Survey Analysis

While it is important for everyone to be aware of how to safely protect themselves online, some groups are markedly more vulnerable than others. School and college going students also fall under this category as they are one of the major users of the internet and related services. Thus, as part of our outreach program, we decided to gauge the levels of awareness about issues pertaining to cybersecurity among the students of BITS-Pilani, a technical university in Pilani, Rajasthan.

Methodology

An online questionnaire survey (Appendix A-1) was designed by the team using Google Forms. This was then circulated among the engineering students in their first year, via WhatsApp Messenger and through e-mail. In the span of two days, 200 responses were logged by the server, following which we stopped accepting responses. The data obtained has been presented and analysed in subsequent sections.

Analysis

Type of Attack Experienced

Through the survey we found that only 19% of the respondents had never faced any form of online attack. This population could be the ones who are safe, however it is more likely that they are not well-informed about the different categories of cyberattacks.

Nearly 60% of the respondents were victims of spamming. Since most of students end up giving their email-ids on various websites, they become more vulnerable to spam. A reassuring fact however is that only 12% of respondents, were victims of phishing. This could be an indication of increased awareness among students. Around one-third of the respondents had encountered fake accounts. This could be because most students in that age group (18-21 years) have accounts on social networking sites, like Facebook, Instagram and Snapchat, were creation of fake accounts is rampant. Password and Data theft is caused usually due to negligence of the user or systemic failure at the server end. It seems that the rather large fraction of respondents (22%) who have experienced this recently could be due to the recent security breach in Yahoo! Inc. Similarly the recent rise of the ransomware malware, WannaCry, could be the reason for 13% of respondents to have experienced this usually corporate cyberattack.

Passwords

All forms of accounts online have at least a single-step authentication method, which is usually a password. While many websites force users to use a certain type or composition of passwords, others allow for variations, which may lead to easily decodable passwords.

Type

It is often advised that we use a password composed of Uppercase alphabet, Lowercase alphabet, Numbers, Symbols in a random order of a significant length, so that it cannot be decoded by brute-force cracking software. It is also advised not to use simple known strings, like birthdates, anniversaries, ‘1234’, “qwerty”, etc. From our survey, it was found that 92% of our respondents choose to keep alpha-numeric passwords. This is a good sign and shows awareness among the students about keeping a strong password.

Also, using similar passwords for all accounts is a common error among students. While it makes it easy for one to remember all their passwords it also puts all their data at a higher risk. From our survey, we have gathered that 54% of respondents use similar passwords for all accounts. This is not a very good practice and students must be made aware of the same.

Frequency of Changing

Another guideline for a secure password, is to keep changing it frequently. While there is no ideal length of time that one should keep a password for, it is advised that passwords for accounts containing sensitive information, like online banking accounts should be changed monthly. Many websites also prompt users to change their passwords periodically.

Nearly half of the respondents said that they changed their passwords only when prompted. As these accounts are likely to be primarily social media accounts, this frequency although not recommended, is relatively harmless. The remaining half change their passwords quite frequently with around 42% changing every semester and approximately 38% changing their passwords annually.

Saving Passwords Online

Many browsers, like Google Chrome, Mozilla Firefox and Microsoft Edge allow the users to save passwords. While this is usually a very secure practice, it is not advisable to do so on public computers, or for accounts containing sensitive information. Even on home computers, it is possible for someone to misuse this access, hence, it is better to be safe.

Logging in on Public Networks

Many times, students are often forced to login to their accounts in public places, like cyber cafes, libraries, airports. In such cases, it is advisable to be very vigilant as public networks have minimal protection and can leave your data susceptible to theft. Using an incognito browser is effective for some threats, however, if the computer you are using, or the network you are connected to have been tampered with, using it will be of no use. Unless absolutely required, it is not advisable to use public computers at all, however, in case it is necessary, prefer one with a reliable antivirus software in a reliable place.

From Figure, nearly two-thirds of the respondents log in to their personal accounts on public networks, around half of them on incognito mode. While this is not a very safe practice, circumstances may mandate the situation.

Use of Antivirus Software

As mentioned in chapter, many students will be reluctant to download paid antivirus software, especially on mobile phones and tablets.

As expected, nearly 75% of the respondents have antivirus on their laptops, while only 35% have it installed on their phones. Similarly, around one-third of those who use tablets, have antivirus software installed on it. The reason why a large percentage of smartphone users do not use antivirus applications could be that very few of the applications are free and it is rare for students to spend money on mobile applications. The large percentage of laptop users owning antivirus software could be attributed to the fact that many trial versions are available for free online.

Frequency of updating antivirus

As technology gets more sophisticated, more serious threats emerge. To combat these, companies like ours frequently update our software so that they are better suited to protect the device. Always having an updated version of the software is a safe practice.

Around 60% of the respondents who use antivirus software, update it as soon as an update is available. A possible reason could be that most software have an auto-update feature. A significant percentage, 18.7% update only when it is absolutely required. This could be because software updates often take up disk space, which is undesirable for many.

Saving Card Details Online

With the growing success of e-commerce, nearly every store online allows for multiple methods of payment including credit and debit cards. Thus, browsers and websites, both allow for their users to save card details online, thus saving the task of typing it in at every instance.

Although most students among the sample space own either a debit card or a credit card, online purchases are not always made using them. Thus, not many people would feel the need to save card details online. This is supplemented by the fact that people are even otherwise, reluctant to save card details online, due to qualms about security.