Cyber-Hygiene in 8 Steps

Step 1: Don’t get phished!
Before clicking on a link on email or social media, think twice: is this legitimate, is this unusual.

Step 2: How good is your password?
It is probably not that good. Passwords have to be long and complex (at least 12 characters). The most important rule: use a password manager!

Step 3: Update your Microsoft Windows, your antivirus and your browser.
Everything on your computer and phone should be up-to-date, even if not connected to the internet all the time. If you need internet credit, contact an IT person.

Step 4: Install an antivirus and uninstall unnecessary software
Keep it up-to-date. There are no need for several antiviruses, just one that works.

Step 5: Don’t take USB devices you don’t know
They very often contain viruses. Keep them safe and scan them with an antivirus. Don’t use it if you have any doubt!

Step 6: Make backups
If something and happen (and something will happen eventually), backup will save your a huge amount of time. Make backup regularly and keep them safe.

Step 7: Keep your desk clean and your computer secured
Protecting your devices physically is as important as protecting your accounts on the internet! Think about: not leaving your laptop or phone unattended in a public place, protect them with a password at all time, and lock them when leave from work.

Step 8: Be extra-cautious when using public wifi
Free wifi might give you free internet, it can also give you free viruses. Preferably use 3G hotspot to access your account or for business activities.