Software Development Unit 3, 1.1

Anna Legaspi

# I can take appropriate steps to avoid risks when working with collaborative technology, in line with relevant guidelines

It’s important to protect one own’s personal data and information from cyber criminals. With everyone connected online and to the cloud, the opportunity for data theft is a serious problem. There are multiple ways to prevent this from happening.

## Anonymity

The first step is to ensure that personal and sensitive information is not shared in the web or cloud. This includes information such as full name, address and date of birth. Identity theft is prevalent and there are people that need to pretend to be someone else to obtain credit and pass applications. I have seen young adults photograph their first debit/credit card (front and back) and sharing this to social media. Needless to say, other people took advantage of this and the credit card was maxed out after a few minutes. Great care should also be taken when sharing bank and card details online.

When connected to public WiFi, all the devices connected can be linked. This opens the possibility for hackers to access personal details on other connected devices. To prevent this from happening, the use of VPN (Virtual Private Network) can help encrypt information being sent over the WiFi whilst simultaneously masking the IP address. I personally use Nord VPN for my personal PC, just to maintain anonymity even if I’m not connected to a public WiFi. This stops my broadband provider from keeping a record of my online activity.

## Password Security

Passwords are becoming easier to hack, especially weak ones. I work in a finance company and have access to customer’s personal data which means my work password requirements have to be robust and complicated. They require a combination of special characters, lowercase and uppercase, and a minimum number of words to have an effective password. To login to my work laptop requires Two-factor-authentication (2FA) For my own personal account, I use a strong password coupled with 2FA.

## Device health and safety

IT devices software are constantly exposed to potential viruses, malware and phishing. When surfing online and downloading information, it’s possible to download a virus by mistake, or even from an unsuspecting e-mail with a virus attachment. It’s vital to ensure that Desktops, tablets and phones all have a good security software to protect from malicious attacks. Not doing so can compromise the data within the device or can even corrupt the operating system.

## Acceptable use policy

Most websites have an acceptable use policy. These policies state how the website or service is to be used. For instance, if I were in possession of confidential information, I need to have due diligence in protecting that information and making sure that it’s not shared to the public. If I were to collaborate with other stakeholders, I need to interact with good behavior and use appropriate language, especially when communicating via social software such as Cisco Jabber, Microsoft teams or Zoom.

## Copyright

If I were to share or use someone else’s original work, I need to make sure that I cite references and give credit. Failing to do so is plagiarism and will impact my reputation and the company I’m representing if this takes place. In worst case scenarios, I or my company can be sued for not obtaining relevant permissions.