NAME ⇒ VISHAL UJJWAL

COURSE ⇒ BCA 5(I)

ROLL NO ⇒ 11211172 (57)

SUBJECT ⇒ INFORMATION SECURITY AND CYBER LAWS

Ans1 MCQ

1) (d) none of the above

2) (a) ~~Software~~ Spyware

(3) (a) Encrypted Signature of a Sender

(4) (c) Cyber laws

(5) (a) only an alphanumeric

(6) (c) All

(7) (a) hash value

(8) (c) The characters are exchanged

(9) (b) to make even no of letters

(10) (b) No of characters in words

Ans: Do a Security Checkup:

- Block someone from using your account without any permission
- Alert you if there's suspicious activity on your account
- Recover your account if you are ever locked out

UPDATE YOUR SOFTWARE:

if your browser, operating system, or apps are out of-date, the software might not be safe from hackers.

- Make sure you're using the latest version of your browser
- Make sure you're using the latest version of the operating system on your device or computer
- Make sure you're using the latest version of the apps on your phone or computer.

USE UNIQUE, STRONG PASSWORDS

It's risky to use the same password on multiple sites. if your password for one site is hacked, it could be used to get into your accounts for multiple sites.

- A password manager can help you generate and manage strong, unique passwords. Consider using one from Chrome or another trusted password manager provider
- That way, you will know if a site is impersonating Google, and you can change your password if its get stolen.

4) Remove apps and browser extensions You don't need

As more apps are installed on a device, it can become more vulnerable. install only essential apps and browser extension on devices that have access to sensitive information. Avoid installing Unknown apps or apps from unknown Sources to protect Your device and pesonal info.

5) Protect against Suspicious messages and content

Hackers Can use emails, text message, Phone Calls, and web pages to pretend to be institution, family members, or Colleagues

- Never give out your passwords. Google will never ask for your password in an email, messages, or phone call.
- Don't reply to Suspicious emails, texts, instant message, webpages, or phone calls that ask for Your personal or financial info.
- Check if a Gmail message might be fake.
- See if the email address and the sender name match.
- Google Chrome and Search are designed to warn you abo Suspicious Content and unwanted Software.

H/W 2

1) Accessing browser history

- Your browser history is a veritable map of where you go on the internet and for what purpose. And it's not only possible to tell where you've been, but when you've been there, establishing your behavioral patterns. Use incognito mode (Private browsing) since no harvestable data is stored (if you must use a public system, always make sure to do so with incognito mode).

2) Harvesting Saved login Credentials

- Saved login paired with bookmarks for the associated sites you visit are a deadly combination. Two mouse clicks might be all it takes for a criminal to have access to your banking/credit card websites. Saved credentials associated with your email account is basically like kryptonite to superman in a scenario like this.

3) Obtaining auto fill information

Autofill information can also be deadly. Chrome can save your home address information to make it easier to shop online, but what if your device fell into the wrong hands? Now an attacker knows where you live - and probably whether you're home. Turn off autofill for any confidential or personal details.

4) Analyzing Cookies

Cookies (files stored locally which identify users/link them to sites) are another potential attack vector. like the browsing history, they can reveal where you go and what your account name might be. Disabling Cookies is touted as potential Solution, but this has been a problematic "fix" for years since many sites depend on Cookies or at least severly limit your functionality (or possibly annoy you with nagging prompts) if these are turned off. instead, purging Cookies periodically can help protect you, though be prepared to enter information repeatedly as prompted by websites.

Ans 4

```
include < Stdio.h >
include < Conio.h >
  Using namespace Std;
  String generate OTP (int len)
  {
     Staing str = " abcdefghijklmnopqrstuvwxyz"
                  "ABCDEFGHIJKLMNOPQRSTUVWXYZ" );
       int n = Str.length();
        String OTP;
  for (int i=1; i<=len; i++)
     OTP.Push_back (Str [rand() %. n]);
       return (OTP);
  }
    int main ()
  {
       Srand (time (NULL));
       Int len = 6;
Printf ("Your OTP is - %.S", generate OTP(len).C-
              Str ());

       return (0);
  }
```