Secure Online Profile Worksheet

To complete this worksheet, you will need to refer to your answers to the *Online Profile Risk Assessment Worksheet*.

Question 1:

If your personal information is easily identifiable via your social media sites you use, identify options within each site that could help prevent or mitigate the security risks this causes.

For example, you may be able to adjust your Facebook settings to make all posts private by default.

Each social media site will have different settings and options for you to control who sees your information. List the site and the option(s) available:

|  |  |
| --- | --- |
| Social Media Site | Options/settings/controls to control visibility of personal information (i.e., privacy settings) |
|  |  |
|  |  |
|  |  |

Question 2:

Reusing passwords and weak passwords two common security threats – especially if your email address appears in a data breach.

Identify which of your social media accounts may need stronger/unique passwords, and whether the site allows you to use two-factor authentication.  
(Two-Factor Authentication, or 2FA, might be an SMS code, email verification, or a code from an authentication app like Google Authenticator)

|  |  |  |  |
| --- | --- | --- | --- |
| Social Media Site | I use a unique and strong password for this site | 2FA is available | 2FA is turned on |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Question 3:

Malware is a common method hackers use to steal personal information. Ransomware is also very damaging to both companies and individuals. But protection against these threats may be moot if you ‘leave the front door open’.

Review the security of your personal devices and answer the following questions:

|  |  |
| --- | --- |
| **Anti-Virus or Anti-Malware Software** Identify any anti-virus or anti-malware software you currently use.  If you do not use any, identify some software you can install on your device(s)  Include your Home PC, Mobile, and any other device |  |
| **Software Updates**  Hackers, viruses and malware may utilise unpatched bugs in software to gain access to systems or spread. These exploits are well known (see <https://www.exploit-db.com/>)  Review your Home PC and Mobile (and any other device) and list any software that needs updating.  (For mobile, list only the Android/iOS operating system) |  |
| **Default Passwords**  Leaving the default password on your home devices (wifi router, security cameras, smart devices, etc) is a big security risk. Hackers may discover these devices (see <https://www.shodan.io/>), log in using the default password, then gain access to your home network. List all your devices in your home and indicate if they are using the default password. |  |

Question 4:

Social media sites rise and fall in popularity. We may find our favourite site changes over time, or we no longer use some sites as much as we once did.

When we stop using a social media site, we can sometimes forget about the information we’ve shared about ourselves on that site. But that information doesn’t go away and may be viewable by more people than we expect.

Identify any unused online accounts that could be deleted. (You do not need to delete your account, but you may wish to consider it)

|  |  |
| --- | --- |
| Social Media Site | Is my account unused / Could I delete my account? |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Question 5:

For this question you are asked to reflect on your online security.

Write 200 - 300 words on changes you could make to secure your online presence and personal mobile and computing devices. You may refer to your answers to any of the questions above.