Data Privacy – 10 Tips to Keep Your Data Private

1. **Create Strong Passwords**
   The days of using the word password or your name as your password are long gone. To help ensure your passwords are secure, at a minimum use the "8-4 rule". This means use at least 8 characters with 4 variations such as lower case, upper case, numeric, and special characters. At a minimum ensure the password used for your email is different than all other accounts. If the password to your email is compromised, resetting other online accounts becomes much easier as your email is mined for information.

2. **Don't Overshare on Social Media**
   Do you know where the answers end up for Facebook questions such as "what was your first car" "or where did you go to school?" Questions like this are commonly used in passwords or as password reset questions. Also, posting information such as your physical location, hobbies, interests, and kids names can be used in social engineering attacks. To help reduce your risks ensure your profiles are set to only friends, monitor who follows you, and avoid revealing personal information you don't want to be shared without your permission.

3. **Encrypt and Password Protect Your Devices.**
   Imagine you have your laptop in your car, and you run into a store. When you get back you notice that your laptop was taken from your front seat! Even if you have your laptop password protected it doesn't protect you from data theft. Internal storage can easily be removed and read by anyone if your device isn't encrypted. Most operating systems (like Microsoft's BitLocker) now offer solutions to encrypt your devices. If your device contains sensitive information, data encryption will help prevent unauthorized access to it.

4. **Don't Open or Click Links in Unexpected Emails**
   Phishing is an all-too-common method to ransom your data, get you to divulge sensitive information, or pay fake invoices. Look out for emails where the sender's tone seems off or unfamiliar, the email address doesn't match what you normally receive, or an attachment was sent that you were not expecting.

5. **Ensure Sites on Which You Share Identifiable Information Have SSL Encryption.**
   If a website exists, this doesn't mean it's secure. To ensure the site has encryption enabled, look at the top of your internet browser and ensure the site you are using has https: before the address. Also, there should be an icon beside the address that you can click on to ensure their certificate is valid and secure.

6. **Be Careful When Allowing an App Access to Information on Your Phone.**
   A lot of phone applications prompt you for permission to use things like your microphone, camera, location, or contacts. Ask yourself before approving these questions: Does the application really need this information for what you are using it for? Also, only download applications from the appropriate device app store to ensure they have been through a vetting process.

7. **Patch and Patch Often**
   Most manufacturers of electronic hardware or operating systems have patch schedules or push out patches to devices. If you are prompted to patch your device, do not hesitate as these patches may fix vulnerabilities to the operating systems that leave you open to attack. Many software vulnerabilities allow for remote takeover of computers without your knowledge, so the general rule is to patch and patch often. For Microsoft, patching your operating systems is as easy as typing update in your start menu and clicking on check for updates.

8. **Be Careful When Connecting to Public Wi-Fi**
   Do you connect to free Wi-Fi whenever you see it? Did you know that if you connect to malicious Wi-Fi, hackers can position themselves between you and the website you are connecting to and collect every web page submission, file, and email you send? When connecting to Wi-Fi ensure it is the correct published Wi-Fi provided by the establishment.

9. **Enable Multifactor Authentication When Possible.**
   Multifactor authentication is the easiest and best method to ensure your account is secured by more than a username and password. This additional layer of security usually comes as an additional code sent via a text or authentication app, The code is needed in addition to your username and password to login to an account. If a hacker obtains your account credentials it is very difficult to also obtain this additional layer of security. Most banks, email providers, and social media companies now have this capability.

10. **Protection and Backup, Backup, Backup**
    Finally, install protection on your devices. Trend, Norton, and McAfee are very good starting points to have some protection on your computers. These solutions watch for strange behavior, notify you, and in most cases clear it from your computer. Also, with any device or computer that has data you want to keep, ensure you have a good backup solution in place. Depending on the importance of the data, this could be as easy as using a flash drive and copying what you want to keep and storing it in a fireproof safe. If you want a “set it and forget it” solution that is also fire, flood, ransom, and theft safe look, into solutions such as Carbonite, Backblaze, or even One Drive to make automatic backups.