



UNIVERSITY OF COLOMBO SCHOOL OF COMPUTING

IS2109 Information Systems Security - Practical 3

Secure Web Browsing

Instructions:

- **Submit answers for all the following questions. Clearly mention the Question Numbers.**
- **You must submit your answers as a PDF document named as P3_GroupNumber (E.g. P3_Group 5)**
- **Only one document should be submitted from a group and make sure to mention the index numbers of the group members at the end of the document.**

1. Google Docs

1. Are Google Docs secure? How? And To what extent?
2. Create a Google doc for the report of this assignment. It should be viewable to anyone who has the link but not allowed to download and print. Also share it with one of your friends who can edit this document but he/she cannot change the access rights and add more people. At the end, provide a screenshot to prove your work.
3. Does that document really belong to you? Explain your answer referring to the terms and conditions of Google.
4. How DropBox, iCloud and SkyDrive differ from Google Drive?

2. Facebook

1. What are the security implications in this post and what context does it really matter?
2. Assume you delete your profile picture from your facebook account. Does that mean it's really deleted from facebook servers?
3. Assume that you have been consulted by a mother because her child is using Facebook and she needs you to advise how to keep her child away from bad things on Facebook. Explain your suggestions under the following sections.
 - i. What if you advise not to allow her child to use Facebook.
 - ii. If the child is not a teenager.
 - iii. If a child is a teenager.
 - iv. What can be reported? And how?
 - v. How to monitor Facebook usage?
 - vi. What if the child is using a fake account?
 - vii. If you are assigned to design a Facebook application for children, what restrictions would you enforce in there?

3. Chat Apps

1. Compare and contrast the security features in Viber, Whatsapp, Telegram
2. Can someone see your skype communication in plain text (online)?
3. Can someone access your skype chat history without login to your account (offline)?
4. In national security perspective what are the threats behind these kinds of apps?

4. Email Security

As email has become central to business communications, attackers have continued to find new ways of using email to breach corporate security. From more routine email threats like viruses and spam to advanced targeted attacks like phishing, spear-phishing and wire transfer phishing, organizations must combat an increasingly varied onslaught of attacks. Malicious email remains one of the most significant and ongoing computer security threats that we face. Cybercriminals use a variety of email-based attacks to deliver malware, lure victims to malicious websites, and steal login credentials, and organizations everywhere need to understand these threats and how to implement effective safeguards.

1. Understand the concept behind tracking an email
 - i. What do you understand about e-mail tracking?
 - ii. What are the benefits from tracking an email?