Hacking

Hacking

[Home](#) [1] | [Viruses](#) [2] | Hacking | [Backups](#) [3]

what is Hacking? Computer hacking is when someone gets into your files by finding out the details to your computer and unlocking it, getting some software to hack into computers or sending you a virus that will then go into all of your files and the person that is on the other computer can see what you are doing. If someone does hack into your computer they can see what website’s you are going on, passwords and personal information

What damage can Hackers do?
Hackers like to get into computer security without permission. They are cyber criminals. This can mean gaining access to a computer across the internet. Below are ways that they can damage.
Vandalism- they can get into your computer and completely mess it up and leave things there to show that they have been there. They want to look clever, and you will never be able to find out who has done it.
Theft- they can steal personal passwords and personal information that they can then use elsewhere to do even more damage.
Hijacking—many hackers are interested in using viruses and Trojan horses to hijack your computer so they can control it for their own home, so say if your computer was doing something and you were doing completely the opposite, there is a chance that a hacker has got control over your computer, but don’t automatically think that because your computer could just be playing up.
Identity theft—Electronic theft of personal information that can be used to steal financial resources, like your bank details and tax’s
Terrorism—Some experts think that terrorists will eventually launch an attack using hacking techniques, so there will be a huge amount of people trying to get into your computer.

how you can prevent hackers: Identifying entry points-Install proper scanning software programs to identify all entry points from the internet into the internal network of the company. These points have the weakest security controls which a hacker can easily target. Identifying these entry points, however is not at all an easy task. It is better to take the help of skilled ethical hackers who have taken special network security training to perform this task successfully.
Attack and penetration tests-By running the attack and penetration tests, you can identify those vulnerable points in the network that can be easily accessed from both external and internal users. After identifying these points, you would be able to thwart attacks from external sources and correct the pitfalls that could become the entry points for intruders to hack into your network. The test must be done from both the internal as well as external perspectives to detect all the vulnerable points.
User-awareness campaigns-All possible steps must be taken to make all the users of the network aware of the pitfalls of security and the necessary security practices to minimise these risks. You can conduct the social-engineering tests to determine the user awareness. Until all the users are aware of certain factors related to the network, protection cannot be carried out in the true sense of the term.

Source URL: https://theingots.org/community/node/23516

Links
[1] http://theingots.org/community/node/22771
[2] http://theingots.org/community/node/23140
[3] http://theingots.org/community/node/23517