Cyber Crime Aspect in Online Teaching

UNIVERSITY OF ENGINEERING & TECHNOLOGY,
PESHAWAR, PAKISTAN

1. Introduction

Due to the COVID-19 pandemic across the globe, academia worldwide has been affected. Educational institutes from schools to degree awarding Institutes have closed their campuses to ensure safety of the students and faculty and to stop the possible spread of the pandemic through these campuses. However, with the recent advances in technology and telecommunications, education can be delivered over the internet. Classrooms can now utilize virtual forums for interaction among the students and instructors. Online forums help instructors to share lesson plans while social media help students collaborate across classrooms. Web-based applications assist instructors in customizing the learning experience for each student to achieve greater learning outcomes.

Early adopters of these technologies have demonstrated their potential to transform the educational process, but they have also called attention to possible challenges. In particular, the use of information sharing, web-hosting, and the software tools for online education have also raised the issues of security and privacy.

This document addresses a number of these security concerns, and presents the requirements and best practices to consider, when using the online educational services. Examples include the use of online services for access to class contents by the students, to view the progression of different courses, to watch video demonstrations, to comment on class activities, or to complete their homework.

1.1 Security issues in Online Educational Services

Cybercrime is the use of a computer for illegal activities such as committing fraud, trafficking intellectual property, stealing identities, or violating privacy. Cybercrime, especially through the Internet, has grown in importance as the computer has become central to commerce, entertainment, and government. Many systems belonging to educational institutes have also become victims of cybercrimes in the recent years.

To battle the rise of cybercrimes in Pakistan, the Prevention of Electronic Crimes Act (PECA) has been accepted by the Parliament of Pakistan in 2016. The Act proposes fines as well as jail punishments for cyber offences. Additionally, a provision is made for Computer Emergency Response Teams that would constitute the personnel having expertise in issues pertaining to cybersecurity on critical infrastructure and associated data. Similarly, officials of intelligence agencies are to be made part of these teams as well to ensure proper defenses and policies are followed by all organizations. The Act also proposes international cooperation in this regard to thwart and investigate all threats of cybersecurity.

1.2 Possible Crimes on Online Education Services

Malicious users can exploit the weaknesses in computer software, mobile applications (apps), and web-based tools used for providing online education. Crimes as stated by PECA Act 2016 are briefly described below in the context of online education:

- **Unauthorized Access to Information Systems:** Refers to accessing any system (e.g., laptop, mobile phone) illegally with the intent of damaging or misusing it or manipulating the information contained in it. Examples include gaining access to the system of a course instructor or administrator for damaging or misusing the course related information e.g., student's grades.

- **Unauthorized copying or transmission of Data**: Refers to acquiring data by illegal means and further disseminating it to others without the consent of the owner, e.g., gathering personal information or course grades of students and disseminating it on social media.

- **Unauthorized use of Identity Information:** Refers to acquiring the personal information of other users and using it for impersonation, e.g., using the email/password of other students to damage their reputation in an online class.

- **Interference with information system or data:** Access a system with the intent of destroying the use of functionality or services provided by it e.g., attacking the system of an instructor to disrupt a scheduled/live lecture.

- **Unauthorized Interception**: Refers to the interception of confidential information by unauthorized persons, e.g., the interception of a list of student email addresses to whom password to a Zoom meeting call is to be sent.

- **Spamming:** is the use of sending unwanted, explicit or illegal messages in huge amounts. It can also be used to send viruses or malware. For example, a student publishing derogatory comments in a chatroom to cause chaos among the other participants.

- **Email Spoofing:** Refers to a cybercriminal activity where an attacker creates a false email message with a forged sender address appearing to have originated from someone or somewhere other than the actual source. It is a popular tactic used in phishing and spam campaigns because people are more likely to open an email when they think it has been sent by a legitimate or familiar source. In the context of online teaching, a student can send a spoofed email to his classmate about the class cancelation, fake assignment, results etc., impersonating as the course instructor.

2. Security Issues, Preventions and Recommendations

We are considering the security issues with the following two types of software tools that we use for education services.

- Classroom management software (Google Classroom)
- Video conferencing software (Google Meet and Zoom)

A complete comparison of the relevant software tools is provided in another document (Comparison of software tool features for online classes).

In this section, we discuss the potential attacks and prevention tips for three software tools, i.e., Zoom, Google Meet and Google Classroom.

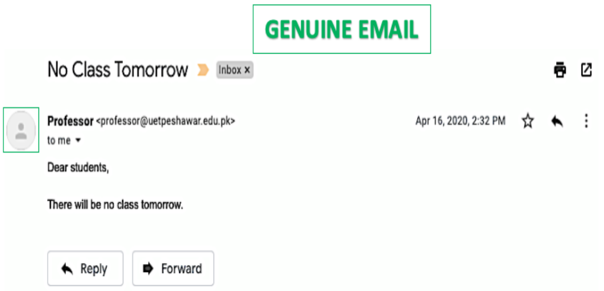
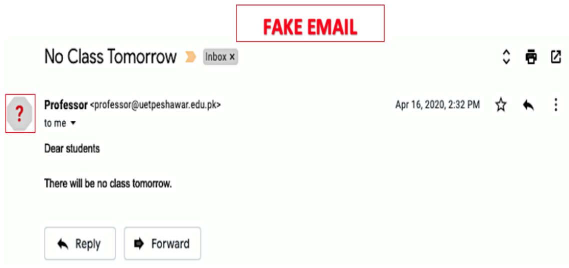
Table 1: Security issues and solutions in Zoom/Google Hangout and Google Classroom

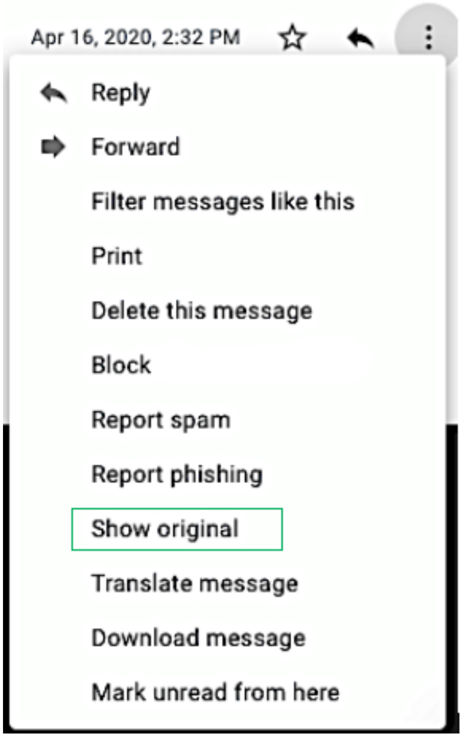
Security Issue	Software	Protection Option(s) available	Recommendation for Instructors
Automated tools can find meeting ID	Zoom, Google Meet	• Generate meeting ID automatically (Zoom) • Enabled meeting password (Zoom, Google Classroom) • Organizational participant can create meeting (Google Meet)	Check and ensure multiple times that all meeting participants are known to you.
An attacker could gain 'root' level privilege by modifying the Installer without anyone noticing	ZOOM, GOOGLE MEET/CLASSROOM (Possible in Mobile App)	Vendor-provided updates and have automated upgrades turned on (Zoom App)	• Make sure software is patched with the latest updates • Ensure use of secure systems and networks during the class.
Meeting Bombing-harassing participants by projecting graphic images.	Zoom, Google Meet, Google Classroom,	• Starting a meeting with a video off option for all participants to avoid any embarrassing moments (only in Zoom) • Mute participant upon entry	• Turn off the camera and microphone functionalities of the participants during class to avoid disturbance (if possible)
Video calls/messages are not end-to-end encrypted	Zoom, Google Meet, Google Classroom	N/A	• Avoid use of personal information about yourself and other participants where possible.
Participants can send a meeting invitation link to other users.	Zoom, Google Meet	• Don't allow participant outside the organization • Deny/admit participant (Zoom, Google Classroom)	• Share links only with the students enrolled in the specified class • Don't send the online class invitation links to others, including within your own classmates
No authentication/control on rejoin during the meeting.	Google Meet	Deny/admit participant after rejoin	The rejoining after the end of the meeting can be prevented by resetting the meeting link.
Website links can be sent in chat or comment	Google Meet, Google Classroom	Link can be sent as plain text (Google Classroom)	Don't open any link share by unauthorized person in chat or comment
No restriction on screen sharing	Google Meet	N/A	Ask the students to not share their screen without taking explicit permission from the instructor.

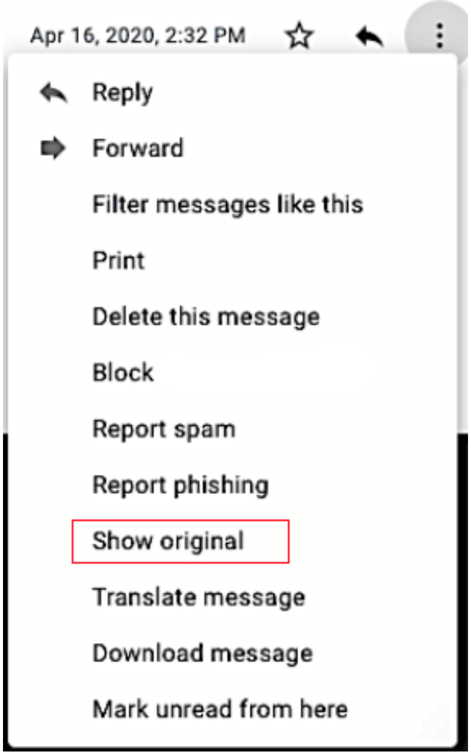
Users can control how their data are displayed	Google Meet, Google Classroom	Fixed user info displayed	Don’t edit your information after the enrollment. Use your official name only.
Uploading malicious files via meeting rooms or class rooms that are unwittingly downloaded by participants.	Zoom, Google Meet,	N/A	Disable file transfer features and instead, use other methods such as email for sending files.
Malware or Zero Day Attacks	Zoom, Google Classroom	N/A	Make sure your video conferencing software is patched with the latest vendor-provided updates and have automated upgrades turned on.
User-created content is reviewed, screened, or monitored by the vendor.	Google Classroom	N/A	Don’t share personal and confidential information
Email Spoofing	All software	N/A	Verify if the email is genuine or not (method shown in last section)

2.1 How to check Spoofed and Genuine email:

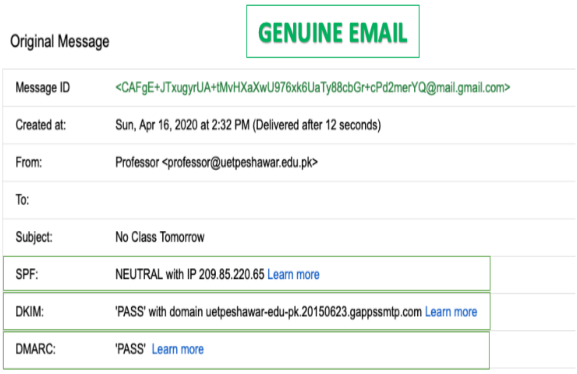
Following are the methods on how to verify if the email is from a legitimate sender or not. It is advised to not rely on a single method of verification and instead use all of them to ensure the authenticity of an email.

<table>
<tr><th colspan="2">Methods for checking spoofed email</th></tr>
<tr><td colspan="2">Check the Photo icon (Only for Gmail)</td></tr>
<tr><td>
No Class Tomorrow
Professor &lt;professor@uetpeshawar.edu.pk&gt;
Apr 16, 2020, 2:32 PM
to me
Dear students,
There will be no class tomorrow.
 </td><td>
No Class Tomorrow
Professor &lt;professor@uetpeshawar.edu.pk&gt;
Apr 16, 2020, 2:32 PM
to me
Dear students
There will be no class tomorrow.
 </td></tr>
<tr><td colspan="2">Check the header of the email by clicking on the three dots and selecting “Show original” option (This example is for Gmail, for other email clients, the settings may slightly differ):</td></tr>
</table>





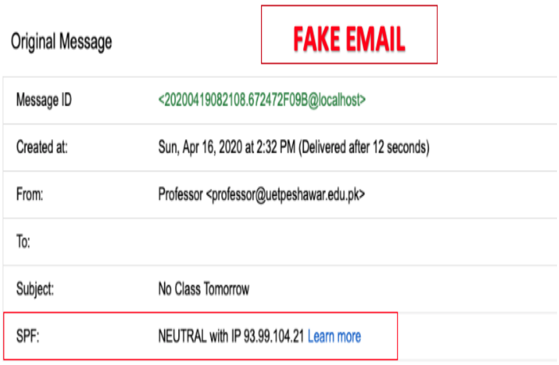
Now, after selecting the “Show original” option, carefully look for SPF, DKIM, and DMARC fields. It will show SPF ‘PASS’ or ‘NEUTRAL’ for genuine and spoofed email but the other two fields will always show “PASS” for genuine emails only.



Original Message

GENUINE EMAIL

Message ID	<CAFgE+JTxugyrUA+tMvHXaXwU976xk6UaTy88cbGr+cPd2merYQ@mail.gmail.com>
Created at:	Sun, Apr 16, 2020 at 2:32 PM (Delivered after 12 seconds)
From:	Professor <professor@uetpeshawar.edu.pk>
To:	
Subject:	No Class Tomorrow
SPF:	NEUTRAL with IP 209.85.220.65 Learn more
DKIM:	'PASS' with domain uetpeshawar-edu-pk.20150623.gappssmtp.com Learn more
DMARC:	'PASS' Learn more



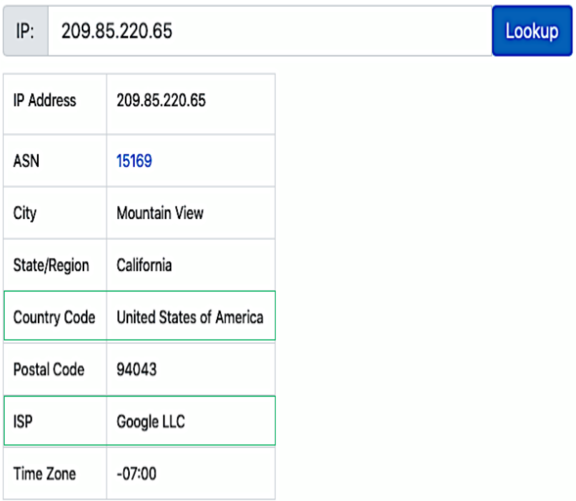
Original Message

FAKE EMAIL

Message ID	<20200419082108.672472F09B@localhost>
Created at:	Sun, Apr 16, 2020 at 2:32 PM (Delivered after 12 seconds)
From:	Professor <professor@uetpeshawar.edu.pk>
To:	
Subject:	No Class Tomorrow
SPF:	NEUTRAL with IP 93.99.104.21 Learn more

You can also check the IP address by any online IP address lookup.

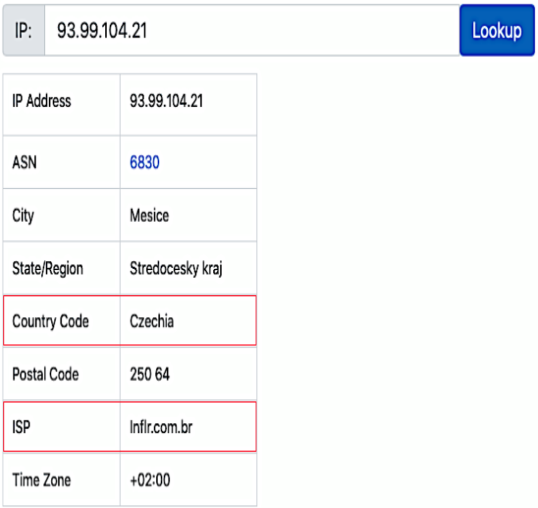
GENUINE EMAIL



IP: 209.85.220.65

IP Address	209.85.220.65
ASN	15169
City	Mountain View
State/Region	California
Country Code	United States of America
Postal Code	94043
ISP	Google LLC
Time Zone	-07:00

FAKE EMAIL

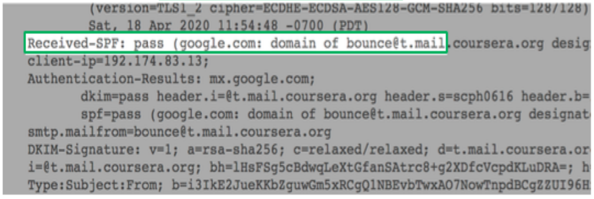


IP: 93.99.104.21

IP Address	93.99.104.21
ASN	6830
City	Mesice
State/Region	Stredocesky kraj
Country Code	Czechia
Postal Code	250 64
ISP	Inflr.com.br
Time Zone	+02:00

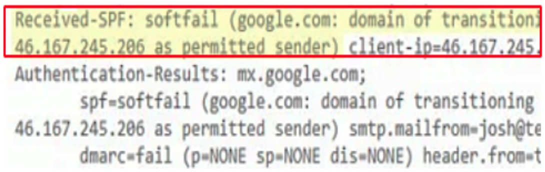
Check the field "Received-SPF" in the header details. The value for genuine email should be “PASS", “NEUTRAL” while for fake emails the value should be "FAIL", "SOFTFAIL" or sometimes “NEUTRAL”.

GENUINE EMAIL



```
            (version=TLS1_2 cipher=ECDHE-ECDSA-AES128-GCM-SHA256 bits=128/128)
            Sat, 18 Apr 2020 11:54:48 -0700 (PDT)
Received-SPF: pass (google.com: domain of bounce@t.mail.coursera.org desig
client-ip=192.174.83.13;
Authentication-Results: mx.google.com;
       dkim=pass header.i=@t.mail.coursera.org header.s=scph0616 header.b=
       spf=pass (google.com: domain of bounce@t.mail.coursera.org designat
smtp.mailfrom=bounce@t.mail.coursera.org
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=t.mail.coursera.or
i=@t.mail.coursera.org; bh=lHsFSg5cBdwqLeXtGfanSAtrc8+g2XDfcVcpdKLuDRA=; h
Type:Subject:From; b=i3IkE2JueKKbZguwGm5xRCgQ1NBEvbTwxAO7NowTnpdBCgZZUI96H
```

FAKE EMAIL



```
Received-SPF: softfail (google.com: domain of transitioni
46.167.245.206 as permitted sender) client-ip=46.167.245.
Authentication-Results: mx.google.com;
       spf=softfail (google.com: domain of transitioning
46.167.245.206 as permitted sender) smtp.mailfrom=josh@te
       dmarc=fail (p=NONE sp=NONE dis=NONE) header.from=t
```