Computer Security

Dr.Ahmed Gadallah

2020

What is Computer Security ?

Computer Security is the process of detecting and preventing any unauthorized use of your laptop/computer. It involves the process of safeguarding against trespassers from using your personal or office based computer resources with malicious intent or for their own gains, or even for gaining any access to them accidentally.

Why Security?

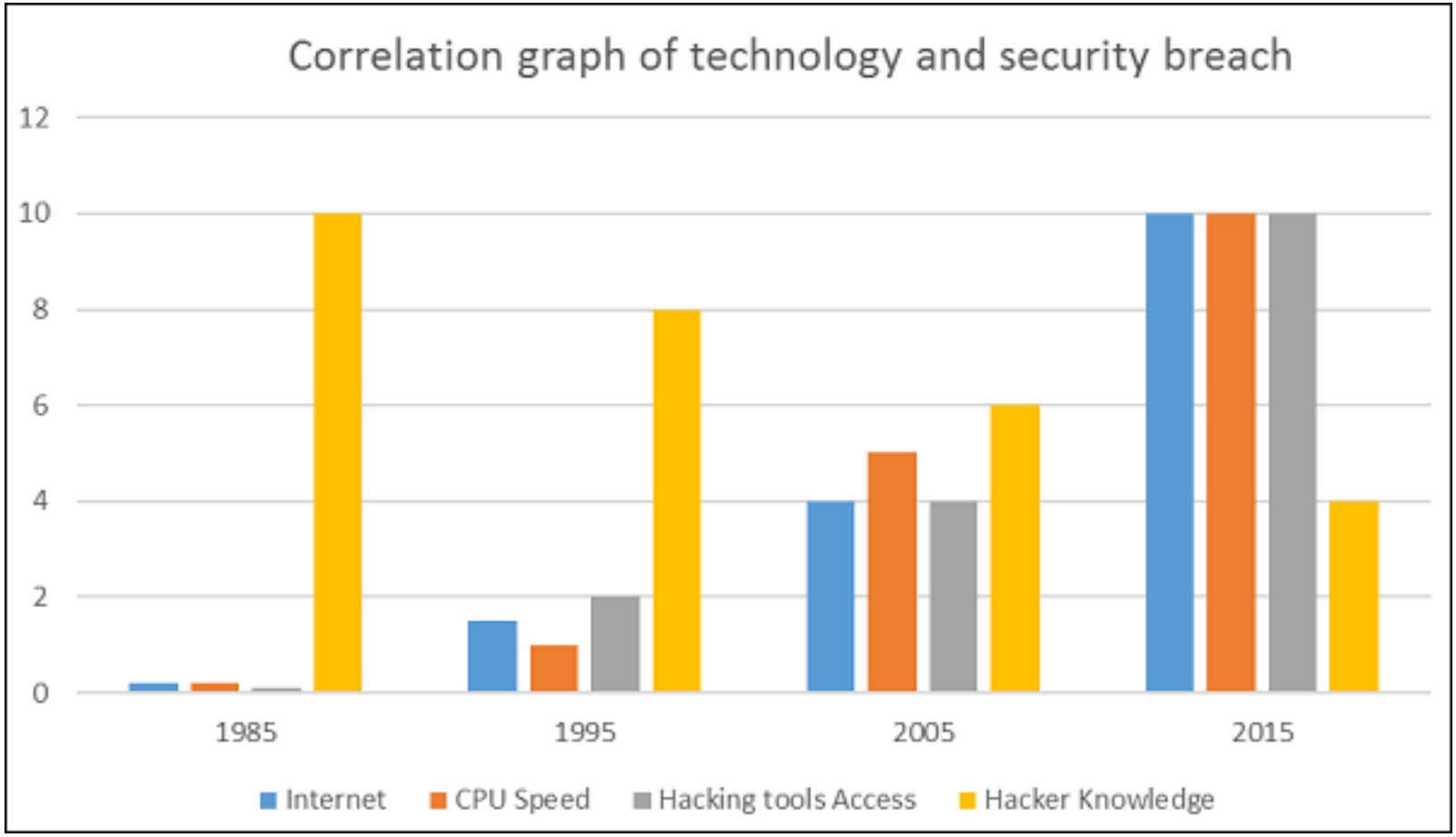
Cyberspace (internet, work environment, intranet) is becoming a dangerous place for all organizations and individuals to protect their sensitive data or reputation. This is because of the numerous people and machines accessing it. It is important to mention that the recent studies have shown a big danger is coming from internal threats or from disappointed employees like the Edward Snowden case, another internal threat is that information material can be easy accessible over the intranet.

One important indicator is the IT skills of a person that wants to hack or to breach your security has decreased but the success rate of it has increased, this is because of three main factors :

- Hacking tools that can be found very easily by everyone just by googling and they are endless.

- Technology with the end-users has increased rapidly within these years, like internet bandwidth and computer processing speeds.
- Access to hacking information manuals.

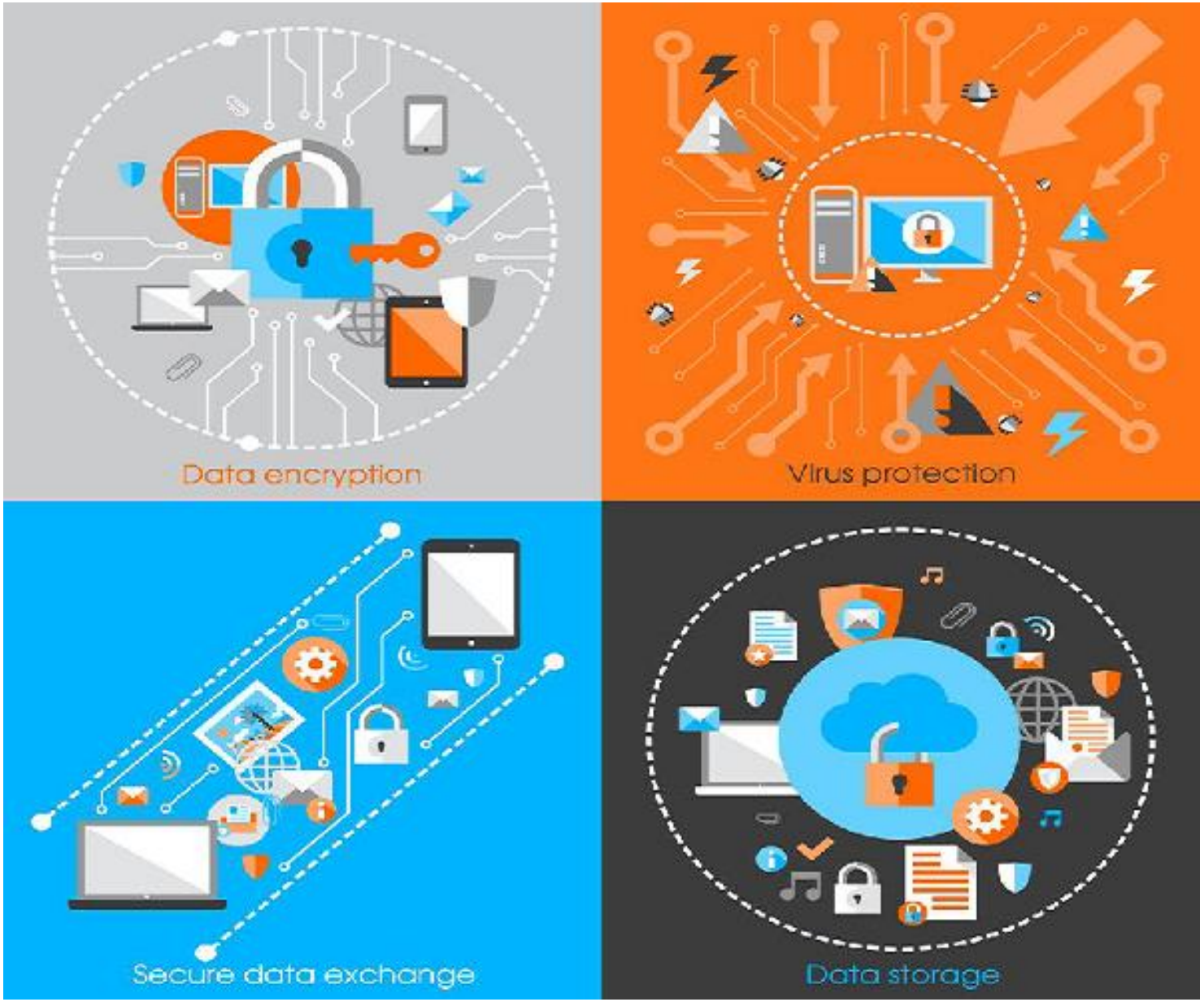
Since locking down all networks is not an available option, the only response the security managers can give is to harden their networks, applications and operating systems to a reasonable level of safety, and conducting a business disaster recovery plan.



What to Secure?

Let’s see this case, you are an IT administrator in a small company having two small servers staying in a corner and you are very good at your job. You are doing updates regularly, setting up firewalls, antiviruses, etc. One day, you see that the organization employees are not accessing the systems anymore. When you go and check, you see the cleaning lady doing her job and by mistake, she had removed the power cable and unplugged the server.

What I mean by this case is that even physical security is important in computer security, as most of us think it is the last thing to take care of.


Data encryption
Virus protection
Secure data exchange
Data storage

Now let's go directly to the point of what all to secure in a computer environment −

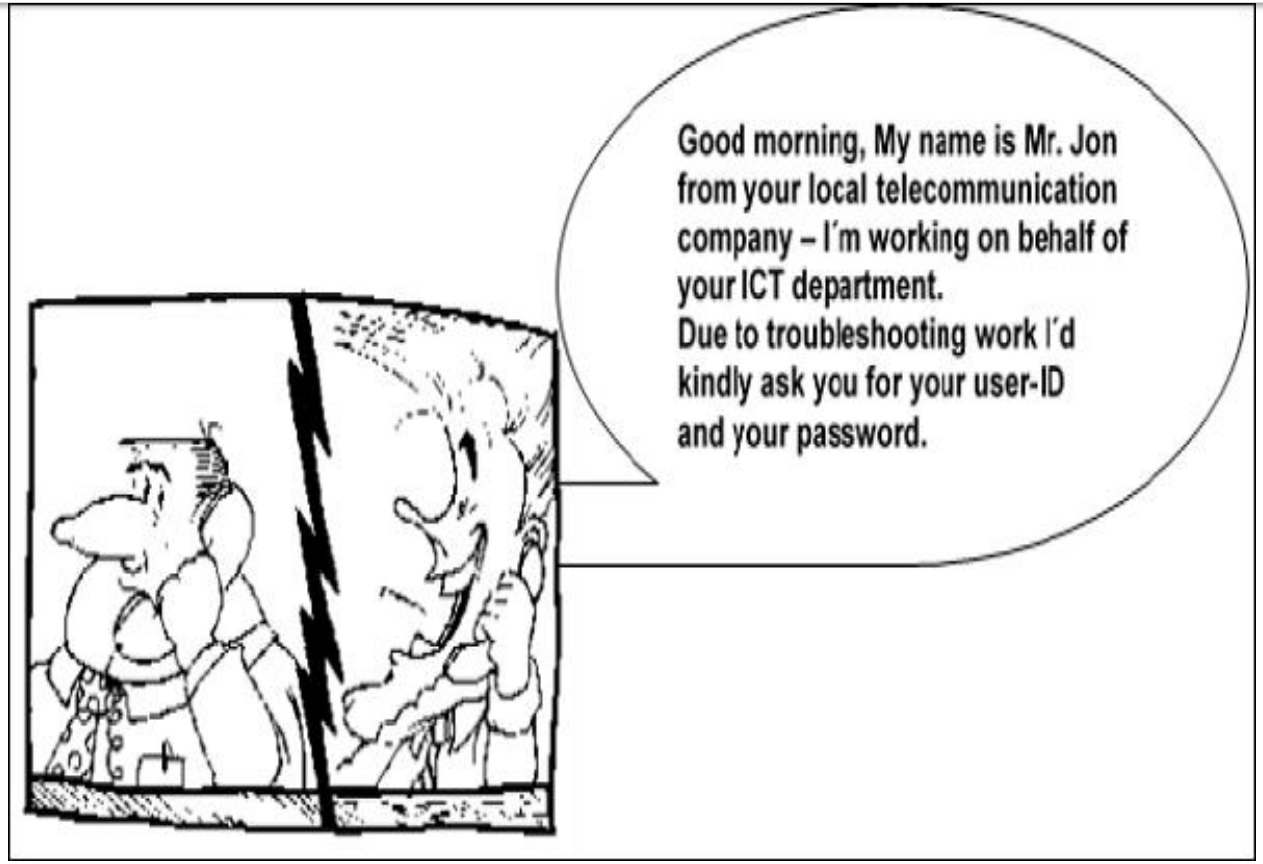
- First of all, is to check the physical security by setting control systems like motion alarms, door accessing systems, humidity sensors, temperature sensors. All these components decrease the possibility of a computer to be stolen or damaged by humans and environment itself.
- People having access to computer systems should have their own user id with password protection.
- Monitors should be screen saver protected to hide the information from being displayed when the user is away or inactive.
- Secure your network especially wireless, passwords should be used.
- Internet equipment as routers to be protected with password.
- Data that you use to store information which can be financial, or non-financial by encryption.
- Information should be protected in all types of its representation in transmission by encrypting it.

What are the Benefits of Computer Security Awareness ?

Do you know in all this digital world, what is the biggest hole or the weakest point of the security?
Answer. It is us, humans.

Most of the security breaches come from uninformed and untrained persons which give information to a third party or publish data in Internet without knowing the consequences.

See the following scenario which tells us what employees might end up doing without computer security awareness –



So the benefits of computer security awareness are obvious as it directly minimizes the potential of you being hacked off your identity, your computer, your organization.

What are Potential Losses due to Security Attacks ?

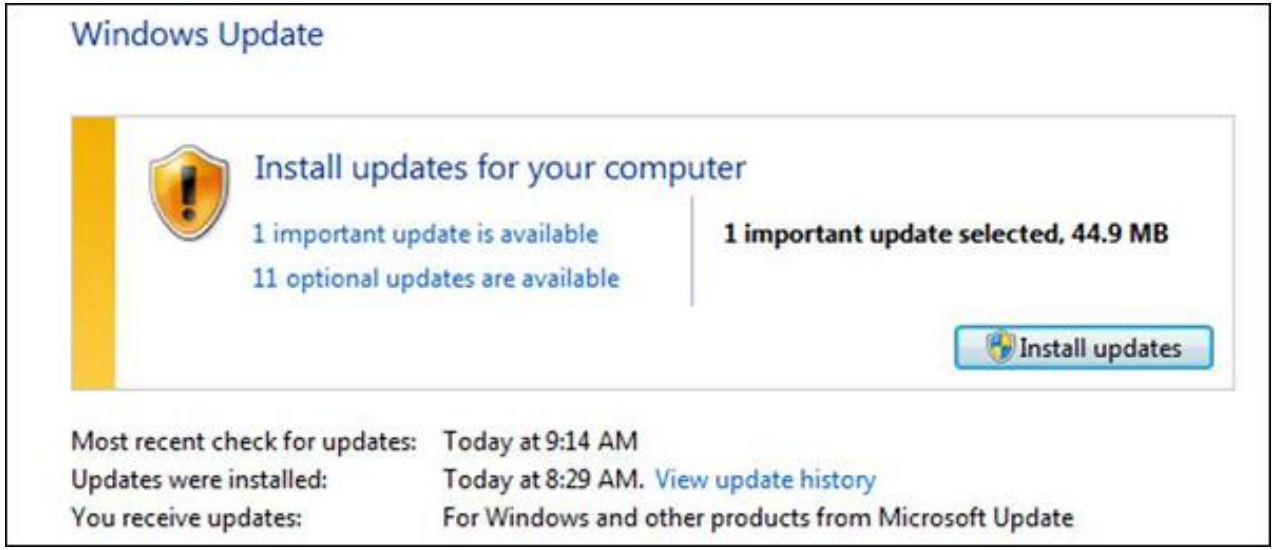
The potential loses in this cyberspace are many even if you are using a single computer in your room. Here, I will be listing some examples that have a direct impact on you and on others −

- **Losing you data** − If your computer has been hacked or infected, there is a big chance that all your stored data might be taken by the attacker.
- **Bad usage of your computer resources** − This means that your network or computer can go in overload so you cannot access your genuine services or in a worst case scenario, it can be used by the hacker to attack another machine or network.
- **Reputation loss** − Just think if your Facebook account or business email has been owned by a social engineering attack and it sends fake information to your friends, business partners. You will need time to gain back your reputation.
- **Identity theft** − This is a case where your identity is stolen (photo, name surname, address, and credit card) and can be used for a crime like making false identity documents.

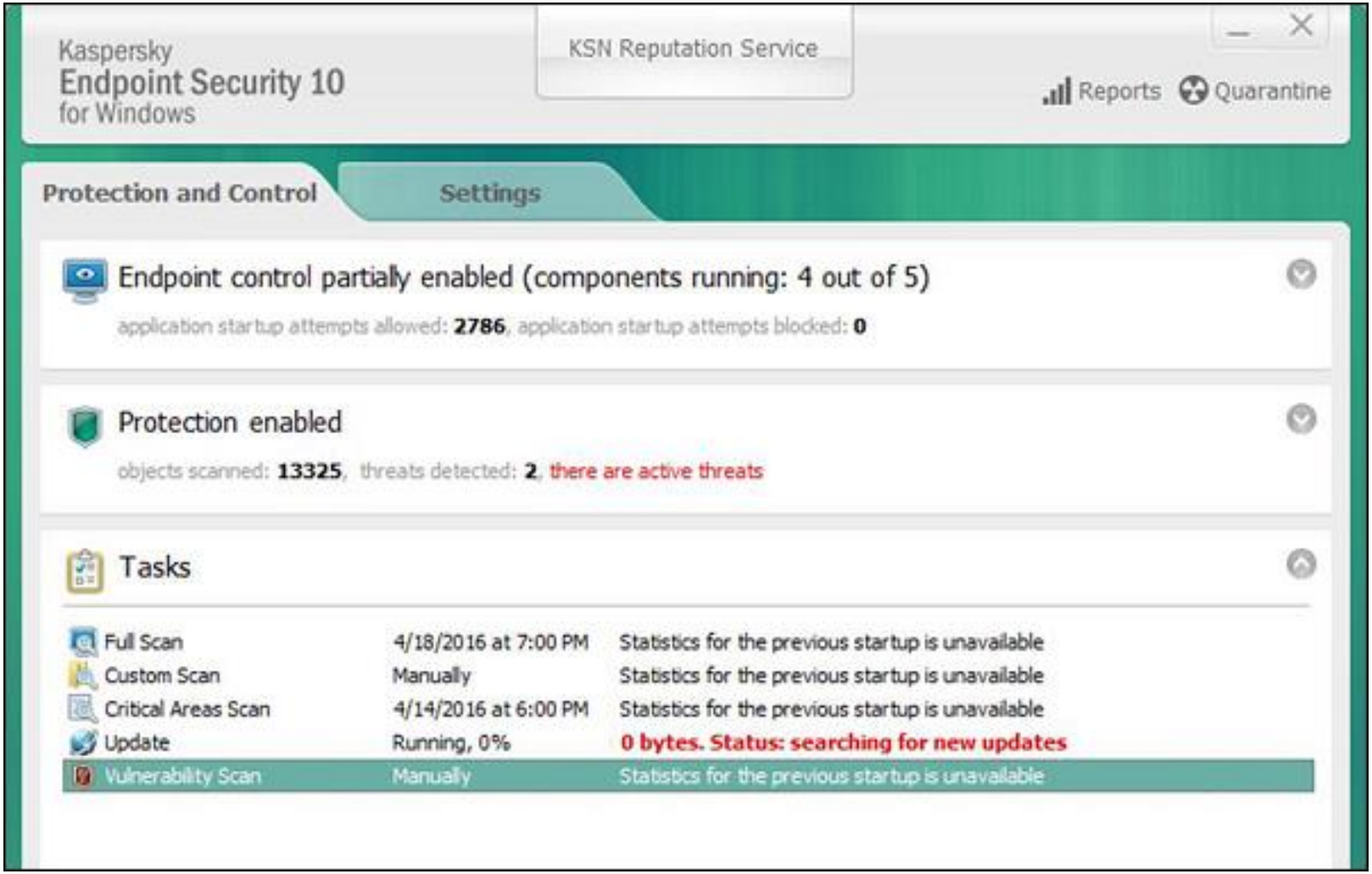
Some Basic Computer Security Checklist

There are some basic things that everyone of us in every operating system need to do –

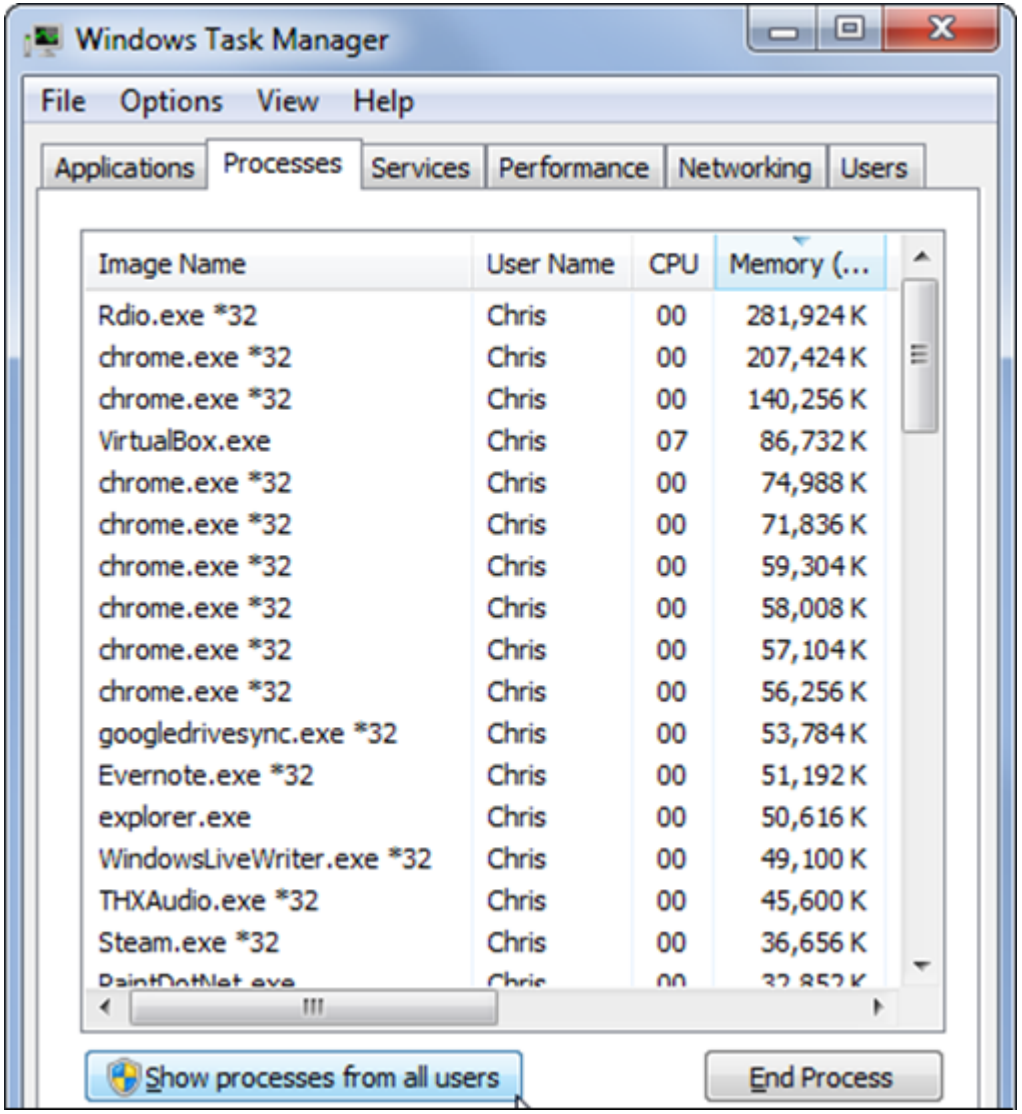
- Check if the user is password protected.
- Check if the operating system is being updated. In my case, I did a screenshot of my laptop which is a Windows 7.



- Check if the antivirus or antimalware is installed and updated. In my case, I have a Kaspersky antivirus being updated.



- Check for the unusual services running that consumes resources.



- Check if your monitor is using a screen saver.
- Check if the computer firewall is on or not.
- Check if you are doing backups regularly.
- Check if there are shares that are not useful.
- Check if your account has full rights or is restricted.
- Update other third party software’s.