Top 10 most common security mistakes

1. **Passwords on Post-it Notes:**

After accepting the importance of having a strong password to improve on the security of the information most users form and structure their passwords as required but often make the error of writing it down on a post-it for example so they don’t forget or have easier access to the password in case of emergencies and they have forgotten it.

This practice is dangerous and puts the owner of the password at risk of a security breach because this password can also be accessed by unauthorised users.

So when choosing a strong password it should be easily remembered by the owner and should NEVER be written down for all prying eyes to see and attain access.

2. **Leaving your computer on, unattended**

When using a computer in our daily lives whether for personal or work related use most people often leave their computer on when they leave their desk and unattended to thus leaving the computer and the information stored on it vulnerable to attack or unauthorised access.

So whether you as a user are rushing to the printer or to answer an important phone call you have to always bear in mind the importance of the security of the information on your computer.

Pressing the buttons ‘**Ctrl, Alt, Delete**’ at the same time will enable the user to log off thus protecting the computer’s content when they have to step aware.

This mistake also applies to mobile phones and devices.
3. Opening e-mail attachments from strangers

People often receive e-mail attachments from friends, family or work colleagues on a daily basis but when the e-mail attachment is from a stranger who you as a user cannot deem as a credible source, it is advisable not to open that attachment.

This is because this attachment could be harmful to your computer; it could be a type of attack like a Trojan, worm or a rootkit.

So when faced in this situation please contact the nearest IT support staff and administrator for their advice on what steps should be done when in the work place or simply ignore the attachment and delete it as a security precaution.

4. Poor password etiquette

When choosing a password the strength of the password is very crucial in the protection of information. Users often select weak passwords that are easy to guess for instance: the users name or birthday or simply the number 1 - 9.

These passwords provide easy access to hackers and other unauthorised personnel. Strong password use is encouraged for example using:
- Upper cases in parts of your password
- Numbers
- Punctuation or quotation marks

All these are ways to strengthen a password and reduce unauthorised access.

5. Laptops on the loose

6. Blabber mouths

There are individuals who often bring their work home with them and share it, in this case confidential information from work which poses as a security threat when this information perhaps shared in a restaurant or on public transportation and is over heard and seen by a third party who has no authorisation to listen in on the conversation and may attempt an attack due to the new information he just received.
Therefore people should be tight lipped about confidential information and no share it with anyone else other than the authorised personnel to keep it secure.

Another approach could be signing confidentiality agreements forbidding either party with knowledge of certain information to speak of it without permission.

7. **Plug and play without protection**

Most users when the find access to free wireless internet, they quickly plug in their devices and play whatever show they want or do assignments without having the proper required security protection on their devices such as antivirus and firewall.

By doing this the user’s information is open and vulnerable to attack by unauthorised users and hackers who will take advantage of the situation.

So it is important to always update the security protection (antivirus and firewall) installed on your mobile devices whether phones or laptops to ensure the content is secure from unauthorised access.

8. **Not reporting security violations**

Most people think when they see a security violation taking place for instance someone breaking into a factory or noticing someone snooping and gaining unauthorised access to another person’s computer or perhaps when their computer have been breached and is attacked they quietly and individually solve their attack and proceed thinking that they shouldn’t report because it somehow doesn’t concern or involve them.

This type of thinking isn’t encouraged because if people speak out and report the perpetrators then the information will be protected. Whether it is to the police or the security or IT department in an organisation such incidents and violations should be taken seriously and people should take it upon themselves to protect one another from security threats.
9. **Always behind the times (the patch procrastinator)**

10. **Not knowing internal threats**

In organisations majority of the security threats and breaches are internal rather than external. Whether it is intentional for example stealing confidential information, or damaging equipment done by a disgruntled employee or ex-employee; and unintentional for example a worker opening an attachment from a stranger or giving out personal information like contact details to a stranger on the phone without checking for their authenticity and credentials.

So organisations should be aware of the external threats of security breaches as well as the internal threats which can be more harmful and dangerous to the productivity of the institution.

They should also provide security surveillance in the interior of the organisation so as to monitor the employees work and also having evaluations, team building events such as retreats or camps even counselling so as to easily identify the disgruntled employees and assist them where necessary to avoid any future threats.