PUNJAB UNIVERSITY JHELUM CAMPUS

Name: Noman Shoaib

Roll no: BSCS-F19-M-86

SEMESTER :4th

Subject: Compiler construction

Section: B

DATE: 23-06-2021

**Precautionary Measures**

1. **Don’t access personal or financial data with public Wi-Fi.**

This may seem like a no-brainer, but you’d be surprised how many people check their bank accounts or make purchases with a credit card while using public Wi-Fi. It’s best to do those things on a secure connection.

1. **Turn off anything you don’t need.**

Hackers can use certain features on your system to get at your information, location or connection. So, instead of keeping your GPS, wireless connection and geo-tracking on all the time, just turn them on when you need them.

1. **Choose your apps wisely.**

Only download apps from trustworthy sources that have established a good reputation. Make sure you update your software and apps regularly and get rid of old apps you don’t use.

1. **Use a password, lock code or encryption.**

Make sure your passwords are at least eight characters long, with a mix of upper and lower case, and include numbers or other characters, and never use the auto-complete feature for passwords. You can use the storage encryption feature on your system to protect your private data, and set your screen to timeout after five minutes or less.

1. **Be skeptical about links and attachments.**

If you’re not sure about the source, don’t use the link or open the attachment.

**If u got hacked…**

1. **Quarantine Your PC**

Life Wire suggests you isolate the infected computer as soon as possible. As long as you’re connected to the internet, the hacker has access to the device and its directory. No need to cut the network cable. Simply unplug your computer from the network and avoid any kind of wireless or physical connection. The goal is to prevent the virus from spreading! Make sure you’re offline and turn all Wi-Fi connections off, both by software and hardware. Some laptops even have a switch for this. Why disconnects hardware? Hacking software is sophisticated and can make your computer seem like you are disconnected while the malware continues to wreak havoc in the background. This is why it’s increasingly important to ensure your sensitive data is encrypted and that your devices are protected by security management software.

1. **Change your passwords**

According to Better buys, “it only takes five hours to decipher a password that’s 6 basic characters long”. On the other hand, if you pick a password that’s 12 characters long, it’ll take a massive **two centuries to crack.** That’s why the first step is: change your PC’s access password. And then change all your passwords using an unaffected computer or smartphone. I mean it. Email, social, subscriptions, etc. Every service you have access to holds precious information, including billing information and personal data. According to CybInt, 95% of breaches are caused by human error. What this means is that you could have unknowingly given enough identifying information for a hacker to guess your password. It could also mean that you’ve mistakenly run an infected program or document that contained malware. Verizon found that 45% of breaches featured hacking 17% involved malware and 22% involved phishing. How many of your accounts use the same password or variations of it?*One* password could be enough to grant access to all sorts of accounts. So, double-check its strength and think it through. According to Cybersecurity & Infrastructure Security Agency (CISA), there are a few criteria you should fallow when creating a safe password.

* It should be between 8 and 64 characters (longer the better).
* It shouldn’t include personal information, like your name, your birthday, or your company’s name. Get creative with it, have fun!
* It has to be *different* from your previous ones and from your other passwords.
* If possible don’t include complete words.
* Use mnemonics and memory techniques. For example, instead of using “hoops” try “IlTpbb” for “[I] [l]ike [T]o [p]lay [b]asket[b]all. “Create it using characters from all four categories: lower and upper case, numbers, and symbols.

Using a password manager makes changing passwords a breeze and also gives you added security benefits such as Two-Factor Authentication and issuing temporary passwords

1. **Alert those connected to you**

Hackers try to spread by breaching an individual and then targeting their network...  Intego also explains that the reason is simple: hackers use your email to send messages pretending to be you because your friends are more likely to open messages from you without thinking

So, before you spam a virus to your family, friends, and co-workers… Give a heads up. Protect your core group and notify them immediately to avoid spreading the attack.