16-124-836
Marcel Matti ZAUDER

11.3 Question 3

11.3.A What would be your immediate reaction on such incident?

The first thing I would do is to send an email to all students and employees of the University of Bern that there was a phishing attack and all should change their passwords in order to ensure the security. Also I would advice everyone to check if any misbehaviour was done with their accounts and in that particular case should contact the "security team" of UniBe.

11.3.B You can see the phishing email from question A in the figure. What's suspicious about it?

The first thing that is particular is that the email address is *security@u***m***ibe.ch*. As there can't be any spelling errors in email addresses this is very suspicious. Furthermore, the IP address the link points to can be checked and it can be determined that his IP address is located in Vietnam which is most definitely not the place where the unibe servers are located at.

11.3.C You want to make the University less prone to phishing attacks. What would you do to raise the awareness of the students and employees so that there's a lower chance that they will be fooled by such emails in the future?

The most important thing is to keep the students and employees informed. Therefore, one must keep updated with the latest phishing techniques and inform the users about new attack opportunieties and ways to prevent it, like not clicking on any link stated in an email without verifying the integrity and confidentiality. Additionally, the users should be adviced to not handing out personal information if stated to do so in an email.