreno@learnalot.com]

Subject: Technical Review Request

Greetings,

We met last summer at the tech conference in Richmond. I very much enjoyed hearing about your research at the University. The following might be of interested to your research. Please take a look as soon as you are able. You can view it on this secure website: Technical Load Data Peer Review.

Respectfully

Carlos Moreno

LearnALot Technologies

Alexandria, VA 22304

Tel – 703.555.1234

- ○ Reply
- ○ Open Link/Attachment
- ○ Delete
- ◉ Report (correct response)

Feedback: *When you choose to report suspicious emails, you're doing your part to prevent industrial espionage and protect national security. Deleting a suspicious email does not ensure that the emails will stop. In order to stop a potential threat, you must report suspicious emails to DCSA so that they can piece together the bigger picture. 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. When you open a link or attachment in the suspicious email, you are exposing yourself to malware. The potential damage could be very severe.*

Review Activity 3

David Surbrook, Project Manager: I just received an email and I'm not sure whether to report it or not.

From: Sarita Smith [mailto: sarita@brightpath.com]

Subject: Quote Request KII-0444-44

Hi,

Thanks for the information.

We are thinking of buying your radar surveillance system. 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

Sarita Smith

Brightpath Technology LLC

Newport News, VA 23602

Tel – 757.555.1234

- ○ Reply
- ○ Delete
- ◉ Report (correct response)

Feedback: *When you choose to report suspicious emails, you're doing your part to prevent industrial espionage and protect national security. Deleting a suspicious email does not ensure that the emails will stop. In order to stop a potential threat, you must report suspicious emails to DCSA so that they can piece together the bigger picture. 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.*

Review Activity 4

Donald Joseph, Business Analyst: I'm not certain about this email. Can you take a look?

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

- ⦿ Reply (correct response)
- ○ Delete
- ○ Report

Feedback: *"When in doubt, contact DCSA." While this is generally a good rule of thumb, if you're reporting one of your own long-term customers, you might want to either reconsider who you're doing business with or double check your customer records. Because the email was not suspicious, what you choose to do with it has no consequences as far as national security and industrial espionage are concerned.*

Review Activity 5

Jack Jones, Project Manager: I just received an email and I'm not sure whether to report it or not.

From: May Chung [mailto: mchung@YourBank.com]

Subject: Account Compromise

Greetings

We detected suspicious activity on your checking account. Please verify your account activity immediately.

Review Account Activity

May Chung

Your Bank

Linthicum, MD 21601

Tel – 410.555.1234

- ○ Reply
- ○ Open Link/Attachment
- ○ Delete
- ⦿ Report (correct response)

Feedback: *When you choose to report suspicious emails, you're doing your part to prevent industrial espionage and protect national security. Deleting a suspicious email does not ensure that the emails will stop. In order to stop a potential threat, you must report suspicious emails to DCSA so that they can piece together the bigger picture. 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. When you open a link or attachment in the suspicious email, you are exposing yourself to malware. The potential damage could be very severe.*