

Activity # 5 - Malware and Friends! (Threats)

Started: Nov 7 at 6:05pm

Quiz Instructions

Key Learnings:

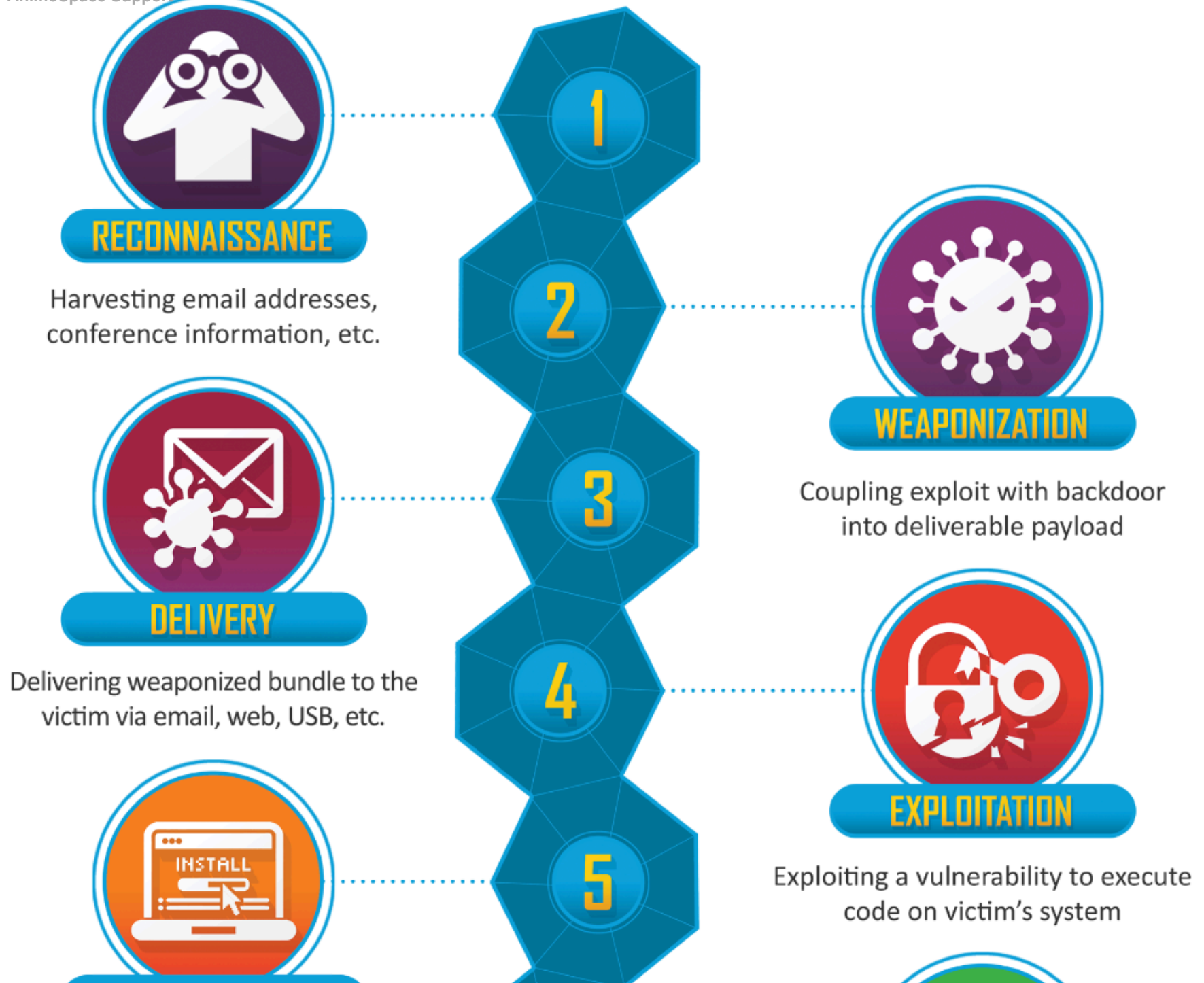
1. You will learn how to detect phishing and investigate basic malware. This is helpful for IT and students like you!
2. YOU can Collaborate with your classmates to help each other investigate the unknowns in the world of cybersecurity.
3. Laptop is a must!!
4. This activity Locks questions after answering.



Question 1 1 pts

Phishing attack is a type of attack aimed at stealing personal data of the user in general by clicking on malicious links to the users via email or running malicious files on their computer.

Phishing attacks correspond to the "**Delivery**" phase in the **Cyber Kill Chain** model created to analyze cyber attacks. The delivery stage the step where the attacker transmits the previously prepared harmful content to the victim systems / people.



AnimoSpace Support

INSTALLATION

Installing malware on the asset

**ACTIONS ON OBJECTIVES**

With 'Hands on Keyboard' access,
intruders accomplish their original goals

6

7

**COMMAND & CONTROL (C2)**

Command channel for remote
manipulation of victim

The attackers generally aim to click on the harmful link in the mail, such as "you have won a gift", "do not miss the big discount", "if you do not click on the link in the mail your account will be suspended" to direct users to click on the links in the mail.

The phishing attack is the most common attack vector for initial access.

Of course, the only purpose of the attack is not to steal the user's password information. The purpose of such attacks is to exploit the human factor, the weakest link in the chain. Attackers use phishing attacks as the first step to infiltrate systems.

type "**Done**" to proceed

Next ▶

AnimoSpace Support

Quiz saved at 6:05pm

Submit Quiz

Activity # 5 - Malware and Friends! (Threats)

Started: Nov 7 at 6:05pm

Quiz Instructions

Key Learnings:

1. You will learn how to detect phishing and investigate basic malware. This is helpful for IT and students like you!
2. YOU can Collaborate with your classmates to help each other investigate the unknowns in the world of cybersecurity.
3. Laptop is a must!!
4. This activity Locks questions after answering.




Question 2 1 pts


Spoofing

Attackers can send emails on behalf of someone else, as the emails do not necessarily have an authentication mechanism. Attackers can send mail on behalf of someone else using the technique called spoofing to make the user believe that the incoming email is reliable. Several protocols have been created to prevent the Email Spoofing technique. With the help of SPF, DKIM and DMARC protocols, it can be understood whether the sender's address is fake or real. Some mail applications do these checks automatically. However, the use of these protocols is not mandatory and in some cases can cause problems.

- Sender Policy Framework (SPF)
- DomainKeys Identified Mail (DKIM)

To find out manually whether the mail is spoof or not, SMTP address of the mail should be learned first. SPF, DKIM, DMARC and MX records of the domain can be learned using tools such as [Mxtoolbox](https://mxtoolbox.com/)  [\(https://mxtoolbox.com/\)](https://mxtoolbox.com/). By comparing the information here, it can be learned whether the mail is spoof or not.

AnimoSpace Support

 MX Lookup

Domain Name

MX Lookup

Solve Email Delivery Problems

Since the IP addresses of the big institutions using their own mail servers will belong to them, it can be examined whether the SMTP address belongs to that institution by looking at the whois records of the SMTP IP address.

An important point here is that if the sender address is not spoof, we cannot say mail is safe. Harmful mails can be sent on behalf of trusted persons by hacking corporate / personal email addresses. This type of cyber attacks has already happened, so this possibility should always be considered.

E-mail Traffic Analysis

Many parameters are needed when analyzing a phishing attack. We can learn the size of the attack and the target audience in the search results to be made on the mail gateway according to the following parameters.

- Sender Address(keinaz.domingo@dlsu.edu.ph)
- SMTP IP Address(127.0.0.1)
- @dlsu.edu.ph (domain base)
- DLSU (Besides the gmail account, attacker may have sent from the hotmail account)
- Subject (sender address and SMTP address may be constantly changing)

In the search results, it is necessary to learn the recipient addresses and time information besides the mail numbers. If harmful e-mails are constantly forwarded to the same users, their e-mail addresses may have leaked in some way and shared on sites such as PasteBin.

type "Done"

Canvas LMS Support

Next ►

Quiz saved at 6:06pm

Submit Quiz

Activity # 5 - Malware and Friends! (Threats)

Started: Nov 7 at 6:05pm

Quiz Instructions

Key Learnings:

1. You will learn how to detect phishing and investigate basic malware. This is helpful for IT and students like you!
2. YOU can Collaborate with your classmates to help each other investigate the unknowns in the world of cybersecurity.
3. Laptop is a must!!
4. This activity Locks questions after answering.



Question 3 1 pts

What is an Email Header and How to Read Them?

In this section, we will explain what the header information in an email is, what can be done with this information and how to access this information. It is important to follow this section carefully as we will explain how to perform the header analysis in the next section.

What is an Email Header?

"Header" is basically a section of the mail that contains information such as sender, recipient and date. In addition, there are fields such as **"Return-Path"**, **"Reply-To"**, and **"Received"**. Below you can see the header details of a sample email.

Delivered-To: nazkiegear@gmail.com
 Received: by 2002:a05:7108:2f09:b0:371:a55d:d011 with SMTP id u9csp136198gdf;
 Thu, 15 Feb 2024 16:00:26 -0800 (PST)
 X-Google-Smtp-Source: AGHT+IGAwcPvdiEES9XdUVF44KtsgB4PZF9+PHBRheB1toHqf5GBmkr7clSFBjC1Q4oNn92+0lmj
 X-Received: by 2002:a0c:c994:0:b0:686:9de1:7016 with SMTP id b20-20020a0cc994000000b006869de17016mr752971qvk.35.1708041625938;
 Thu, 15 Feb 2024 16:00:25 -0800 (PST)
 ARC-Seal: i=1; a=rsa-sha256; t=1708041625; cv=none;
 d=google.com; s=arc-20160816;
 b=VBoAMUwKxqcEDVyFMIT1P/4eq1aEHefaijK4QFkBMjqp+ycn13q5gBv1FoZ2bJyk8/
 mSfkhJX+QHAX3TJLyF0eb8eNEtVgIFM2TdFpG2VocKh4W8djJSRA7IBSDrQ1ycn2zN8c
 wD5JUTZKh5ZxYk86JaqwVK0Q4AabsJTXcrIjLw33mSNHLrQW9xTqkZILUdbedM0hcKgX
 jhj6f2vj5Cx/Vmr4WYfKhyKAWfvV8klcByXFCT3k0BmhYxv5wAPoE262CNUgOVfLe/fz
 4VAz5G0w0HwWJLaP/X4o1FlbPjxxtB1atPeRD5BpmW0QA9ThkJ5Ho88BYu120Q3juib
 rt+g==
 ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
 h=feedback-id:message-id:subject:to:reply-to:from:date:mime-version
 :dkim-signature:dkim-signature;
 bh=eyZ4Ka8Au23+pmNIKuMhNbBwQwu8amhRFiKif1LXpgk=;
 fh=auD8iLYnWdpOD7DR+xNLMYH0kbOhmshbCkX5iVWRxFQ=;
 b=lihLwKAIwIQbzUCY5HaBU0dHg0RgYzMn3wVW4Xt5car15NGAzSWE2kZFudIpvspHmr
 7KrkjW8Tk5ZoKnYag5NjiIpIRu52t0BxWzWU5+YdNpL9o3De6U2YIJKEDLog4KzLNiHB
 QQPWQhR4iWBD/b1ZT3bNpCP8Shi7c7Ze6RULbs8FjnnjRwaNwA7gk5As4Zt1YC96D5F
 iQhC428QxM7a/By0FdQAZ5Fg+wVYDqYa8jIcIBvj09leqDHFLbyL1264eM3gxdCLx9m2
 9f/TvBLf+62sRFQs3hGw7T9kC1sp34xoIEd6v9/vVcmI97DfzFWLFbSdvTYPUHct3oy
 sxxg==;
 dara=google.com
 ARC-Authentication-Results: i=1; mx.google.com;
 dkim=pass header.i=@moveit.com.ph header.s=gs2py5fzfmrzc3emduyoqo7rv5sp4czj header.b=HkElGRSb;
 dkim=pass header.i=@amazonses.com header.s=224i4yxa5dv7c2xz3womw6peuasteono header.b=fFoEIupa;
 spf=pass (google.com: domain of 0100018daf36dd4b-6a4daf6c-a912-4aeb-89fa-0c9804eb9cb2-000000@amazonses.com designates
 54.240.49.45 as permitted sender) smtp.mailfrom=0100018daf36dd4b-6a4daf6c-a912-4aeb-89fa-0c9804eb9cb2-000000@amazonses.com;
 dmarc=pass (p=QUARANTINE sp=QUARANTINE dis=NONE) header.from=moveit.com.ph
Return-Path: <0100018daf36dd4b-6a4daf6c-a912-4aeb-89fa-0c9804eb9cb2-000000@amazonses.com>
Received: from a49-45.smtp-out.amazonses.com (a49-45.smtp-out.amazonses.com. [54.240.49.45])
 by mx.google.com with ESMTPS id fq4-20020a056214258400b0068c77810855si2796011qvb.556.2024.02.15.16.00.25
 for <nazkiegear@gmail.com>
 (version=TLS1_2 cipher=ECDHE-ECDSA-AES128-GCM-SHA256 bits=128/128);
 Thu, 15 Feb 2024 16:00:25 -0800 (PST)
 Received-SPF: pass (google.com: domain of 0100018daf36dd4b-6a4daf6c-a912-4aeb-89fa-0c9804eb9cb2-000000@amazonses.com designates
 54.240.49.45 as permitted sender) client-ip=54.240.49.45;
 Authentication-Results: mx.google.com;
 dkim=pass header.i=@moveit.com.ph header.s=gs2py5fzfmrzc3emduyoqo7rv5sp4czj header.b=HkElGRSb;
 dkim=pass header.i=@amazonses.com header.s=224i4yxa5dv7c2xz3womw6peuasteono header.b=fFoEIupa;
 spf=pass (google.com: domain of 0100018daf36dd4b-6a4daf6c-a912-4aeb-89fa-0c9804eb9cb2-000000@amazonses.com designates
 54.240.49.45 as permitted sender) smtp.mailfrom=0100018daf36dd4b-6a4daf6c-a912-4aeb-89fa-0c9804eb9cb2-000000@amazonses.com;
 dmarc=pass (p=QUARANTINE sp=QUARANTINE dis=NONE) header.from=moveit.com.ph

```

DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/simple;
s=gs2py5fzfmrzc3emduyoqo7rv5sp4czj; d=moveit.com.ph; t=1708041625;
h=MIME-Version:Date:From:Reply-To:To:Subject:Content-Type:Message-ID;
bh=eyZ4Ka8Au23+pmNIKuMhNbBwQwu8amhRFiKif1LXpgk=;
b=HkElGRSbWxSJqikqwuzYThhffu+R5tjvFhicgu9vdu5bz9uFj/E9CD6Xg5Npi4wW
xFqi+YRzzUAw1Ey87uUeD0q+eE4obyi2tyzpXyNpdvg72D69L8E5gJosIcdyIcaAkk
7a959nyRC6CSBKx010YM7ZY8D7K25tNJaZhA30wQ937K8I92WXvMoLVpjZbByxBJSrK
QPAJPLi0tRKi7G9iD90aVTmj94QfSrnrRrOPcmfL00c8+o8BJy8EzegWdjw2D5UGja0
MMHAgT1qji4NC22gcAwDL0t4TTMjr09tmWswVmxyXgwNguMHj2Nv2znrX5e6pt0wZ5Y
uPk9xbMlvA==
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/simple;
s=224i4yxa5dv7c2xz3womw6peuasteono; d=amazonses.com; t=1708041625;
h=MIME-Version:Date:From:Reply-To:To:Subject:Content-Type:Message-ID:Feedback-ID;
bh=eyZ4Ka8Au23+pmNIKuMhNbBwQwu8amhRFiKif1LXpgk=;
b=fFoEIupaT3vEEYVJc1UyycSCvjY0s7QWVEN9K7Ar9JX7W0p4bPNAjKKyXn0/S7eT
U+OKvUS1SNfKvFkMaIb+bxWd59MrSzPorZ91mqcwEwe9+jm0Z6vqHPoB0wpfChvWfQy
pZzM4Fp0+3kYT+lZpa4WumIS8vvfjxapUDXKh0Is=
MIME-Version: 1.0
Date: Fri, 16 Feb 2024 00:00:24 +0000
From: Moveit <no-reply@moveit.com.ph>
Reply-To: Moveit <no-reply@moveit.com.ph>
To: nazkiegear@gmail.com
Subject: Your Move It E-Receipt
Content-Type: multipart/alternative;
boundary=b71ba9a3dfb07fdefaf2a7fa6c57b72e1a7bbfbcca59971c73182c29b625
Message-ID: <0100018daf36dd4b-6a4daf6c-a912-4aeb-89fa-0c9804eb9cb2-000000@email.amazonses.com>
Feedback-ID: 1.us-east-1.v0KPKuSkkprzUq6+f6w9DAEJmnreZyJFq6hDYHOnNAK=:AmazonSES
X-SES-Outgoing: 2024.02.16-54.240.49.45

--b71ba9a3dfb07fdefaf2a7fa6c57b72e1a7bbfbcca59971c73182c29b625
Content-Transfer-Encoding: base64
Content-Type: text/plain; charset=UTF-8

--b71ba9a3dfb07fdefaf2a7fa6c57b72e1a7bbfbcca59971c73182c29b625
Content-Transfer-Encoding: base64
Content-Type: text/html; charset=UTF-8

```

What does the Email Header do?

Enables Shipper and Recipient Identification

AnimoSpace Support

Thanks to the "From" and "To" fields in the header, it is determined from whom an email will go to whom. If we look at the email above that you downloaded in "eml" format, we see that it was sent from the address " **Moveit <no-reply@moveit.com.ph>**" to **"nazkiegear@gmail.com"**

```
From: Moveit <no-reply@moveit.com.ph>  
Reply-To: Moveit <no-reply@moveit.com.ph>  
To: nazkiegear@gmail.com  
Subject: Your Move It F Receipt
```

Spam Blocker

It is possible to detect spam emails using Header analysis and other various methods. This protects people from receiving SPAM emails.

Allows Tracking an Email's Route

It is important to check the route it follows to see if an email came from the right address. If we look at the sample email above, we see that it came from the "no-reply@movit.com.ph" address, but did it actually come from the "movit.com.ph" domain or from a different fake server that mimics the same name? We can use the header information to answer this question.

Important Fields

From

The "From" field in the internet header indicates the name and email address of the sender.

To

This field in the mail header contains the email's receiver's details.

It includes their name and their email address. Fields like CC (carbon copy) and BCC (blind carbon copy) also fall under this category as they all include details of your recipients.

If you want to find out more about carbon copy and blind carbon copy, check out how to use CC and BCC.

Date

This is the timestamp that shows when the email was sent.

In Gmail, it usually follows the format of "day dd month yyyy hh:mmss

So if an email had been sent on the 16th of November, 2021, at 4:57:23 PM, it would show as Wed, 16 Nov 2021 16:57:23.

Subject

The subject mentions the topic of the email. It summarizes the content of the entire message body.

Return-Path

This mail header field is also known as Reply-To. If you reply to an email, it will go to the address mentioned in the Return-Path field.

Domain Key and DKIM Signatures

The Domain Key and Domain Key Identified Mail (DKIM) are email signatures that help email service providers identify and authenticate your emails, similar to SPF signatures.

Message-ID

The Message ID header field is a unique combination of letters and numbers that identifies each mail. No two emails will have the same Message ID.

MIME-Version

Multipurpose Internet Mail Extensions (MIME) is an internet standard of encoding. It converts non-text content like images, videos, and other attachments into text so they can be attached to an email and sent through SMTP (Simple Mail Transfer Protocol).

Received

The received field lists each mail server that went through an email before arriving in the recipient's inbox. It's listed in reverse chronological order — where the mail server on the top is the last server the email message went through, and the bottom is where the email originated.

AnimoSpace Support

X-Spam Status

The X-Spam Status shows you the spam score of an email message.

First, it'll highlight if a message is classified as spam.

Then, the spam score of the email is shown, as well as the threshold for the spam for the email.

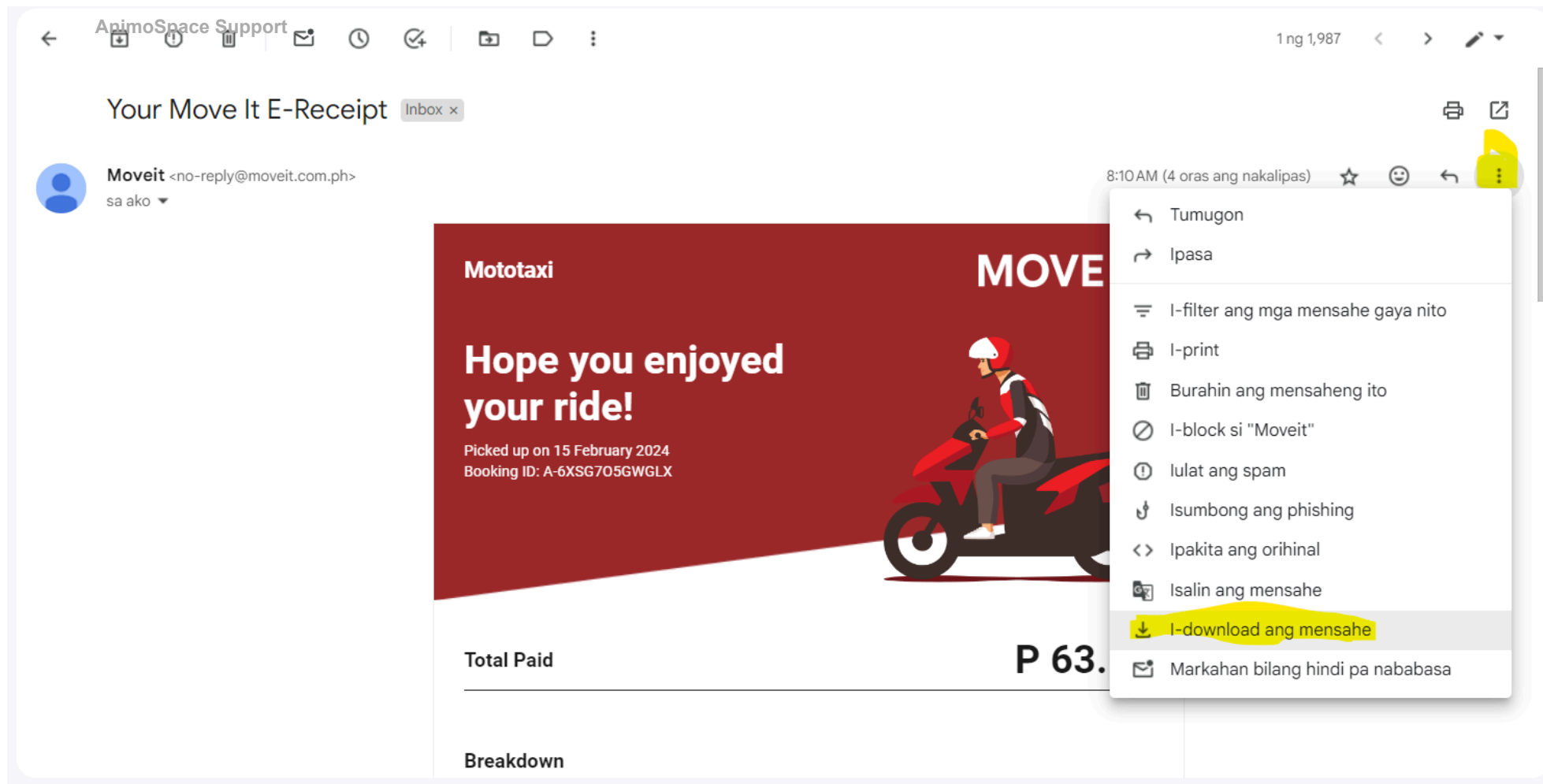
An email can meet either the spam threshold of an inbox or exceed it. If it's too spammy and exceeds the threshold, it will automatically be classified as spam and sent to the spam folder.

Field Definitions: gmass.co

How to Access Your Email Header?

Gmail

- 1- Open the relevant e-mail
- 2- Click on the 3 points at the top right "..."
- 3- Click on the "Download message" button.



4- Downloaded ".Open the file with the extension ".eml" with any notebook application

Outlook

1- Open the relevant e-mail

2- File - > Info -> Properties - > Internet headers

AnimoSpace Support

Gain new skill: 15% OFF 🤖 - Message (HTML)

←

Info

Save


Save As

Save Attachments

Print

Close


Gain new skill: 15% OFF 🤖



Encrypt

Encrypt this item

Set up restrictions for this item. For example, you may be able to restrict recipients from forwarding the email message to other people.




Move to Folder

Move item to a different folder

Move or copy this item to a different folder.


- Current Folder: Inbox



Resend or Recall

Message Resend and Recall

Resend this email message or attempt to recall it from recipients.



Properties

Properties

Set and view advanced options and properties for this item.

- Size: 67 KB

Office Account

Feedback

Options

The screenshot shows an Outlook email window titled "AnimoSpace Support" with a blue header bar. The ribbon includes "File", "Message", and "Help". The "Message" tab is active, showing icons for "Delete", "Archive", "Reply", "Reply All", "Forward", "Move to:?", "To Manager", "Team Email", "Move", "Mark Unread", "Follow Up", "Translate", "Read Aloud", "Immersive Reader", and "Zoom". The email is from "L" (umut@letsdefend.io) dated "Fri 3/18/2022 7:02 PM" with the subject "LetsDefend <in>". The body text includes "Gain new skill: 15% O" and "To umut@letsdefend.io". The "Properties" dialog box is open, showing "Settings" (Importance: Normal, Sensitivity: Normal), "Security" (Encrypt message contents and attachments, Add digital signature to outgoing message, Request S/MIME receipt for this message), "Tracking options" (Request a delivery receipt for this message, Request a read receipt for this message), "Delivery options" (Have replies sent to: LetsDefend, Expires after: None, 12:00 AM), "Contacts...", "Categories" (None), and "Internet headers" (highlighted with a red box). The "Internet headers" section contains the following text: "Delivered-To: umut@letsdefend.io", "Received: by 2002:a05:7110:5292:b0:15e:c6b3:3eeb with SMTP id k18csp2152533gec", "Fri, 18 Mar 2022 09:02:31 -0700 (PDT)", "X-Google-Smtp-Source: ABdhPJzm4eptPF+yzck/Vn6raCwEOu7PxFjsRoCzFwrMeF81my8ykTQ+r0Q7GG", and "dupEhZ+aFSpJqh". A "Close" button is visible at the bottom right of the dialog box.

type "Done"

AnimoSpace Support

Next ►

Quiz saved at 6:07pm

Submit Quiz

Activity # 5 - Malware and Friends! (Threats)

Started: Nov 7 at 6:05pm

Quiz Instructions

Key Learnings:

1. You will learn how to detect phishing and investigate basic malware. This is helpful for IT and students like you!
2. YOU can Collaborate with your classmates to help each other investigate the unknowns in the world of cybersecurity.
3. Laptop is a must!!
4. This activity Locks questions after answering.




Question 7 2 pts

In previous sections we talked about what a phishing email is, what header information is and what it does. Now, when we suspect that an email is phishing, we will know what we should do and what the analysis process should be like.

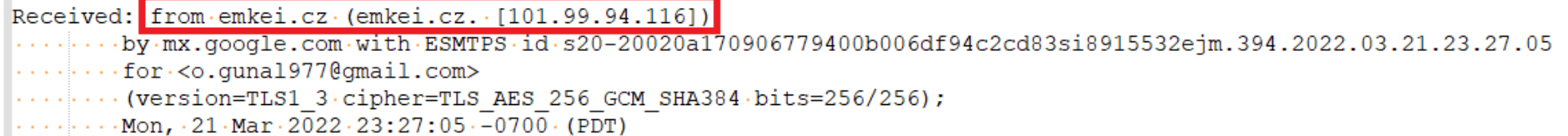
Here are the key questions we need to answer when checking headings during a Phishing analysis:

- Was the email sent from the correct SMTP server?
- Are the data "From" and "Return-Path / Reply-To" the same?

Try it! Download me: [Account details.eml \(https://dlsu.instructure.com/courses/184262/files/21759492?wrap=1\)](https://dlsu.instructure.com/courses/184262/files/21759492?wrap=1) 
(https://dlsu.instructure.com/courses/184262/files/21759492/download?download_frd=1) (Not scored but great information on why we need to analyze email headers!)

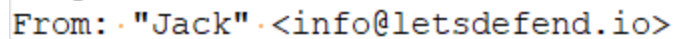
Was the email sent from the correct SMTP server?

We can check the "Received" field to see the path followed by the mail. As the image below shows, the mail is "101[.]99.94.116" from the IP address server.



```
Received: from emkei.cz. ([101.99.94.116])  
.....by mx.google.com with ESMTPS id s20-20020a170906779400b006df94c2cd83si8915532ejm.394.2022.03.21.23.27.05  
.....for <o.gunal977@gmail.com>  
.....(version=TLS1_3, cipher=TLS_AES_256_GCM_SHA384, bits=256/256);  
.....Mon, 21 Mar 2022 23:27:05 -0700 (PDT)
```

If we look at who is sending the mail ("sender"), we see that it came from the domain Letsdefend.io



```
From: "Jack" <info@letsdefend.io>
```

So under normal circumstances, "letsdefend.io" should use, "101[.]99.94.116" to send mail. To confirm this situation, We can query the MX servers actively used by "letsdefend.io"

"mxtoolbox.com" helps by showing you the MX servers used by the domain you searched.

SuperTool - Online Space Support

letsdefend.io

MX Lookup

mx:letsdefend.io

Find Problems

Solve Email Delivery Problems

Pref	Hostname	IP Address	TTL
1	aspmx.l.google.com	172.253.122.26 Google LLC (AS15169)	5 min
1	aspmx.l.google.com	2607:f8b0:4004:c06::1b	5 min
5	alt1.aspmx.l.google.com	209.85.202.27 Google LLC (AS15169)	5 min
5	alt1.aspmx.l.google.com	2a00:1450:400b:c00::1b	5 min
5	alt2.aspmx.l.google.com	64.233.184.27 Google LLC (AS15169)	5 min
5	alt2.aspmx.l.google.com	2a00:1450:400c:c0b::1a	5 min
10	alt3.aspmx.l.google.com	142.250.27.27 Google LLC (AS15169)	5 min
10	alt3.aspmx.l.google.com	2a00:1450:4025:401::1b	5 min
10	alt4.aspmx.l.google.com	142.250.153.26 Google LLC (AS15169)	5 min
10	alt4.aspmx.l.google.com	2a00:1450:4013:c16::1a	5 min

If we look at the image above, the "letsdefend.io" domain uses Google addresses as an email server. So there is no relationship with the emkei[.]cz or "101[.]99.94.116" addresses.

In this check, it was determined that the email did not come from the original address, but was spoofed.

Are the data "From" and "Return-Path / Reply-To" the same?

Except in exceptional cases, we expect the sender of the e-mail and the person receiving the responses to be the same. An example of why these areas are used differently in Phishing attacks:

Someone sends an email (gmail, hotmail etc.) with the same last name of someone working for Google to LetsDefend, LetsDefend tells the employee that he has issued the invoice and they must make the payment to his XXX account. It puts the e-mail address of the real Google employee in the "Reply-to" field so that the fake e-mail address does not stand out in case of replying to a possible e-mail.

Returning to the e-mail we downloaded above, all we have to do is compare the email addresses in the "From" and "Reply-to" fields.

```
From: "Jack" <info@letsdefend.io>  
X-Priority: 3 (Normal)  
Importance: Normal  
Errors-To: info@letsdefend.io  
Reply-To: info.letsdefend123722@gmail.com
```

As you can see, the data is different. In other words, when we want to reply to this e-mail, we will send a reply to the gmail address below. Just because this data is different doesn't always mean it's definitely a phishing email, we need to consider the event as a whole. In other words, in addition to this suspicious situation, if there is a harmful attachment, URL or misleading content in the e-mail content, we can understand that the e-mail is phishing. In the continuation of the training, we will analyze the data in the body part of the e-mail.

type "Done"

Next ►

Activity # 5 - Malware and Friends! (Threats)

Started: Nov 7 at 6:05pm

Quiz Instructions

Key Learnings:

1. You will learn how to detect phishing and investigate basic malware. This is helpful for IT and students like you!
2. YOU can Collaborate with your classmates to help each other investigate the unknowns in the world of cybersecurity.
3. Laptop is a must!!
4. This activity Locks questions after answering.



Question 14 1 pts

VirusTotal inspects items with over 70 antivirus scanners and URL/domain blocklisting services, in addition to a myriad of tools to extract signals from the studied content. Any user can select a file from their computer using their browser and send it to VirusTotal.




Analyze suspicious files and URLs to detect types of malware,
automatically share them with the security community

FILE

URL

SEARCH



By submitting data below, you are agreeing to our [Terms of Service](#) and [Privacy Policy](#), and to the sharing of your Sample submission with the security community. Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. [Learn more.](#)

Much like a search engine, you can search for reports by a few characteristics, for example:

- The IP Addresses that samples communicate with
- Checksums
- The file itself

VirusTotal not only tells you whether a given antivirus solution detected a submitted file as malicious, but also displays each engine's detection label (e.g., I-Worm.Allapple.gen). The same is true for URL scanners, most of which will discriminate between malware sites, phishing sites, suspicious sites, etc. Some engines will provide additional information, stating explicitly whether a given URL belongs to a particular botnet, which brand is targeted by a given phishing site, and so on.

type "**Done**"

Next ►

Not saved

Submit Quiz

Activity # 5 - Malware and Friends! (Threats)

Started: Nov 7 at 6:05pm

Quiz Instructions

Key Learnings:

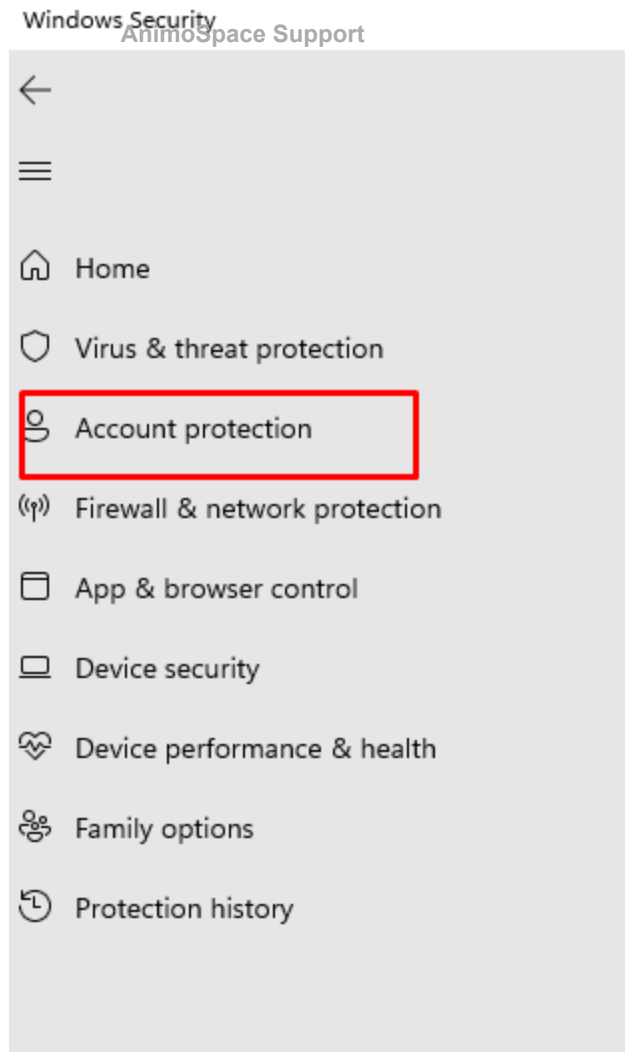
1. You will learn how to detect phishing and investigate basic malware. This is helpful for IT and students like you!
2. YOU can Collaborate with your classmates to help each other investigate the unknowns in the world of cybersecurity.
3. Laptop is a must!!
4. This activity Locks questions after answering.



Question 24 2 pts

Q# 3

PRE-REQ: TURN OFF YOUR ANTIVIRUS FOR THIS TYPE OF ACTIVITY. THIS IS SAFE AS LONG AS YOU DO NOT RUN THE APPLICATION.




Virus & threat protection settings

View and update Virus & threat protection settings for Microsoft Defender Antivirus.

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

 Real-time protection is off, leaving your device vulnerable.

☐ Off

Turn on real-time protection to use this feature.

Dev Drive protection

Scans for threats asynchronously on Dev Drive volumes to reduce performance impact.

Keystroke logging often referred to as keylogging or keyboard capturing, is the action of recording the keys struck on a keyboard, typically covertly, so that a person using the keyboard is unaware that their actions are being monitored. What if someone monitors your Laptop/Desktop. What will you do? Let's try some real scenario:

1.) Go to this website

[bytesin.com/software/Download-Spyrix-Free-Keylogger/](https://www.bytesin.com/software/Download-Spyrix-Free-Keylogger/)  (<https://www.bytesin.com/software/Download-Spyrix-Free-Keylogger/>)

2.) Click Bytesin **External Mirror 1**



Download Spyrix Free Keylogger 11.6.14

File: sfk_setup.exe (3.10 Mb)



Review



Download



1 Screenshot



No Video

Please select a download mirror:



BytesIn US Mirror



BytesIn EU Mirror

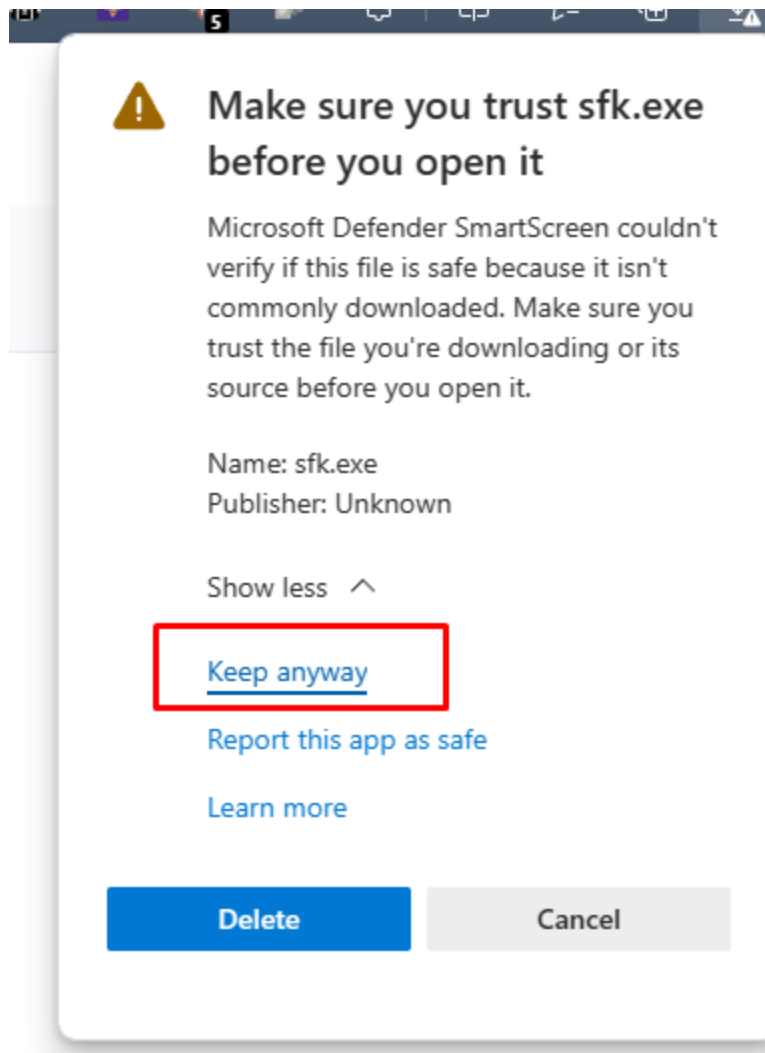
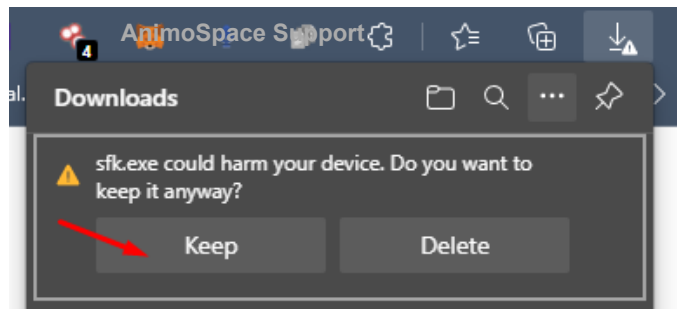


External Mirror 1

Remote monitoring of your PC activity Spyrix Free Keylogger is a useful and reliable tool created to log PC's activity such as keystrokes, accessed webpages, entered password and more. Spyrix Keylogger can take screenshots of the current...[full software details](#)

If you encounter any problems in accessing the download mirrors for **Spyrix Free**

3.) Click **KEEP (WARNING: DO NOT RUN THE APPLICATION)**



5.) Now, upload this file in **Virustotal**.



Question: it has detection? If yes, how many?

Next ►

Quiz saved at 6:49pm

Submit Quiz